



UNIVERSIDADE ESTADUAL PAULISTA
“JÚLIO DE MESQUITA FILHO”
Câmpus de Marília

Cecília Preciosa Cabsela

PROTEÇÃO DE DADOS PESSOAIS EM MOÇAMBIQUE:

Uma questão arquivística

Marília

2025

Cecília Preciosa Cabsela

PROTEÇÃO DE DADOS PESSOAIS EM MOÇAMBIQUE:

Uma questão arquivística

Tese apresentada ao Programa de Pós-Graduação em Ciência da Informação como parte das exigências para a obtenção do título de Doutor em Ciência da Informação pela Faculdade de Filosofia e Ciências, Universidade Estadual Paulista (UNESP), Campus de Marília.

Área de Concentração: Informação, Tecnologia e Conhecimento

Orientador (a): Prof. Dra. Sonia Maria Troitiño Rodriguez

Marília

2025

Ficha catalográfica

C117p

Cabsela, Cecília Preciosa

PROTEÇÃO DE DADOS PESSOAIS EM MOÇAMBIQUE :
Uma questão arquivística / Cecília Preciosa Cabsela. -- Marília,
2025

321 p. : il.

Tese (doutorado) - Universidade Estadual Paulista (UNESP),
Faculdade de Filosofia e Ciências, Marília

Orientadora: Sonia Maria Troitiño Rodriguez

1. proteção de dados pessoais. 2. gestão de documentos. 3.
política arquivística nacional. 4. Moçambique. 5. legislação. I.
Título.

Sistema de geração automática de fichas catalográficas da Unesp. Dados fornecidos
pelo autor(a).

Impacto potencial desta pesquisa

A tese tem um impacto potencial em várias dimensões com destaque para os potenciais científico, social, de internacionalização e impacto potencial aliado aos objetivos de desenvolvimento sustentável, concretamente o objetivo 16 sobre “Paz, Justiça e Instituições Eficazes”. Esta pesquisa foi desenvolvida num cenário em que os dados pessoais têm estado cada vez mais expostos. Atendendo que os dados pessoais estão contidos em documentos, de arquivo em particular, na dimensão científica a pesquisa tem o potencial de confirmar a relação indissociável entre a proteção de dados pessoais e a gestão de documentos, vistos dentro de uma política arquivística nacional, proporcionando deste modo um aprofundamento teórico nos campos da Arquivologia e da Ciência da Informação, bem como uma extensão dessa discussão à Moçambique, um contexto em que a estas ciências e a própria temática da proteção de dados pessoais são embrionárias, consubstanciando-se assim a dimensão inerente à internacionalização. Quanto ao objetivo 16, dos objetivos de desenvolvimento sustentável, esta pesquisa tem um impacto potencial especificamente nos objetivos 16.6 “Desenvolver instituições eficazes, responsáveis e transparentes em todos os níveis” e 16.10 “Assegurar o acesso público à informação e proteger as liberdades fundamentais, em conformidade com a legislação nacional e os acordos internacionais”, pois com esta tese, que se situa no balanço entre o acesso e a privacidade, espera-se contribuir para a elaboração de uma política arquivística em Moçambique que contemple a proteção de dados pessoais, por um lado, e por outro, esperamos contribuir para a elaboração de normativas de proteção de dados pessoais que respeitem os preceitos arquivísticos. Na sua dimensão social, a tese tem um impacto potencial na vida de cidadãos moçambicanos, brasileiros e outros que residem em Moçambique, através do maior cuidado com os dados pessoais que as instituições públicas, em particular, poderão passar a ter decorrente das diretrizes que a tese avança, colocando assim esses cidadãos menos vulneráveis a crimes perpetráveis através de seus dados pessoais.

Potential impact of this research

The thesis has a potential impact in several dimensions, with emphasis on the scientific, social, internationalization and potential impact allied to the Sustainable Development Goals, specifically Goal 16 on “Peace, Justice and Effective Institutions”. This research was carried out against a backdrop in which personal data has been increasingly exposed. Given that personal data is contained in documents, archival documents in particular, in the scientific dimension the research has the potential to confirm the inseparable relationship between personal data protection and document management, seen within a national archival policy, thus providing a theoretical deepening in the fields of Archival Science and Information Science, as well as an extension of this discussion to Mozambique, a context in which these sciences and the very subject of personal data protection are embryonic, thus embodying the inherent dimension of internationalization. As for goal 16 of the Sustainable Development Goals, this research has a potential impact specifically on goals 16.6 “Develop effective, accountable and transparent institutions at all levels” and 16.10 “Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements”, because this thesis, which is located in the balance between access and privacy, hopes to contribute to the development of an archival policy in Mozambique that takes into account the protection of personal data, on the one hand, and on the other, we hope to contribute to the development of personal data protection regulations that respect archival precepts. In its social dimension, the thesis has a potential impact on the lives of Mozambican citizens, Brazilians and others who live in Mozambique, through the greater care with personal data that public institutions, in particular, will be able to take as a result of the guidelines that the thesis puts forward, thus making these citizens less vulnerable to crimes perpetrated through their personal data.

Cecília Preciosa Cabsela

PROTEÇÃO DE DADOS PESSOAIS EM MOÇAMBIQUE:

Uma questão arquivística

Tese apresentada ao Programa de Pós-Graduação em Ciência da Informação como parte das exigências para a obtenção do título de Doutor em Ciência da Informação pela Faculdade de Filosofia e Ciências, Universidade Estadual Paulista (UNESP), Campus de Marília.

Área de Concentração: Informação, Tecnologia e Conhecimento

Orientador (a): Prof. Dra. Sonia Maria Troitiño Rodriguez

Banca Examinadora

Prof^a. Dr^a. Sonia Maria Troitiño Rodriguez
UNESP – Câmpus de Marília
Orientadora

Prof^a. Dr^a. Rúbia Martins
UNESP – Câmpus de Marília

Prof. Dr. Juan Bernardo Montoya Mogollón
UFPA

Prof. Dr. Marcelo Fernandes de Oliveira
UNESP – Câmpus de Marília

Prof^a. Dr^a. Maria Cristina Vieira de Freitas
UC – Portugal

Marília, 24 de outubro de 2025.

A mim...

E ao país que sonho ver arquivisticamente melhor, Moçambique!

AGRADECIMENTOS

Gratidão é o sentimento que enche o meu peito ao chegar até aqui.

O que seria de mim sem o onnipresente e onipotente? Obrigada, Senhor, por estar sempre comigo, levantar, iluminar e guiar. Por ser a minha força, quando fraca estou.

Quero endereçar os meus agradecimentos, aos meus pares, Gildo Carlos Macie, Leonor Celeste Silva e Ranito Zambo Waete, pelas discussões intensas, profundas, sem hora e incessantes. Discussões que não se encerram com a apresentação desta tese. Vocês tornaram o trabalho da reflexão e escrita menos solitário.

Incontornavelmente devo manifestar a minha gratidão aos meus pais, Adija Bunaia N. Mandu e Cosme Cabsela Mandu, por terem sido desde sempre tão compreensivos, solidários, pacientes e amorosos. Foram obrigados a ter uma filha ausente, foram obrigados a adiar conversas, foram obrigados inclusive a compreender o que é uma tese de doutorado. Meus pais, minha eterna gratidão por sempre serem vocês. Os meus irmãos, como peixinhos filhos de peixes, foram e são sublimes. Cella Cosme Cabsela, Beatriz Cosme Cabsela e Tina Adija Cosme, obrigada pelo incentivo, partilha do peso e compreensão pela ausência.

À coordenação do PPGCI, desde a gestão da Profa. Marta, passando pela gestão da Profa. Helen, até a gestão da Profa. Dra. Márcia, só tenho a agradecer por toda a atenção, confiança e ensinamento. Esse agradecimento é extensivo a todos os Professores do PPGCI da UNESP.

À minha orientadora, Profa. Sonia Troitiño, manifesto a minha profunda gratidão por ter abraçado o desafio proposto, mesmo quando tudo ainda não estava tão claro. Por ter segurado em minha mão no enfrentamento dos desafios todos que vieram com o andar do doutorado. Por ter sentido junto comigo, as minhas próprias dores. Agradeço-lhe pela confiança que depositou em mim desde o primeiro momento e por me ter permitido ousar e tentar. Muito obrigada!

Os meus agradecimentos se estendem aos membros da banca de defesa do Doutorado, as Professoras Rúbia Martins (UNESP) e Maria Cristina Vieira de Freitas

(UC), os Professores Marcelo Fernandes de Oliveira (UNESP) e Juan Bernardo Montoya Mogollón (UFPA).

A Profa. Rosângela Caldas, uma mulher de uma sensibilidade indescritível, agradeço pelo papel imensurável que teve na minha estadia no Brasil e até o dia que me levou à Rodoviária de Marília, de volta à Moçambique. O carinho e gratidão que tenho por si são para a vida inteira.

A Profa. Luana e Prof. Carlos pela hospitalidade, sempre!

Aos colegas brasileiros pelo acolhimento durante a estadia no Brasil e a continuidade virtual. Um especial “obrigada!” ao Wilson Veronez, ao Raidan da Cruz (que “carimbava as Três Lagoas”), Franciele Franco e Mariana Borges, por tudo. Junta-se a colega venezuelana Orledys López Caldera, “amiga linda”, por todo suporte, apoio, toda atenção e predisposição, mas também por toda risada e amizade que transcende o Doutorado.

À Escola Superior de Jornalismo (Moçambique), pela oportunidade ímpar!

Ao senhor Domingos Simba da Assembleia da República de Moçambique, manifesto a minha gratidão pela dedicação e entrega na busca das fontes necessárias para consecução desta tese.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001. Graças a Capes PROEX pude ter um dos anos mais produtivos do doutorado no Brasil.

A todos os pesquisadores, escritores, arquivistas que, através dos seus escritos, pude montar o mosaico desta tese.

A todas as pessoas singulares e coletivas que contribuíram para a concretização desta tese, obrigada!

“O segredo impediria um *controle* mais efetivo por parte da sociedade sobre seus governantes, constituindo uma forma de evitar o julgamento, preservando, assim, o lugar do poder.”

José Maria Jardim (2008, p. 86)

RESUMO

A proteção de dados pessoais figura como um direito fundamental em vários instrumentos legais e ordenamentos jurídicos mundo afora. À semelhança do direito à informação, este direito, quando violado, pode afetar, gravemente, outros direitos fundamentais das pessoas. Portanto, a preocupação com a proteção de dados pessoais toca os mais variados setores de atuação profissional e, obviamente, áreas do saber científico, com destaque aqui para a Arquivologia e a Ciência da Informação. É neste sentido que a presente tese foi desenvolvida embasada nos questionamentos como: (a) de que forma se estabelece a relação da proteção de dados pessoais com a gestão de documentos dentro do escopo de uma política arquivística no cenário moçambicano?; (b) Os aspectos da gestão de documentos para a proteção de dados pessoais estão devidamente incorporados nas normativas moçambicanas atinentes à proteção de dados pessoais?; (c) Como é tratada a proteção de dados pessoais na legislação moçambicana?. Todo o exercício que conduziu este trabalho de pesquisa procurou, de forma geral, estabelecer a relação da gestão de documentos e a proteção de dados pessoais no bojo de uma política arquivística e propor diretrizes arquivísticas para a elaboração de normativas de proteção de dados pessoais em Moçambique. A consecução deste objetivo e a prossecução da tese, foi mediante a adoção de uma abordagem ou natureza qualitativa, sob a qual foi realizada uma pesquisa aplicada do tipo documental e igualmente exploratório-descritiva. Esta tese reveste-se de estudo de caso como método de pesquisa e no qual utilizou-se da análise de conteúdo como método de tratamento e análise de dados, que foram levantados através da revisão de literatura, da observação indireta e da pesquisa documental. Da pesquisa realizada, identificamos o lugar da proteção de dados pessoais no processo de gestão de documentos, o papel do arquivista nessa proteção, assim como foram identificadas uma série de normativas específicas de proteção de dados em diversos países, incluindo Brasil. Em Moçambique a proteção de dados pessoais configura-se como direito fundamental desde a Constituição da República de 1990, mas ainda não foi adotada uma normativa específica, existindo uma Proposta de Lei de Protecção de Dados Pessoais e estando em implementação normativas conexas. Constatou-se igualmente que Moçambique não conta com uma política arquivística nacional formulada e formalizada e infere-se que essa inexistência contribui para, em cadeia, a inexistência, de fato, de um sistema nacional de arquivos e consequente operações e procedimentos da gestão de documentos *ad hoc*. Conclui-se que gestão de documentos e proteção de dados pessoais têm uma relação indissociável e que Moçambique tem legislação de base para a proteção de dados pessoais, contudo deve adotar uma normativa específica consentânea com a gestão de documentos, assim como deve elaborar e formalizar uma política arquivística nacional a fim de eliminar as incongruências atualmente existentes no cenário arquivístico e melhor orientar as atividades de gestão de documentos, que reforçam a proteção de dados pessoais. Para isso foram propostas diretrizes arquivísticas para a elaboração de normativas de proteção de dados pessoais e que são igualmente diretrizes para a reversão do cenário arquivístico moçambicano.

Palavras-chave: proteção de dados pessoais; gestão de documentos; política arquivística nacional; Moçambique; legislação.

ABSTRACT

Personal data protection is a fundamental right in various legal instruments and legal systems around the world. Like the information rights, this right, if violated, can seriously affect people's other fundamental rights. Therefore, the concern with personal data protection touches the most varied sectors of professional activity and, obviously, areas of scientific knowledge, with emphasis here on Archival Science and Information Science. It is in this sense that this thesis was developed based on the questions (a) how is the relationship between the personal data protection and records management established within the scope of an archival policy in the Mozambican scenario? (b) Are the aspects of records management for the personal data protection duly incorporated into Mozambican regulations on the personal data protection? How is personal data protection dealt with in Mozambican legislation? (c) The whole exercise that led to this research work sought, in general, to establish the relationship between records management and the personal data protection within an archival policy and to propose archival guidelines for the drafting of personal data protection regulations in Mozambique. This objective and the thesis were achieved by adopting a qualitative approach, under which applied documental research and exploratory-descriptive type was carried out. This thesis is based on a case study as the research method, in which content analysis was used as the method for processing and analyzing the data, which was collected through a literature review, indirect observation and documentary research. From the research carried out, we identified the place of personal data protection in the records management process, the role of the archivist in this protection, as well as a series of specific data protection regulations in various countries, including Brazil. In Mozambique, personal data protection has been a fundamental right since the Constitution of the Republic of 1990, but specific legislation has not yet been adopted, although there is a Personal Data Protection Bill and related legislation is being implemented. It was also found that Mozambique does not have a formulated and formalized national archives policy, and it can be inferred that this absence contributes to the *de facto* lack of a national archives system and consequent *ad hoc* records management operations and procedures. The conclusion is that records management and the personal data protection are inextricably linked and that Mozambique has basic legislation for the personal data protection, but must adopt specific regulations in line with records management, as well as draw up and formalize a national archival policy in order to eliminate the inconsistencies that currently exist in the archival landscape and better guide records management activities, which reinforce the personal data protection. To this end, archival guidelines have been proposed for the development of personal data protection regulations, which are also guidelines for reversing the Mozambican archival scenario.

Keywords: personal data protection; records management; national archival policy; Mozambique; legislation.

LISTA DE FIGURAS

Figura 1 – Etapas da aplicação da análise de conteúdo	18
Figura 2 – Relação de políticas públicas, política arquivística e sistema de arquivo	51
Figura 3 – Abordagens sobre Arquivística em Rousseau e Couture (1998)	63
Figura 4 – Características de documentos de arquivo em Durante (1994)	65
Figura 5 – O arquivista na proteção de dados pessoais	80
Figura 6 – Principais atores da arena arquivística moçambicana	119
Figura 7 – Legislação moçambicana de Proteção de dados pessoais	174
Figura 8 – Principais entidades na proteção de dados pessoais em Moçambique	181
Figura 9 – Direitos do titular dos dados na Proposta de Lei de Protecção de Dados Pessoais	201
Figura 10 – Atores do processo de Proteção de dados pessoais em Moçambique	215
Figura 11 – Ecossistema da Proteção de dados pessoais em Moçambique	216
Figura 12 – Diretrizes arquivísticas para a elaboração de normativas de proteção de dados pessoais	228
Figura 13 – Proteção de dados pessoais consentânea com a gestão de documentos	229

LISTA DE QUADROS

Quadro 1 – Aplicação da análise de conteúdo	22
Quadro 2 – Natureza de assuntos de documentos de arquivo	39
Quadro 3 – Princípios e funções arquivísticas	71
Quadro 4 – Definições nas versões do Sistema Nacional de Arquivos (de Estado)	108
Quadro 5 – Disciplinas nucleares do curso de Arquivística da UEM	122
Quadro 6 – Gestão de documentos e Tratamento de dados pessoais	132
Quadro 7 – Definições no âmbito da proteção de dados pessoais	132
Quadro 8 – Princípios de tratamento de dados pessoais	134
Quadro 9 – Princípios de tratamento de dados pessoais face aos princípios arquivísticos e ao papel do arquivista na proteção de dados pessoais	135
Quadro 10 – Principal legislação internacional de proteção de dados pessoais	141
Quadro 11 – Principal legislação brasileira de proteção de dados pessoais	146
Quadro 12 – Principal legislação africana de proteção de dados pessoais	153
Quadro 13 – Definições no âmbito da Lei de Transacções Electrónicas	160
Quadro 14 – Princípios de tratamento de dados pessoais no RGPD, na LGPD e na Proposta de Lei de Protecção de Dados Pessoais de Moçambique	189
Quadro 15 – Direito de informação e Direito de acesso na Proposta de Lei de Protecção de Dados Pessoais	197

LISTA DE ABREVIATURAS E SIGLAS

AAM	Associação dos Arquivistas de Moçambique
AfDec	<i>African Declaration on Internet Rights and Freedoms (AfDec)</i> <i>Coalition</i>
AHM	Arquivo Histórico de Moçambique
AMOABI	Associação Moçambicana de Arquivistas e Bibliotecários
ANPD	Autoridade Nacional de Proteção de Dados
ARBIDOC	Associação Moçambicana de Arquivistas, Bibliotecários e Documentalistas
ARCO	Acesso, Retificação, Cancelamento e Oposição
BD	Biblioteconomia e Documentação
BI	Bilhete de Identidade
BM	Banco de Moçambique
BR	Boletim da República
CEDIMO	Centro Nacional de Documentação e Informação de Moçambique
CI	Ciência da Informação
CIDOC	Instituto Médio de Ciências Documentais
CIRAP	Comissão Interministerial da Reforma da Administração Pública
CIRESP	Comissão Interministerial da Reforma do Sector Público
CGTSJ	Centro de Gestão de Tecnologias do Sector da Justiça
CNA	Conselho Nacional de Arquivos
CNAD	Comissão Nacional de Avaliação de Documentos
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
CPF	Cadastro de Pessoa Física
CPISE	Comissão Nacional para Implementação das Normas de Segredo do Estado

CPLP	Comunidade dos Países de Língua Portuguesa
CRM	Constituição da República de Moçambique
DUDH	Declaração Universal dos Direitos Humanos
ECA	Escola de Comunicação e Artes
EGDAE	Estratégia para a Gestão de Documentos e Arquivos do Estado
EGRSP	Estratégia Global da Reforma do Sector Público
ESJ	Escola Superior de Jornalismo
e-SNGD	Sistema Nacional De Gestão Documental
FRELIMO	Frente de Libertação de Moçambique
GD	Gestão de Documentos
IES	Instituições do Ensino Superior
INAGE	Instituto Nacional de Governo Electrónico
INCM	Instituto Nacional das Comunicações de Moçambique
INTIC	Instituto Nacional de Tecnologias de Informação e Comunicação
IP	<i>Internet Protocol</i>
LGPD	Lei Geral de Protecção de Dados Pessoais
MAEFP	Ministério da Administração Estatal e Função Pública
MICTES	Ministério da Ciência, Tecnologia e Ensino Superior
MJACR	Ministério da Justiça, Assuntos Constitucionais e Religiosos
OCDE	Organização para a Cooperação e o Desenvolvimento Económico
ODS	Objetivos de Desenvolvimento Sustentável
OUA	Organização da Unidade Africana
PNUD	Programa das Nações Unidas para o Desenvolvimento
PQG	Programa Quinquenal do Governo
RENAMO	Resistência Nacional Moçambicana
RGPD	Regulamento Geral sobre a Protecção de Dados

SADC	<i>Southern African Development Community</i> (Comunidade de Desenvolvimento da África Austral)
SADCC	Conferência de Coordenação do Desenvolvimento da África Austral
SCDM	Sistema de Certificação Digital de Moçambique
Séc.	Século
SISE	Serviço de Informações e Segurança do Estado
SNA	Sistema Nacional de Arquivos
SNAE	Sistema Nacional de Arquivos do Estado
SNE	Sistema Nacional de Educação
TIC	Tecnologia de Informação e Comunicação
UA	União Africana
UCTT	Unidade de Controlo de Tráfego de Telecomunicações
UC3M	Universidade Carlos III de Madrid
UEM	Universidade Eduardo Mondlane
UFMG	Universidade Federal de Minas Gerais

SUMÁRIO

1 INTRODUÇÃO.....	7
1.1 Problema	8
1.2 Hipótese.....	9
1.3 Objetivos	10
1.4 Justificativa	11
1.5 Tese.....	12
1.6 Procedimentos metodológicos	12
2 DOS DADOS AOS DOCUMENTOS DE ARQUIVO.....	25
2.1 Dado.....	25
2.2 Informação	28
2.2.1 Dados pessoais vs informação pessoal	31
2.3 Documento	33
2.3.1 Documento de arquivo	34
3 DA GESTÃO DE DOCUMENTOS E POLÍTICA ARQUIVÍSTICA À PROTEÇÃO DE DADOS PESSOAIS.....	41
3.1 Gestão de documentos.....	41
3.2 Política arquivística.....	47
3.2.1 Sistema nacional de arquivo	52
3.3 Proteção de dados pessoais	54
4 A PROTEÇÃO DE DADOS PESSOAIS DESDE UMA PERSPECTIVA ARQUIVÍSTICA	62
4.1 A Arquivologia, seus principais princípios e teoria.....	62
4.2 O Arquivista e a ética profissional.....	71
4.3 O arquivista na Proteção de Dados Pessoais	75

5 A ARENA ARQUIVÍSTICA MOÇAMBICANA.....	81
5.1 Moçambique: da estrutura administrativa em direção à estrutura arquivística.....	81
5.2 O Sistema Nacional de Arquivos do Estado e sua (des)estrutura arquivística.....	96
5.3 O Sistema Nacional de Gestão Documental (e-SNGD): um projeto	110
5.4 Principais atores da arena arquivística moçambicana.....	111
5.4.1 Arquivo Histórico de Moçambique (AHM)	111
5.4.2 Centro Nacional de Documentação e Informação de Moçambique (CEDIMO).....	113
5.4.3 Conselho Nacional de Arquivos (CNA)	117
5.4.4 Comissão Nacional de Avaliação de Documentos (CNAD).....	118
5.5 O arquivista moçambicano face à proteção de dados pessoais	119
5.5.1 Formação	119
5.5.2 Atuação profissional e associativismo.....	124
6 PANORAMA INTERNACIONAL E BRASILEIRO DA PROTEÇÃO DE DADOS PESSOAIS.....	129
6.1 Legislação internacional.....	129
6.2 Legislação brasileira	141
6.3 A África e a proteção de dados pessoais.....	147
7 O QUADRO LEGAL MOÇAMBICANO DA PROTEÇÃO DE DADOS PESSOAIS	155
7.1 Legislação moçambicana de proteção de dados pessoais: linha de tempo	155
7.2 Principais atores do cenário de proteção de dados pessoais em Moçambique.....	174
7.2.1 Instituto Nacional das Comunicações de Moçambique (INCM)	175
7.2.2 Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC)	176

7.2.3 Instituto Nacional de Governo Electrónico (INAGE).....	179
8 PELA PROTEÇÃO DE DADOS PESSOAIS CONSENTÂNEA COM POLÍTICA ARQUIVÍSTICA EM MOÇAMBIQUE	182
8.1 A Proposta de Lei de Proteção de Dados Pessoais sob a lupa arquivística	182
8.2 Diretrizes arquivísticas para a elaboração de normativas de proteção de dados pessoais.....	217
8.2.1 Elaboração e formalização de política arquivística em Moçambique.....	217
8.2.2 Revisão do sistema nacional de arquivos de Moçambique	219
8.2.3 Institucionalização da gestão de documentos em Moçambique	221
9 CONSIDERAÇÕES FINAIS	230
REFERÊNCIAS	241
Legislação	249
APÊNDICES	255
Apêndice A – Legislação moçambicana de arquivos e de proteção de dados pessoais	256
Apêndice B – Mapeamento de rol de matérias da Assembleia da República de Moçambique.....	261
ANEXOS.....	268
Anexo A – Proposta de Lei de Protecção de Dados Pessoais.....	269

1 INTRODUÇÃO

É consensual que com o passar do tempo, junto da evolução e transformação proporcionada pelas tecnologias, comunicação e informação, em particular, a vida das pessoas tem sido bastante afetada, positivamente assim como negativamente. À medida que essas tecnologias aumentam a capacidade do Homem em determinados cenários, outros diminui a sua capacidade. Aliás, Bellotto (2006) apontou que as tecnologias aumentaram a capacidade de gerar, reunir, recuperar, examinar e utilizar dados com os mais diversos objetivos.

Portanto, estes objetivos podem ser dos mais nocivos aos mais benéficos para a vida em sociedade. Bellotto (2006) indicou que uma vantagem dessas tecnologias é possibilitar o acesso à informação a distância e auxiliar na eliminação de dados/informações que podem ser supérfluas ou mesmo redundantes. Ora, essa possibilidade de aceder a dados remotamente pode ser um fator de risco para as pessoas singulares e/ou coletivas, públicas e/ou privadas, pois por esta via dados pessoais podem ser violados dolosamente.

Como Traça e Neves (2016) entendem, essas tecnologias afetaram todos os países, sejam de capitalismo central ou não. Afetaram de tal maneira que criaram severos impactos sem alguns direitos que se consideravam garantidos, como é o caso do direito à privacidade. Moçambique não é exceção, à semelhança de muitos outros países, a estrutura legal parece ainda não conseguir fazer face a este cenário.

Ora, com um quadro legal robusto ou não, o profissional da informação, concretamente o arquivista é chamado a aliar os seus saberes mais específicos com o saber fazer de outras áreas visando intervir de forma mais completa possível no cenário de recrudescimento de uso de tecnologias e suas consequências para o Estado, para as instituições ordinárias e a sociedade em geral, para não falar para cada um dos cidadãos.

Nesta introdução, apresentamos o problema de pesquisa identificado e suas questões de partida, a hipótese que levantamos, os objetivos traçados, a justificativa, a tese que defendemos e os procedimentos metodológicos adotados.

Antes de avançarmos para as subseções, importa referenciar que neste trabalho são exploradas diversas normativas moçambicanas, desde as que são atinentes à gestão de documentos, àquelas que são conexas à proteção de dados pessoais em Moçambique. Este fato, em particular, propicia a ocorrência em grande escala, de ortografia e terminologia usual em Moçambique e, por via de questões históricas, em Portugal também. Ademais, a nossa condição de pesquisadora moçambicana nos coloca em posição de facilmente incorrerem ao uso de expressões mais comumente usadas nos contextos que acabamos de apontar. Portanto, o(a) leitor(a) é convidado(a) ao convívio de duas formas ortográficas ao longo desta tese.

1.1 Problema

Moçambique é um país caracterizado, na generalidade, por uma desordem informacional nas mais diversas instituições, de diversos domínios. Essa desordem pode estar intimamente ligada a falta de gestão de documentos (e uma política arquivística que a embase) que por sua vez pode ser motivada por questões técnicas e/ou político-administrativas. Dentro deste contexto, são igualmente vários constrangimentos causados às próprias instituições e aos cidadãos. Estes últimos se vêm muitas vezes impedidos de usufruir dos seus direitos ou então vêm os seus direitos violados, fruto da má ou inexistente gestão de documentos. Dos impedimentos e/ou violações, podemos destacar o impedimento ao acesso à informação e a violação da proteção dos dados pessoais.

Em matéria de gestão de documentos, Moçambique tem instrumentos normativos que regulam a atividade, mas que muitas vezes não espelham a realidade, além de serem contraditórios entre si. Aliás estas normativas não nascem de uma política arquivística nacional explícita formalizada em um documento. Ora, possuindo um marco legal desde finais do século XX, a situação arquivística em Moçambique carece ainda de maturação, como se pode compreender a partir dos trabalhos de alguns autores moçambicanos, com destaque para os trabalhos de Nharreluga (2006, 2009, 2014, 2021). Nos dias que correm, os arquivos continuam ausentes dentro das estruturas das diversas instituições públicas mesmo que o chamado Sistema Nacional de Arquivos de Estado esteja na sua terceira versão, tendo, a primeira, sido inaugurada em 1992.

Sobre a proteção de dados pessoais, Moçambique conta nos dias atuais com alguma legislação não específica, como é o caso da Lei de Direito à Informação (2014), Lei de Transacções Electrónicas (2017), Política e Estratégia Nacional de Segurança Cibernética (2021), entre outros, portanto dispositivos legais conexos, sem haver necessariamente uma normativa sobre a proteção de dados pessoais. Contudo, a questão da proteção de dados pessoais encontra fundamentos desde a Constituição da República de Moçambique de 1990.

A combinação destes cenários que indicam a ausência de normativas específicas de proteção de dados pessoais e uma desordem arquivística representam uma fragilidade para o cumprimento dos deveres das instituições e fruição dos direitos do cidadão moçambicano na medida em que, não há até aqui, o que possa assegurar de forma efetiva que os seus dados pessoais não sejam violados e/ou extraviados, mesmo dentro do circuito das instituições públicas. Ora, aspectos de proteção de dados pessoais aparecem de forma mais ou menos explícita nas normativas atinentes à gestão de documentos, porém muito implicitamente ou mesmo inexistente estão as questões de gestão de documentos nessas normativas conexas de proteção de dados pessoais que colocam o acento tônico na informática.

Diante dessa temática relativamente nova no contexto moçambicano, vista geralmente na ótica da Informática e do Direito, nos inquietamos sob olhar da Arquivologia ao perguntar: (a) de que forma se estabelece a relação da proteção de dados pessoais com a gestão de documentos dentro do escopo de uma política arquivística no cenário moçambicano? (b) Os aspectos da gestão de documentos para a proteção de dados pessoais estão devidamente incorporados nas normativas moçambicanas atinentes à proteção de dados pessoais? (c) Como é tratada a proteção de dados pessoais na legislação moçambicana?

1.2 Hipótese

Hipótese é considerado por Marconi e Lakatos (2023) como um enunciado geral de relações entre variáveis que é formulado como solução provisória para determinado problema, apresentando caráter explicativo ou preditivo, compatível com o conhecimento científico e revelando consistência lógica, bem como passível de

verificação empírica em suas consequências. A autora indica que “as hipóteses podem ser formuladas *a priori*, antes da análise dos dados coletados, ou *a posteriori* depois da análise dos dados coletados ter sido realizada” (Marconi; Lakatos, 2023, p. 153).

Assim formulamos, *a priori*, uma hipótese para o nosso trabalho, tendo em conta o tema e o problema levantados:

- Se a política arquivística deve orientar o desenvolvimento de atividades que dizem respeito à gestão de documentos, então na gestão de documentos residem as ações para o controle e proteção de dados pessoais contidos nos documentos, havendo assim uma relação indissociável entre a gestão de documentos e a proteção de dados pessoais, no escopo de uma política arquivística nacional.

1.3 Objetivos

Tendo em conta o problema identificado, são apresentados aqui o objetivo geral e os objetivos específicos, de modo a procurar responder a inquietação levantada. Assim, o nosso objetivo geral consiste em estabelecer a relação da gestão de documentos e a proteção de dados pessoais no bojo de uma política arquivística e propor diretrizes arquivísticas para a elaboração de normativas de proteção de dados pessoais em Moçambique. Diante deste objetivo geral, foram definidos os seguintes objetivos específicos:

- Compreender os conceitos de política arquivística nacional, de gestão de documentos e de proteção de dados pessoais;
- Analisar o cenário arquivístico moçambicano;
- Levantar o quadro legal da proteção de dados pessoais no âmbito internacional, no Brasil e traçar uma linha de tempo da proteção de dados pessoais em Moçambique.
- Identificar o papel da gestão de documentos e do seu profissional na proteção de dados pessoais;
- Analisar a relação da gestão de documentos e proteção de dados pessoais;
- Propor diretrizes para a elaboração de normativas de proteção de dados pessoais consentâneas com a gestão de documentos.

1.4 Justificativa

Diante de um cenário em que os dados pessoais têm estado cada vez mais vulneráveis e agravando-se em contextos sem uma configuração arquivística robusta e estável, auguramos que com a realização desta tese, possamos contribuir para a elaboração de uma política arquivística em Moçambique que contemple a proteção de dados pessoais, por um lado, e por outro, esperamos contribuir para a elaboração de normativas de proteção de dados pessoais em Moçambique que respeitem os preceitos arquivísticos. Portanto, a tese sugere modificações no cenário arquivístico moçambicano através da formulação de uma política arquivística nacional, para se efetivar a gestão de documentos e por via desta se assegurar a proteção de dados pessoais.

Ao estabelecermos a relação da gestão de documentos com a proteção de dados pessoais dentro do grande guarda-chuvas que é a política arquivística, esperamos contribuir para a confirmação desta relação, não só teoricamente como também na prática através do estudo do contexto moçambicano.

Esperamos que a tese possa contribuir para o aprofundamento do campo teórico da Arquivologia e da Ciência da Informação destacando elementos que colocam mais evidente a relação indissociável da gestão de documentos e a proteção de dados pessoais. Esta contribuição vê-se ainda de maior importância em Moçambique, nosso referencial empírico, pois é um contexto em que a Arquivologia, a Ciência da Informação, bem como a temática da proteção de dados pessoais são embrionárias.

A tese oferece um ampliar de temáticas de pesquisa na área da Arquivologia e da Ciência da Informação em Moçambique e no mundo, despertando assim nos estudiosos da área mais um eixo de pesquisa a explorar.

Esperamos igualmente apresentar subsídios para que seja considerada a gestão de documentos na legislação de proteção de dados pessoais de Moçambique. Assim, a tese reafirma também a relação interdisciplinar entre a Arquivologia, o Direito e a Informática.

Com forte carga social, esperamos que a tese possa suscitar maior cuidado para a proteção de dados pessoais dos cidadãos moçambicanos e demais residentes

em Moçambique, observando-se assim um direito fundamental e um direito humano. Aliás, aqui reside a maior contribuição desta tese além fronteiras. Ela se situa no “corredor” da vida das pessoas de todo o mundo e pretende-se uma espécie de manifesto para que os Estados, as empresas privadas, etc., ao não se escaparem das questões de proteção de dados pessoais, tomem as rédeas da gestão de documentos para esse feito.

1.5 Tese

Defende-se aqui a tese segundo a qual não se pode garantir a efetiva proteção de dados pessoais (dos moçambicanos e outros) sem, junto a outras ações, realizar efetivamente a gestão de documentos, pois esses dados pessoais são parte indissociável da composição documental, sejam eles documentos digitais ou não. E para que a gestão de documentos ocorra, a política arquivística, em particular a nacional, deve ser elaborada, formalizada em documento e implementada, orientando entre outras, o desenvolvimento de atividades de gestão de documentos.

1.6 Procedimentos metodológicos

A presente seção visa apresentar os procedimentos metodológicos a serem seguidos para a realização da tese intitulada “Proteção de dados pessoais em Moçambique: uma questão arquivística”. Essa tese, em sua finalidade, classifica-se como pesquisa aplicada pois, conforme Gil (2025, p. 41), essas pesquisas são “voltadas à aquisição de conhecimentos com vistas à aplicação numa situação específica”. Portanto, ao analisarmos o contexto moçambicano e ao elaborarmos diretrizes arquivísticas para a formulação de normativas de proteção de dados pessoais, augura-se a implementação dessas diretrizes propostas de modo a melhorar não apenas as condições de proteção de dados pessoais em Moçambique, mas também o cenário arquivístico moçambicano, de um modo geral.

A pesquisa realizada classifica-se, quanto a natureza, em qualitativa justamente pela natureza dos dados. Ou seja, se os resultados das pesquisas quantitativas são expressos em números, nas pesquisas qualitativas, como esta que realizamos, os resultados são apresentados por meio de descrições verbais, como avança Gil (2025) e, antes, na coleta e análise de dados, foram empregadas técnicas de pesquisa qualitativa, a saber: revisão de literatura, observação indireta e análise de conteúdo categorial.

Dentro desta abordagem ou natureza qualitativa, a pesquisa desenvolvida é do tipo documental e igualmente exploratório-descritivo. A característica da pesquisa documental, segundo Marconi e Lakatos (2023, p. 202), “é tomar como fonte de coleta de dados apenas documentos, escritos ou não, que constituem o que se denomina de fontes primárias”. Dentre diferentes fontes de documentos deste tipo de pesquisa, as autoras apontam os arquivos públicos, que podem ser municipais, estaduais e nacionais. Em sua maior parte, conforme indicam, eles contêm documentos oficiais (ordens régias, leis, ofícios, relatórios, anuários, alvarás etc.), publicações parlamentares (atas, documentos, projetos de lei, impressos, relatórios etc.), documentos jurídicos oriundos de cartórios (registros de nascimentos, casamentos, desquites e divórcios, mortes; escrituras de compra e venda; falências e concordatas; testamentos, inventários etc.) e iconografia (Marconi; Lakatos, 2023).

Para além das fontes de documentos, Marconi e Lakatos (2023) também falam de tipos de documentos. Dentre eles, destaca os escritos, constituídos por documentos oficiais, publicações parlamentares, documentos jurídicos, fontes estatísticas, publicações administrativas e documentos particulares.

Para o desenvolvimento desta pesquisa nos servimos de documentos como normativas do Brasil, de Moçambique e de outros países inerentes a proteção de dados pessoais e a gestão de documentos, localizáveis impressos na biblioteca do Arquivo Histórico de Moçambique, como também em formato eletrônico pelo portal do Governo de Moçambique, pelo Gazettes.Africa¹, uma coleção que compila diversa legislação do continente africano. Neste contexto, analisamos a proposta de lei de proteção de dados pessoais de Moçambique, versão de 2024² consultada à 20 de

¹ Disponível em <https://gazettes.africa/> .

² Datada de 26 de junho de 2024.

abril de 2025, relatórios de diferentes entidades e publicações administrativas da Assembleia da República de Moçambique.

Sobre as normativas, importa ainda precisar que foram analisadas aquelas que estiveram em vigor até ao momento da submissão do trabalho. Para casos como o do Sistema Nacional de Arquivos (de Moçambique), alguns instrumentos normativos revogados foram mobilizados com vista a apontar a história da configuração arquivística moçambicana.

Toda pesquisa tem seus objetivos, diferentes dos de outras, sendo que em seus propósitos elas podem ser classificadas em exploratórias, descritivas e explicativas (Gil, 2022). Atendendo aos objetivos mais gerais da nossa pesquisa, ela é classificada como exploratória-descritiva.

A combinação destas duas, deve-se ao fato de que as pesquisas exploratórias têm como propósito proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito, podendo ter a coleta de dados envolvendo o levantamento bibliográfico e entrevistas com pessoas que tiveram experiência prática com o assunto. Aliás, Gil (2022) diz que se pode afirmar que a maioria das pesquisas realizadas com propósitos acadêmicos, num primeiro momento, assume o caráter de pesquisa exploratória, pois nesse momento é pouco provável que o pesquisador tenha uma definição clara do que irá investigar.

É neste contexto que a pesquisa exploratória nos ajudou a melhor delimitar a pesquisa e obter maior proximidade com referencial empírico que ela proporciona. Quer dizer, o tipo exploratório não só nos permitiu desenhar um quadro teórico resultante do levantamento bibliográfico que fizemos sobre gestão de documentos, política arquivística e proteção de dados pessoais como também nos permitiu visualizar a arena arquivística moçambicana e o quadro regulatório da proteção de dados pessoais em Moçambique.

Para a realização desta tese, esteve previsto a realização de entrevistas semiestruturadas com membros da(s) comissões da Assembleia da República de Moçambique, membro(s) do Conselho Nacional de Arquivos, funcionário(s) do órgão coordenador de implementação do Sistema Nacional de Arquivos do Estado, Centro Nacional de Documentação e Informação (CEDIMO), funcionário(s) da Divisão de Segurança Cibernética e Protecção de Dados do Instituto Nacional de Tecnologias de

Informação e Comunicação (INTIC) de Moçambique e pesquisadores da área da Arquivologia e da Ciência da Informação em Moçambique. Com a entrevista, o nosso principal interesse era captar as perspectivas e experiências dos entrevistados em relação às variáveis estudadas, bem como conhecer o significado que eles dão à gestão de documentos e à proteção de dados pessoais, bem como a relação destas duas. Ora, as entrevistas não foram realizadas dado o contexto sócio-político que se despoletou em Moçambique desde 2023 com as eleições autárquicas e que sofreu agravamento com as tensões políticas pós-eleitorais de 2024.

Pelas mesmas razões, o questionário previsto com perguntas abertas e fechadas, não foi aplicado. Através deste questionário seriam coletados dados através dos responsáveis pela gestão de documentos em Moçambique ao nível provincial³ (11 províncias), visto que essa população alvo não está agrupada geograficamente.

Importa referir que a não aplicação destas técnicas de coleta de dados acessórios, não colocaram em causa os resultados do trabalho de pesquisa uma vez que com a sua aplicação pretendia-se colher apenas a percepção dos potenciais entrevistados e inquiridos o que não alteraria a proposição das diretrizes arquivísticas fruto da pesquisa documental.

No que toca à parte descritiva, as pesquisas vão além da simples identificação da existência de relações entre variáveis, e pretendem determinar a natureza dessa relação. Elas também servem para proporcionar uma nova visão do problema (Gil, 2022). Assim, como pode ser visto pelos objetivos traçados, a “gestão de documentos” e a “proteção de dados pessoais” são as variáveis que identificamos ter uma relação indissociável, mas mais do que isso, apresentamos através desta tese, uma perspectiva diferente da problemática de proteção de dados pessoais que muito e mais é abordada (a perspectiva informática), colocando a problemática sob ótica da política arquivística nacional.

Vários são os métodos de pesquisa existentes, desde estudo de caso, metateórico, teoria fundamentada, análise de domínio, análise de discurso, análise de

³ Moçambique organiza-se territorialmente e administrativamente em províncias, distritos, postos administrativos, localidades e povoações, conforme o n.º 1 do artigo Artigo 7º da Constituição da República.

conteúdo, protocolo verbal etc. A presente tese reveste-se de estudo de caso como método de pesquisa.

Yin (2015) explica que quanto mais as questões de uma pesquisa procurarem explicar o “como” ou o “por quê”, o estudo de caso será mais indicado a adotar. Acrescenta o autor que, este método é indicado quando as questões de uma pesquisa demandarem uma ampla e aprofundada descrição da situação. Esses estudos de caso podem ser tanto estudos de caso único, assim como de múltiplos casos. Ora, para definir “estudo de caso”, Yin (2015) antes de o fazer, entende que apresentar uma definição não é tarefa fácil e nem consensual. Todavia, apresenta uma definição que reflete uma visão em duas partes dos estudos de caso. A primeira parte aponta que o

estudo de caso é uma investigação empírica que investiga um fenômeno contemporâneo em profundidade e em seu contexto de mundo real, especialmente quando os limites entre o fenômeno e o contexto puderem não ser claramente evidentes (Yin, 2025, p.17).

A segunda parte dá conta que o estudo de caso

enfrenta a situação tecnicamente diferenciada em que existirão muito mais variáveis de interesse do que pontos de dados, e, como resultado, conta com múltiplas fontes de evidência, com os dados precisando convergir de maneira triangular, e como outro resultado, beneficia-se do desenvolvimento anterior das proposições teóricas para orientar a coleta e a análise de dados (Yin, 2015, p.17).

Portanto, ao questionarmos (a) de que forma se estabelece a relação da proteção de dados pessoais com a gestão de documentos dentro do escopo de uma política arquivística no cenário moçambicano? (b) Os aspectos da gestão de documentos para a proteção de dados pessoais estão devidamente incorporados nas normativas moçambicanas atinentes à proteção de dados pessoais? (c) Como é tratada a proteção de dados pessoais na legislação moçambicana?”, já se adotava o método de estudo de caso para o desenvolvimento da pesquisa desta tese.

Como pode ser visto nas seções subsequentes, para além da própria problemática levantada, a discussão é atual e toda a mobilização teórica feita, apoio a coleta e análise de dados. O arcabouço teórico permitiu analisar e interpretar o cenário arquivístico moçambicano e a proposta de lei de proteção de dados pessoais.

Nesta tese, como fizemos referência, as entrevistas não foram realizadas, tendo sido adotadas a observação e a análise de documentos no estudo de caso

desenvolvido. E existem, como aponta Valentim (2005, p. 124), “diferentes métodos e técnicas aplicados à pesquisa científica na área de Ciência da Informação. A análise de conteúdo é uma delas”. Assim, para a realização desta pesquisa adotamos o método de análise de conteúdo.

Bardin (1977, p. 42) define análise de conteúdo como “um conjunto de técnicas de análise das comunicações visando obter indicadores que permitam a inferência de conhecimentos relativos às condições de produção/recepção destas mensagens”. Por outra, conforme Silva *et al.* (2005, p. 74) “método da análise de conteúdo aparece como uma ferramenta para a compreensão da construção de significado que os atores sociais exteriorizam no discurso”.

A análise de conteúdo é um método de tratamento e análise de informações consubstanciadas em um documento, colhidas por meio de técnicas de coleta de dados. Aplica-se à análise de textos escritos ou de qualquer comunicação traduzida a um texto ou documento. O seu objetivo é compreender o sentido das comunicações, seu conteúdo manifesto ou latente, as significações explícitas ou ocultas (Chizzotti, 2000). Portanto, nesta tese aplicamos análise de conteúdo, não para comunicações transcritas, como seria o caso das entrevistas. Aplicamos a análise de conteúdo para as normativas que analisamos e, muito particularmente, aplicamos este método na análise da proposta de lei de proteção de dados pessoais elaborada pelo Instituto Nacional de Tecnologias de Informação e Comunicação de Moçambique, procurando compreender e extrair desses textos legais, o sentido do seu conteúdo, sobretudo os alinhamentos entre a gestão de documentos e a proteção de dados pessoais.

A análise de conteúdo possui duas funções, que na prática podem ou não se dissociar: uma função heurística (onde ela enriquece a tentativa exploratória, aumenta a propensão à descoberta), e; uma função de administração da prova (verificação de uma confirmação ou de uma infirmação de hipóteses). Ora, as duas funções da análise de conteúdo podem coexistir de maneira complementar (Bardin, 1977). De fato, na presente tese elas coexistem. Por um lado, o contato com a temática e com as normativas de proteção de dados pessoais de Moçambique, do Brasil e do Mundo, bem como com os textos bibliográficos sobre a gestão de documentos, a política arquivística e a própria proteção de dados pessoais, nos possibilitou o estabelecimento da relação indissociável entre gestão de documentos e a proteção

de dados pessoais. Por outro lado, a análise de conteúdo nos permitiu verificar e/ou confirmar a hipótese colocada no início da pesquisa.

Bardin (1977) aponta três etapas da análise de conteúdo: a pré-análise (seleção do material e definição dos procedimentos a serem seguidos); a exploração do material, e; o tratamento dos resultados, a inferência e a interpretação. A figura 1 mostra estas etapas ou fases na realização desta tese.

Figura 1 – Etapas da aplicação da análise de conteúdo



Fonte: Elaborado pela autora.

Portanto, ao utilizarmos este método no desenvolvimento desta tese, seguimos estas etapas, onde num primeiro momento fizemos o mapeamento de onde encontrar, física ou digitalmente, o material necessário para a pesquisa, isto é, a legislação (ver Apêndice A) e a Proposta de Lei de Proteção de Dados Pessoais⁴ (ver Anexo A), fizemos o levantamento documental, com destaque para o trabalho realizado na Biblioteca da Assembleia da República com vista a identificar a existência (em discussão ou não) de uma proposta ou projeto de lei de proteção de dados pessoais naquela instância (ver Apêndice B), e definimos como procederíamos para explorar o material identificado e selecionado. No segundo momento, analisamos as normativas de gestão de documentos e conexas à proteção de dados pessoais, bem como analisamos a proposta de lei de proteção de dados pessoais. Por último, resultante da análise realizada, apresentamos os resultados e a interpretação que é feita deles, tendo em conta, não só os objetivos, mas também o quadro teórico elaborado.

⁴ Versão de 2024, datada de 26 de abril, consultada aos 20 de abril de 2025.

Ora, Marconi e Lakatos (2023, 202) definem a técnica como “um conjunto de procedimentos de que se serve uma ciência ou arte; é a habilidade para usar esses preceitos ou normas. Toda ciência utiliza inúmeras técnicas na obtenção de seus propósitos”. Estas técnicas podem ser, como estamos a ver aqui, de coleta de dados, mas também como veremos mais adiante, de análise de dados. Para a consecução do nosso trabalho de pesquisa, utilizamos a revisão de literatura e a observação indireta.

Segundo Severino (2017) a revisão de literatura é o processo necessário para poder se avaliar o que já foi produzido sobre o assunto e daí situar a contribuição que a pesquisa projetada pode dar ao conhecimento do objeto a ser pesquisado. Aliás, “pesquisa alguma parte da estaca zero” (Marconi; Lakatos, 2021, p. 257). Uma procura de fontes bibliográficas, torna-se indispensável para que não haja duplicação de esforços (Marconi; Lakatos, 2021), de tal forma que, nas teses e dissertações um capítulo ou seção é dedicado à revisão bibliográfica, “elaborada com o propósito de fornecer fundamentação teórica ao trabalho, bem como a identificação do estágio atual do conhecimento referente ao tema” (Gil, 2022, p. 44).

Gil (2022) considera que na revisão de literatura o que interessa é contextualizar teoricamente o problema e apresentar o estágio atual de conhecimento acerca da questão. Este exercício, implica segundo o autor, para além da apresentação das contribuições das investigações já realizadas, o esclarecimento dos pressupostos teóricos que dão fundamentação à pesquisa a ser realizada.

A fundamentação teórica do nosso trabalho de pesquisa está na noção de Política Arquivística Nacional, vista na perspectiva de uma política pública (*policy*) e a partir da qual se visualiza a gestão de documentos. Também se apoia na noção de proteção de dados pessoais, importada do Direito. É na gestão de documentos que buscamos os argumentos de que a proteção de dados pessoais se constitui em uma questão, antes de mais, arquivística.

Para a revisão de literatura nos servimos de fontes bibliográficas, em formato físico e eletrônico, localizadas nas bibliotecas física da Universidade Estadual Paulista-Campus de Marília e na Biblioteca Brazão Mazula da Universidade Eduardo Mondlane (Moçambique) para além de obras impressas disponíveis no acervo particular da autora. Diferentes bibliotecas virtuais serviram de fonte para esta tese,

com particular destaque para a Rede de Bibliotecas UNESP que tem disponibilizado coleções de *e-books* adquiridos ou assinados pela Unesp. Foram utilizados livros, teses, dissertações, periódicos científicos, anais de encontros científicos, obras de referência, entre outros. Na internet, foram utilizadas as bases de dados *Scientific Electronic Library Online* (SciELO), Base de dados de Periódicos em Ciência da Informação (Brapci), *Web of Science* e Scopus.

No que respeita a observação, vale dizer que “é uma técnica de coleta de dados para conseguir informações que utiliza os sentidos na obtenção de determinados aspectos da realidade. Não consiste apenas em ver e ouvir, mas também em examinar fatos ou fenômenos que se deseja estudar.” (Marconi; Lakatos, 2021, p. 221). Ela pode ser não estruturada ou assistemática, também designada espontânea, livre etc. Esta técnica de observação “consiste em recolher e registrar os fatos da realidade sem que o pesquisador utilize meios técnicos especiais ou precise fazer perguntas diretas [...] e não tem planejamento e controle previamente elaborados” (Marconi; Lakatos, 2021, p. 222).

A observação pode ainda ser não participante, onde, apesar de o pesquisador tomar contato com a comunidade, grupo ou realidade estudada, ele “não se integra a ela: permanece de fora. Presencia o fato, mas não participa dele; [...] faz mais o papel de espectador [...]” (Marconi; Lakatos, 2021, p. 223).

Na nossa dimensão de pesquisadora moçambicana, residente em Moçambique e estudando sobre Moçambique, tomaremos a observação indireta não estruturada e não participante como mais uma técnica de coleta de dados. Deste modo, não foi elaborado algum instrumento de observação, pois esta foi espontânea ou acidental, através da qual tomaremos contato ou presenciaremos os fatos em Moçambique, mas fizemos o papel de espectadores. Ademais, a observação indireta apoia-se, entre outros, em consultas bibliográficas e documentais, que fazem parte dos nossos procedimentos metodológicos.

Não só para fazer a coleta de dados que os pesquisadores se servem de técnicas, para a análise desses dados coletados e/ou a coletar, os pesquisadores também utilizam técnicas. Existe uma vasta gama delas. Ora, a escolha por uma(s) ou outra(s) está ou deve estar alinhada aos objetivos previamente traçados. Assim, atendendo o método de pesquisa identificado para o desenvolvimento desta tese, bem

como os objetivos delimitados, nós utilizamos a técnica de análise de conteúdo categorial.

Entre as técnicas utilizadas para a realização da análise de conteúdo destaca-se a análise léxica e a análise categorial (Valentim, 2005), mas a análise de conteúdo pode privilegiar também outras técnicas como análise da enunciação ou análise de conotações (Chizzotti, 2000). Ora, a técnica utilizada por nós é a análise categorial, sendo aquela que classifica o conteúdo do texto em categorias. Isto é, a “análise de conteúdo categorial, é uma técnica de pesquisa que permite a criação de inferências sobre determinado conteúdo, por meio de codificação do conteúdo, fazendo a aplicação de códigos, que vão formar categorias” (Sampaio; Lycarião, 2021, p. 45).

A categorização é uma operação de classificação de elementos constitutivos de um conjunto, por diferenciação e, em seguida, por reagrupamento segundo o género, com os critérios previamente definidos. As categorias, são rubricas ou classes, as quais reúnem um grupo de elementos (unidades de registo) sob um título genérico. Esse agrupamento é efetuado em razão dos caracteres comuns destes elementos. Portanto, “a categorização tem como primeiro objetivo fornecer, por condensação, uma representação simplificada dos dados brutos” (Bardin, 1977, p. 119).

O critério de categorização pode ser semântico (categorias temáticas), sintático (os verbos, os adjetivos), léxico (classificação das palavras segundo o seu sentido, com emparelhamento dos sinónimos e dos sentidos próximos) e expressivo (por exemplo, categorias que classificam as diversas perturbações da linguagem) (id.) A categorização que fizemos é semântica apontando as categorias de temas concernentes à gestão de documentos e à proteção de dados pessoais.

Tendo em conta a técnica utilizada para analisar os dados coletados no decurso desta pesquisa, enquanto instrumento para torná-la exequível, utilizamos o sistema de categoria *a posteriori*. Bardin (1977) indica que a categorização pode empregar dois processos inversos. Um em que é fornecido o sistema de categorias e repartem-se da melhor maneira possível os elementos, à medida que vão sendo encontrados. Outro em que o sistema de categorias não é fornecido, antes resultando da classificação analógica e progressiva dos elementos. Sendo chamados, procedimento por “caixas” e procedimento por “milha”, respectivamente (Bardin, 1977, p. 119).

Atendendo a nossa opção metodológica, o título conceptual de cada categoria componente do nosso sistema de categorias foi definido somente no final da operação de classificação. O quadro 1 que segue, ilustra a aplicação da análise de conteúdo e sua técnica de análise categorial temática *à posteriori* nesta tese.

Quadro 1 – Aplicação da análise de conteúdo

	Código	Presente	Ausente	Parcialmente Presente ou Ausente
Categoria I: Política Arquivística Nacional	Legislação arquivística	X		
	Lei de Direito a Informação	X		
	Conselho Nacional de Arquivos			X
	Infraestrutura tecnológica			X
	Graduação em Arquivologia	X		
	Associação de arquivistas		X	
Categoria II: Sistema Nacional de Arquivos	Arquivo Nacional	X		
	Arquivos Públicos Provinciais		X	
	Arquivos Públicos Distritais		X	
Categoria III: Gestão de documentos	Plano de Classificação	X		
	Tabela de Temporalidade	X		
	Classificador de informação	X		
Categoria IV: Lei de Proteção de Dados Pessoais	Proposta/Projeto de Lei	X		
	Legislação conexa	X		
	Princípios de Proteção de dados pessoais	X		
	Princípios e funções arquivísticas			X
	Atores arquivísticos		X	

Fonte: Elaborado pela autora.

As inferências decorrentes da aplicação da análise de conteúdo estão patentes, com maior incidência, na quinta e oitava seção desta tese. Contudo, um pouco por todas outras seções deste trabalho, são apresentados dados resultantes de um exercício de análise de conteúdo, em termos mais gerais.

Apresentados os procedimentos metodológicos adotados para o desenvolvimento desta tese e antes de passarmos para a parte central, vale discorrer, de forma breve, sobre a estrutura deste trabalho. Neste sentido, a primeira seção é a presente INTRODUÇÃO onde são apresentados o problema de pesquisa e perguntas

de partida; a hipótese; os objetivos; a justificativa; e, os procedimentos metodológicos que acabamos de apresentar acima.

As bases conceituais que sustentam esta tese são apresentadas ao longo de três seções, da segunda à quarta. Portanto, na segunda seção, DOS DADOS AOS DOCUMENTOS DE ARQUIVO, encontra-se a discussão dos conceitos de dado, informação, com a sua ramificação para dados pessoais vs informação pessoal, e, documento, com desdobramento para documento de arquivo. Na seção três, DA GESTÃO DE DOCUMENTOS E POLÍTICA ARQUIVÍSTICA À PROTEÇÃO DE DADOS PESSOAIS, residem as discussões sobre gestão de documentos, política arquivística, desdobrando-se em sistema nacional de arquivo, e, proteção de dados pessoais. A terceira seção de bases conceituais, corresponde à seção quatro desta tese. A seção é intitulada A PROTEÇÃO DE DADOS PESSOAIS DESDE UMA PERSPECTIVA ARQUIVÍSTICA e nela é revisitada a definição de a Arquivologia, seus principais princípios e teoria, passando pela definição de arquivista (identificando o seu papel na/para a proteção de dados pessoais) junto dos aspectos da ética profissional.

A quinta seção, A ARENA ARQUIVÍSTICA MOÇAMBICANA, apresenta e analisa o cenário arquivístico de Moçambique. Começa com uma ilustração da estrutura político-administrativa daquele país na subseção Moçambique: da estrutura administrativa em direção à estrutura arquivística, de seguida é apresentado o histórico dos ditos sistema nacional de arquivos de Estado. Uma subseção é dedicada a apresentar o projeto de Sistema Nacional de Gestão Documental (e-SNGD). As primeiras subseções desta seção permitiram a identificação dos principais atores da arena arquivística moçambicana. Na subseção final desta seção, O arquivista moçambicano face à proteção de dados pessoais, buscamos conhecer o arquivista moçambicano, desde a sua formação à sua atuação profissional.

Na sexta seção, PANORAMA INTERNACIONAL E BRASILEIRO DA PROTEÇÃO DE DADOS PESSOAIS, faz-se o mapeamento legal atinente à proteção de dados pessoais desde a legislação internacional (exceto Moçambique), passando pela legislação brasileira e finalizando com um olhar geral à proteção de dados pessoais em África.

A legislação moçambicana que foi exceção na seção anterior, ela é identificada e analisada na sétima seção, O QUADRO LEGAL MOÇAMBICANO DA PROTEÇÃO DE DADOS PESSOAIS. Para além deste levantamento legal que é feito nesta seção, nela também são identificados, justamente através da legislação, os Principais atores do cenário de proteção de dados pessoais em Moçambique.

A tese tem a seção oito, PELA PROTEÇÃO DE DADOS PESSOAIS CONSENTÂNEA COM POLÍTICA ARQUIVÍSTICA EM MOÇAMBIQUE, reservada para analisar, sub ótica arquivística, a Proposta de Lei de Proteção de Dados Pessoais de 2024 apresentada pelo Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC). Depois da análise, são apresentadas diretrizes para a elaboração de normativas de proteção de dados pessoais consentâneas com a gestão de documentos. Essas diretrizes partem da elaboração e formalização de política arquivística nacional em Moçambique, enquanto diretriz primeira e que fornece condições para a revisão do sistema nacional de arquivos consubstanciando-se em diretriz segunda e a diretriz terceira, a institucionalização da gestão de documentos.

Por fim, apresentamos as nossas CONSIDERAÇÕES FINAIS, conjugando todo o exercício feito, desde a identificação do problema até a proposição de diretrizes arquivísticas para a elaboração de normativas de proteção de dados pessoais.

2 DOS DADOS AOS DOCUMENTOS DE ARQUIVO

Nesta seção em específico, nos debruçamos sobre os conceitos de dados e de informação, buscando compreender os dados pessoais *vis-à-vis* da informação pessoal. O conceito de documento é discutido orientando-se a discussão para o conceito de documento de arquivo, do qual procurou-se conhecer suas características.

2.1 Dado

Buckland (1991) ao falar de tipos de informação em seu clássico *Information as thing*, considera o termo “dado” como sendo um termo adequado para designar informação como coisa ou objeto e que foi processada de alguma forma para uso. Ele entende que, normalmente, denota quaisquer registros armazenados em um computador. De primeira, essa definição pode causar algum ruído para compreensão, sobretudo se tomada em consideração a acepção popular de dados como qualquer sinal, elemento, coisa, signo, não processada, nem interpretada. Contudo, num segundo momento compreende-se, o que vamos chamar de grau de processamento desse dado, apontado por Buckland: um grau de processamento bastante diminuto que não o faz atingir a qualidade de informação. Ou como prefere Semidão (2014, p. 71) “dado figura como fato ou átomo, um elemento bruto, desprovido de significação imediata. Algo perceptível e de baixo teor semântico”.

Para Alves *et al.* (1993, p. 30), dado é “representação de factos, conceitos ou instruções, de um modo convencional e adequado à comunicação, interpretação ou tratamento por meios humanos ou automáticos”. Essa possibilidade de tratamento ou processamento por máquinas ou por Homens está presente em várias definições de dado.

O Arquivo Nacional (2005) define dado como a representação de todo e qualquer elemento de conteúdo cognitivo, que pode ser comunicada, processada e interpretada manualmente ou automaticamente. Dois anos antes desta definição, Amaral (2003) havia definido dado, também como uma representação, mas no seu caso é uma “representação mínima de todo e qualquer elemento de carácter cognitivo,

passível de ser transferido, processado e interpretado de forma manual ou automática” (Amaral, 2003, p. 47).

O *Multilingual Archival Terminology Database* (s.d.) do Conselho Internacional de Arquivos, para além de apresentar uma definição semelhante à do Arquivo Nacional que vimos acima, também toma dado como a menor unidade de informação dotada de significado. É preciso distinguir a ideia de unidade de informação que se faz alusão aqui, da unidade de informação, como serviço ou instituição (a ideia de instituição arquivística, especificamente, arquivo nacional, arquivos públicos provinciais, como unidades de informação, estão presentes nesta tese desembocada das lógicas de política arquivística nacional e sistema nacional de arquivos).

Cunha e Cavalcanti (2008) no Dicionário de Biblioteconomia e Arquivologia, não só consideram a qualidade de representante e a possibilidade de ser comunicado, interpretado, tratado ou processado por humanos (manual) ou por máquinas (automático) que o dado tem, abrem um pouco mais o sentido de dado apontando que abarca toda informação quantificável como números, letras, imagens, sons ou a combinação destes. Avançam concebendo dados como “blocos construtivos da informação” (Cunha; Cavalcanti, 2008, p. 113), como conjunto de caracteres alfabéticos, numéricos, alfanuméricos ou outros, que representam uma condição ou valor específico.

Capurro e Hjørland (2007) avançaram que quando os dados são representados em sistemas de informação, é com o propósito de dar suporte à determinadas atividades do Homem, envolvendo aspectos teóricos, sociais, históricos etc.). Nesta senda, dado faz parte do cotidiano dos arquivistas. O dado pode ser definido como “[...] a mais pequena representação convencional e fundamental de uma informação sob forma analógica ou digital, que permita efetuar o seu tratamento manual ou informático” (Rousseau; Couture, 1998, p. 137).

Neste contexto, é importante levantar aqui o conceito de metadados. Grácio (2002), faz lembrar como de forma comum, os metadados são tidos como “dados sobre dados” (Grácio, 2002, p.21). Ao mesmo tempo, o autor chama atenção para o fato dos metadados poderem ser melhor descritos como um conjunto de dados chamados de elementos, que pode variar em número conforme o padrão, e eles elementos descrevem o conteúdo de um recurso, dando a possibilidade de busca,

recuperação e acesso ao recurso descrito. Nesta senda, Grácio percebe “metadados possui um conceito de acordo com o profissional e a área em que é utilizado, mas tem sempre como objetivo principal a descrição da informação para sua busca e recuperação” (Grácio, 2002 p.21). O autor define metadados como

Conjunto de elementos que descrevem as informações contidas em um recurso, com o objetivo de possibilitar sua busca e recuperação. O conjunto de elementos ou o conjunto semântico de campos representa o conteúdo do recurso descrito, ou seja, as informações que possibilitam identificar o que o recurso representa e o que ele contém. Esse conjunto pode ter um número de elementos variável de acordo com o padrão de metadados utilizado. Os elementos devem conter dois tipos de informações: - descritivas, ou seja, aquelas referentes às características explícitas do recurso, tais como título, data, formato, tipo etc; - e temáticas, de conteúdo intelectual, ou seja, aquelas que expressam o conteúdo do recurso, tais como palavras-chave e referências cruzadas (Grácio, 2002 p.23)

De acordo com Machado (2023), metadados são um conjunto de dados que descreve e dá informações sobre outros dados. O seu uso é visto como uma solução para descrição e representação de objetos digitais em ambientes informacionais (Machado, 2023, p.7) Portanto, metadados podem ser utilizados para representar vários recursos, dependendo do domínio: em um provedor Web, para identificar e localizar páginas na Internet; na digitalização de imagens, para descrever a informação contida nelas; em dados eletrônicos, para descrever a informação contextual contida no documento eletrônico (Grácio, 2012, p.122).

Santos e Flores (2016) entendem, que a inserção de metadados é essencial para o cumprimento das funções arquivísticas, desde o momento da produção e/ou da aquisição de documentos arquivísticos digitais. Os autores percebem que os metadados auxiliam a classificação, a avaliação, a preservação digital, em particular, e a difusão. Adicionar dados pertinentes às estruturas de metadados é uma atividade de descrição que se relaciona com todo o ciclo de vida dos documentos, e que exerce uma tarefa vital em qualquer acervo digital.

Portanto, diante das definições acima, neste trabalho toma-se o dado nas suas diversas facetas, como unidade de trabalho do arquivista, como elemento que dá suporte à determinadas atividades dos seres humanos, como elemento comunicável e/ou interpretável de forma manual ou de forma automática ou informática, como

grupo de caracteres alfanuméricos ou simplesmente alfabéticos ou numéricos etc., vislumbrando-se aqui os dados pessoais que definiremos mais adiante.

2.2 Informação

A informação é relacionada, de forma analógica, à documentos impressos, quando de fato a informação de que trata a Ciência da Informação (CI), tanto pode estar num diálogo entre cientistas, em comunicação informal, numa fotografia ou objeto, no registro magnético de uma base de dados, na Internet, etc. Embora os campos do saber se nutrem de informação, poucos a tomam por objeto de estudo como o faz a CI (Pinheiro, 2004).

No campo da CI, destaca-se o posicionamento de Buckland (1991) ao distinguir três significados de “informação”. “Informação como processo”; “informação como conhecimento”; e “informação como coisa”. Parte da noção de “informação como coisa” foi abordada no tópico anterior. Portanto, para Buckland, que recorreu ao *Oxford English Dictionary* de 1989, “informação como coisa” é usado de forma atributiva para objetos, como dados e documentos, que são chamados de “informação” porque são considerados informativos, ou ainda, como aqueles objetos que têm a qualidade de transmitir conhecimento ou comunicar informações. Buckland (1991) acrescenta que a informação como coisa é de especial interesse em relação aos sistemas de informação porque eles podem lidar diretamente com as informações somente nesse sentido.

Buckland (1991) vai mais longe ao distinguir “informação como conhecimento” (intangíveis) e “informação como coisa” (tangíveis). Conforme o autor, o conhecimento pode ser representado, assim como um evento pode ser filmado. Contudo, a representação não é mais conhecimento e nem filme é o evento. Qualquer representação desse tipo está necessariamente em uma forma tangível (sinal, dados, texto, filme, etc.) e, portanto, são necessariamente “informação como coisa”.

Ainda no texto que estamos a citar, Buckland esmerou-se sobre “tipos de informação”, como fizemos referência mais acima, para indicar com mais

especificidade os tipos de “coisas” a incluir quando se fala de “*information as thing*”. Ele aponta dados; texto e documentos; e, objetos. Vamos destacar aqui, “dados” e “texto e documentos”. Sobre o primeiro já discorremos acima e sobre o segundo, trabalharemos mais à baixo.

Por sua vez, Heredia Herrera (1991, p. 128) fala de “Informações brutas” e “informações processadas”. Para ela, as informações brutas contidas nos documentos podem ser: intensiva, quando oferece muitos dados sobre algo ou algumas pessoas, como arquivos pessoais, provas, listas de méritos e serviços; extensiva, quando há poucos dados sobre um grande número de pessoas ou coisas, por exemplo, cadernos eleitorais, listas eleitorais, e; diversificada, quando a informação contém uma variedade de dados sobre diferentes assuntos, como correspondência, documentos legislativos.

Ora, Pinheiro (2004), assim como Capurro e Hjørland (2007), apontam que quase toda disciplina científica usa o conceito de informação dentro de seu próprio contexto e com relação à fenômenos específicos. Eles recorreram à vários autores, desde filósofos à cientistas, para compreender a “informação”. Através de Mahler, compreendem que “a informação não é um elemento observável puro, mas um construto teórico. É um “dato interpretado” (Capurro; Hjørland, 2007, p. 164).

Os autores também, e diante de uma multiplicidade de perspectivas de “informação”, apontam ser importante questionar “que diferença faz se usarmos uma ou outra teoria ou conceito de informação?”. Ainda assim, percebem haver duas distinções: informação como coisa (retomando Buckland, 1991) e informação como signo, que depende da interpretação de um agente cognitivo (Capurro; Hjørland, 2007).

Duas distinções também são percebidas por Lesca e Lesca (2010). Informação como processo e informação como o resultado de um processo. A primeira refere-se à uma sucessão de ações pelas quais se informa. Segundo os autores, a circulação da informação, o acesso à informação, ilustram esta perspectiva. A segunda, conforme os autores apontam, refere-se, de algum modo, a um objeto. Nesta ótica se aborda o volume de informação, variedade de informação, sobrecarga de informação, entre outros.

Cunha e Cavalcanti (2008) arrolam várias definições de informação. Eles vêm a informação como “registro de um conhecimento que pode ser necessário a uma decisão”; “uma prova que sustenta ou apoia um fato”; “registro de um conhecimento para utilização posterior”; “dados numéricos, alfabéticos ou alfanuméricos processados por computador”, “elemento referencial, noção, ideia ou mensagem contidos num documento” (Cunha; Cavalcanti, 2008, p. 201).

Conforme Silva (2012), na CI, a noção de informação participa quase sempre de dois tipos de acepção. Uma é a de autonomia do conteúdo em relação à forma, de maneiras que a informação é entendida como o conteúdo, ou partes do conteúdo de um documento, que pode ser transportada, sem prejuízo, de uma forma a outra. A segunda acepção apregoa que a informação, enquanto significação de um sujeito, não existe em si mesma, mas só para um sujeito do conhecimento, em sua interpretação. Estas duas concepções de informação aceitam a materialidade do documento e a imaterialidade da informação.

Ao falarmos das diferentes definições de informação, e dado ao balanço em que este trabalho se posiciona, entre o acesso e o inaccess, é oportuno pontuarmos aqui, ainda que de forma breve, os conceitos de Direito à informação e acesso à informação. É comum nos depararmos com situações em que estes termos são usados indiscriminadamente e como sinônimos, mas eles não são, embora tenham relação quase que indissociável. Uma definição de Direito à informação é apresentada por Alves *et al.* (1993) como sendo o

“reconhecimento legal de que a ninguém pode ser negado o acesso, livre e gratuito, aos documentos, dados ou informações que lhe digam diretamente respeito, assim como, de um modo mais geral, a todos os documentos que não estejam abrangidos por qualquer restrição de comunicabilidade” (Alves et al, 1993, p. 34).

Martins (2012) aponta que este conceito é vital para um governo aberto, que propõe processos e procedimentos pautados na transparência. Esse é um direito essencial e estratégico para a realização de muitos outros direitos humanos e impõe duas obrigações sobre os governos: obrigação de publicar e disseminar informações essenciais sobre o que estão fazendo, e, a obrigação de responder a pedidos de informação que receber do público.

Ora, o Direito a informação, como estamos a constatar, é, regra geral o caminho para se dar o acesso a informação, e aqui reside a distinção. Enquanto o primeiro diz

respeito a norma, ao aspecto legal, o segundo diz respeito a efetivação, na prática, deste direito. Portanto, o acesso a informação vai ser atravessado por questões, em primeira instância, legais, mas também por aspectos técnico-tecnológicos, materiais, humanos e culturais. Estamos a dizer que, num determinado ordenamento jurídico, por exemplo, o Direito a informação pode estar consagrado na constituição desse país (para além de ser um direito humano), mas esse Estado pode não ter criado as condições para que os cidadãos do tal país gozem do direito que têm. Seja porque o Estado diz-se democrático, mas efetivamente não o é, seja por uma cultura de secretismo, seja por uma infraestrutura de informação precária.

A definição de Alves *et al.* (1993) deixa nas entrelinhas o fato de que as pessoas têm direito à informação sobre os seus próprios dados e/ou informação pessoal, desde as razões para a sua coleta ou registro, seu tratamento, seu compartilhamento, sua eliminação, entre demais ações que incidam sobre os seus dados pessoais. Assim, passamos a seguir, a revisitar a noção de dados e/ou informação pessoal.

2.2.1 Dados pessoais vs informação pessoal

É recorrente, em diferentes situações, dados pessoais e informação pessoal serem tomados como sinónimos. Depois do exposto acima, onde discutimos os conceitos de “dados” e de “informação”, podemos sem dúvidas afirmar que, rigorosamente, ao nos referirmos à dados, o nível de significação e/ou mesmo de granularidade ou ainda, o grau do teor semântico, é diferente de informação.

Aliás, Doneda (2011) apontou este imbróglio em relação à utilização dos termos dado e informação e especificou que ambos os termos servem para representar um fato, determinado aspecto de uma realidade, mas que cada um carrega um peso particular. A informação pessoal está, segundo o autor, ligada à privacidade na medida em que um maior grau de privacidade significa uma menor difusão de informações pessoais e vice-versa. Doneda (2011) avança e aponta que determinada informação pode possuir um vínculo objetivo com uma pessoa e revelar alguma coisa sobre esta pessoa, o que significa que tal informação faz referência às características ou ações da referida pessoa, ou tal informação pode provir de seus atos. Doneda ainda sublinha a importância de se estabelecer esse vínculo objetivo, pois assim

afastam-se outras categorias de informações que não seriam, de fato, informações pessoais.

No dicionário que temos estado a citar, da autoria de Cunha e Cavalcanti (2008), “dados pessoais” é tido como registro ou informação sobre um indivíduo, armazenado em base de dados ou sistema informático. Compreendendo por exemplo a identidade, o estado civil, dados de natureza financeira, médica etc.

A Internet Society tem um glossário de termos da internet. Nele, o termo “dados pessoais” diz respeito a qualquer informação que, quando reunida, possa ser usada para identificar uma pessoa específica (Internet Society, s.d.). Esta definição parece apontar para alguma necessidade de processamento para possibilitar a identificação da pessoa.

Do Regulamento Geral sobre a Proteção de Dados, doravante RGPD, lê-se em seu Artigo 4º que

Dados pessoais: qualquer informação relativa à uma pessoa física identificada ou identificável (titular dos dados); uma pessoa física identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador on-line ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa física (RGPD, 2016, artigo 4º).

Garcia (2018) faz uma síntese apontando que dados pessoais seriam todas as informações codificadas de determinada pessoa e que o tratamento desses dados gera uma informação pessoal. Garcia (2018) dá exemplo de dados pessoais como endereço, número de telefone fixo, número de celular, data de nascimento, cadastro de pessoa física (CPF), título de eleitor, passaporte, carteira de trabalho, nome de familiares, cidade natal, dados bancários, contatos de e-mails, fotografias e vídeos, endereço de *Internet Protocol (IP)*, entre outros dados pessoais.

Diante do exposto, podemos considerar que, os dados pessoais são elementos numéricos, alfabéticos ou alfanuméricos, como um nome, um número de identificação, CPF, através dos quais, tendo sido tratados e/ou processados manualmente ou automaticamente, é possível identificar uma pessoa específica. Assim, a partir do momento que se tem identificada a pessoa, se está diante da informação pessoal. Estes dados e/ou informações pessoais podem ser encontrados em documentos de variada tipologia. A seguir vamos nos debruçar sobre o conceito de documento.

2.3 Documento

Ao discorrermos sobre o texto de Buckland (1991) mais acima, indicamos que revisitaríamos a dimensão de “*information as thing*” que envolve os documentos. Assim, enquanto “coisa” ou “objeto”, Buckland (1991) entende que “documento” é normalmente usado para designar textos ou, mais exatamente, objetos que contêm textos e incluem, imagens e sons. Os textos podem ser as cartas, formulários, livros, periódicos, manuscritos e registros escritos de vários tipos, em papel, microformas e em formato eletrônico. Nesse sentido, uma tabela de números pode ser considerada como texto, como documento ou como dados.

Alves *et al.* (1993) apresentaram uma definição bastante analógica de documento como sendo uma “unidade constituída pela informação e respetivo suporte” (Alves *et al.*, 1993, p. 36). Paes não foge muito desta definição apontando documento como o “registro de uma informação independentemente da natureza do suporte que a contém” (Paes, 2004, p. 26). Na mesma senda seguiu o Arquivo Nacional (2005) definindo documento como unidade de registro de informações, qualquer que seja o suporte ou formato. Destas definições podemos inferir que elas acomodam as perspectivas tradicionais e eletrônicas do documento.

Em um sentido mais amplo e genérico, aponta Heredia Herrera (1999), documento é “qualquer registro de informação, independentemente de seu meio físico”, quer dizer, “engloba tudo o que pode transmitir conhecimento humano” (Heredia Herrera, 1999, p. 121).

Amaral (2003, p. 52) define documento como “qualquer suporte que contenha informação registada, formando uma unidade, que possa servir para consulta, estudo ou prova” e indica que “inclui impressos, manuscritos, registos audiovisuais, imagens, entre outros”. O mesmo exercício de indicar o que engloba o “documento”, Bellotto fez. A autora remonta à conceituação clássica e genérica, definindo que “documento é qualquer elemento gráfico, iconográfico, plástico ou fônico, pelo qual o Homem se expressa. É o livro, o artigo de revista, o relatório, a carta, a legislação, a fotografia, o disco, etc.” (Bellotto, 2006, p. 35).

Os documentos para além de se apresentarem em diferentes gêneros, eles podem ser analógicos (como já se fez indicação acima), eletrônicos e/ou digitais. Tem

sido comum se referir ao documento eletrônico como digital, usando os termos como sinônimos, mas tecnicamente são distintos. Podemos dizer de forma simplificada que, todo o documento digital é eletrônico, mas nem todo documento eletrônico é digital, de tal modo que há documentos eletrônicos que são digitais e outros que são analógicos.

Duranti (2009) define documento digital como um componente digital, ou grupo de componentes digitais, que são guardados, tratados e geridos como um documento, ou seja, o conteúdo e forma são codificados utilizando valores numéricos (valores binários 0 e 1) em vez de um espectro contínuo de valores como os gerados por um sistema analógico. Para a autora, documento analógico é a representação de um objeto ou processo físico através da utilização de sinais eletrônicos continuamente variáveis ou padrões mecânicos. Ela entende documento eletrônico como qualquer documento analógico ou digital que é transportado por um condutor elétrico e requer o uso de equipamento eletrônico para ser inteligível por uma pessoa.

Parece que atento a estes aspectos, Rabello (2019, p.20) conclui que o documento “se constitui como um produto de ações e práticas sociais, sendo definido, especificamente, por distintas institucionalidades da informação as quais têm o acesso e as condições de atuação condicionadas pela materialidade em diferentes perspectivas.

Bellotto vinca que documento é “tudo o que seja produzido por motivos funcionais, jurídicos, científicos, técnicos, culturais ou artísticos, pela atividade humana” (Bellotto, 2006, p. 35). A autora ainda esclarece que “é a razão de sua origem e de seu emprego, e não o suporte sobre o qual está constituído, que vai determinar a sua condição de documento de arquivo, de biblioteca, de centro de documentação ou de museu” (Bellotto, 2006, p. 36). No âmbito desta tese, interessa-nos discutir o documento de arquivo, como o fazemos a seguir.

2.3.1 Documento de arquivo

Antes de falarmos de documentos de arquivo, é importante revisitarmos o conceito de “arquivo”. Ao retomarem à origem da palavra “arquivo”, Rousseau e Couture (1998) compreendem que, através do termo em grego “*archeion*”, fica patente

que o arquivo (em singular ou plural) refere-se à atividade administrativa e faz parte de todas as épocas, regendo as relações entre os governos, as organizações e as pessoas singulares.

Silva (2012) percebeu também que a noção de “arquivo” tem sido sinónimo de lugares, bem como de documentos. Lugares em que são preservados registros de importância histórica, gerencial e informacional. Conjuntos de documentos marcados pelas ações que os fizeram existir enquanto instrumento dos atos administrativos, mantidos no presente pela intenção de preservação, para testemunhar o passado em termos de usos previstos (Silva, 2012).

Nesta ótica de arquivo enquanto conjunto de documentos, Heredia Herrera (1991) define arquivo como

um ou mais conjuntos de documentos, qualquer que seja seu registro, forma e suporte material, acumulados em um processo natural por uma pessoa ou instituição pública ou privada no curso de sua gestão, preservados, respeitando essa ordem, para servir como testemunho e informação para a pessoa ou instituição que os produz, para os cidadãos ou para servir como fontes de história (Heredia Herrera, 1991, p. 89, tradução nossa).

Atento à polissemia do termo “arquivo”, Silva (2012) detalha que o conceito de arquivo, enquanto o lugar que preserva e os registros preservados, contempla três noções. A noção de conjuntos de documentos, elevados no presente, à categoria de bens culturais, que são preservados por seu valor alicerçado na visão histórica. Contempla a noção de serviço técnico dentro das instituições, que contam com lugares em que os documentos são gerenciados. E contempla a noção de sistemas de recuperação de informação (Silva, 2012).

No RGPD embora não seja definido o termo, a noção de “arquivo” utilizada é aquela para se referir a todos os documentos criados e recebidos por uma pessoa, família ou organização, pública ou privada, na condução de seus negócios, e selecionados para preservação permanente (Comissão Europeia, s.d.). Se ignorarmos a importância dos dados pessoais e sua proteção no contexto dos arquivos permanentes, neste trabalho o acento tônico é colocado nos arquivos corrente e intermediário. Sobre estas idades ou estágios de evolução, abordaremos mais adiante.

Achamos oportuno, antes de falarmos de “documento de arquivo”, mobilizarmos Paes (2004) com sua classificação dos arquivos. A autora classifica os

arquivos segundo diferentes critérios, a saber: entidade mantenedora; estágio de evolução; extensão da sua atuação; e, natureza dos documentos. Portanto, quanto à entidade mantenedora, os arquivos podem ser públicos (Federal/nacional; estadual; regional; provincial; municipal ou distrital); arquivos pessoais; etc. Quanto ao estágio de evolução, a autora faz corresponder à teoria das três idades (que abordaremos mais adiante), corrente, intermediária e permanente. No que toca à extensão da sua atuação, os arquivos podem ser setoriais e centrais ou gerais. Na classificação quanto à natureza dos documentos, podem ser arquivo especial e arquivo especializado, conforme Paes (2004, p. 20-23). Esta classificação é importante pois nos ajudará a visualizar, na esteira do sistema nacional de arquivos em Moçambique, que arquivos existem, sobretudo no que toca a entidade mantenedora, ou seja, arquivo nacional, provincial ou distrital; e no que toca a extensão da sua atuação, os arquivos centrais e setoriais.

Tendo feito esta breve discussão do conceito de arquivo e aferido a sua classificação, é momento de adentrarmos para a discussão do termo “documento de arquivo” que é

documento de qualquer natureza ou sobre qualquer suporte material que uma pessoa, entidade ou organismo criou ou recebeu e conservou em virtude das suas funções ou das suas actividades, para assegurar a prova de um facto ou acção, ou simplesmente a título de informação (Amaral, 2003, p. 53).

Na base de dados multilinguístico de terminologia arquivística usa-se a expressão “documento arquivístico” para se referir ao “documento elaborado ou recebido, no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência (Multilingual Archival Terminology Database, s.d.).

Heredia Herrera insiste na distinção de “documento de arquivo” dos outros significados genéricos de documentos, com base em sua gênese, sublinhando que estes são “produzidos ou recebidos por uma pessoa ou instituição durante o curso de sua gestão ou atividade para o cumprimento de seus propósitos e preservados como evidência e informação” (Heredia Herrera, 1991, p. 123, tradução nossa). Para além destes, Alves *et al.* (1993, p. 38) lembram um interessante aspecto do documento de arquivo, ao afirmarem que “É a mais pequena unidade arquivística, indivisível do ponto de vista funcional. Pode ser constituído por um ou mais documentos simples”. Mais detalhes são colocados à vista por Bellotto ao afirmar que

Os documentos de arquivo são os produzidos por uma entidade pública ou privada ou por uma família ou pessoa no transcurso das funções que justificam sua existência como tal, guardando esses documentos relações orgânicas entre si. [...] São em geral exemplares únicos e de variadas formas e suportes (Bellotto, 2006, p. 37).

Diante destas definições, parece-nos ser uma boa altura para convidarmos Duranti (1994) que através do seu texto, *Registros Documentais Contemporâneos*, nos apresenta as características (ou qualidades, ou ainda propriedades) dos documentos de arquivo, em suas palavras, dos registros documentais. São elas a imparcialidade, a autenticidade, a naturalidade, o inter-relacionamento e a unicidade.

A imparcialidade é a primeira característica levantada por Duranti pois, segundo a autora, os documentos trazem uma promessa de fidelidade aos fatos e ações que manifestam e para cuja realização contribuem. Os mesmos também ameaçam revelar fatos e atos que alguns interesses não gostariam de ver revelados. Nesta senda, Duranti (1994) defende que proteger os documentos contra manipulação ilegítima ou contra a destruição é o primeiro dever dos arquivistas.

A segunda característica é a autenticidade. A autenticidade está vinculada à produção, manutenção e custódia. Assim, os documentos de arquivo são autênticos porque são produzidos, mantidos e conservados sob custódia de acordo com procedimentos regulares que podem ser comprovados (Duranti, 1994).

Naturalidade é a terceira característica dos registros documentais identificada por Duranti. Conforme a autora, esta característica diz respeito ao modo como os documentos se acumulam no curso das transações, isto é, “não são coletados artificialmente como os objetos de um museu” (Duranti, 1994, p. 52).

A quarta característica dos documentos de arquivo é o inter-relacionamento. Ele deriva do fato de que os documentos estabelecem relações no decorrer do andamento das transações e de acordo com suas necessidades, ou seja,

Os documentos estão ligados entre si por um elo que é criado no momento em que são produzidos que é determinado pela razão de sua produção e que é necessário à sua própria existência, à sua capacidade de cumprir seu objetivo, ao seu significado, confiabilidade e autenticidade. Na verdade, os registros documentais são um conjunto indivisível de relações intelectuais permanentes tanto quanto de documentos (Duranti, 1994, p. 52).

A quinta e última característica apontada por Duranti, é a unicidade. Esta característica advém do fato de que “cada registro documental assume um lugar único

na estrutura documental do grupo ao qual pertence e no universo documental” (Duranti, 1994, p. 52).

Portanto, em matéria que envolve documento de arquivo, não se deve perder de vista estas características que são perenes independentemente da forma, formato, gênero, espécie etc. Não se deve perder de vista estas características inclusive ao discutir a proteção de dados pessoais, dados estes que são encontrados em inumeráveis documentos de arquivo.

Ora, como vimos, os documentos [de arquivo] são produzidos para fins práticos, administrativos e jurídicos específicos da pessoa singular ou coletiva que os gera, como nos relembra Heredia Herrera (1991). A autora acrescenta que a conservação e organização desses documentos em arquivos não tem outra razão senão a de servir os documentos através da sua comunicação. Contudo, Heredia Herrera (1991) alerta que há documentos cujo conteúdo não é do domínio público durante um certo período, enquanto outros precisam ser divulgados imediatamente. Portanto, as condições de acesso têm algumas limitações, relacionadas à segurança do Estado, à privacidade dos cidadãos, etc. (Heredia Herrera, 1991).

Nesta senda, a autora identifica obstáculos que marcam estas limitações como sendo de dois tipos. Obstáculos legais ou jurídicos e obstáculos práticos. Interessam ao nosso estudo os obstáculos legais ou jurídicos pois estes incluem a

necessidade de proteger a segurança do Estado e as suas relações multilaterais; o direito ao respeito pela vida privada; a propriedade intelectual; o segredo industrial e comercial; o direito dos titulares de arquivos à livre utilização dos seus bens pessoais (Heredia Herrera, 1991, p. 494, tradução nossa).

Para melhor entendimento das limitações ligadas à natureza do conteúdo dos documentos, recorreremos à Paes (2004) que apresenta uma classificação dos documentos. De acordo com as características, forma e conteúdo, Paes aponta que os documentos de arquivo podem ser classificados segundo gênero e segundo natureza do assunto. Vejamos a classificação feita por Paes face à natureza do assunto.

Segundo a natureza do assunto, os documentos podem ser ostensivos ou sigilosos. São ostensivos os documentos cuja divulgação não prejudica a administração. São sigilosos aqueles que devam ser de conhecimento restrito e requeiram medidas especiais de salvaguarda para a sua custódia e divulgação (Paes,

2004). A autora aponta quatro níveis de sigilo, a saber: ultrassecreto; secreto; confidencial; e, reservado. No quadro abaixo, estão representados estes níveis de sigilo.

Quadro 2 – Natureza de assuntos de documentos de arquivo

Natureza do assunto	Nível de sigilo	Descrição
Ostensivo	Não se aplica	Documentos cuja divulgação não prejudica a administração
Sigiloso	Ultrassecreto	Assuntos que requeiram excepcional grau de segurança e que o teor ou características só devam ser do conhecimento de pessoas intimamente ligadas ao seu estudo ou manuseio. São assim classificados aqueles de assuntos da política governamental de alto nível e segredos de Estado (negociações para alianças políticas e militares, planos de guerra; descobertas e experiências científicas de valor excepcional; etc.)
	Secreto	Assuntos referentes à planos, programas e medidas governamentais, os assuntos extraídos de matéria ultrassecreta que, sem comprometer o excepcional grau de sigilo, necessitam de maior difusão (planos ou detalhes de operações militares; dados de elevado interesse sob aspectos físicos, políticos, econômicos, psicossociais e militares de países estrangeiros; etc.)
	Confidencial	Assuntos que seu conhecimento por pessoa não autorizada pode ser prejudicial a um indivíduo ou criar transtornos administrativos. São os assuntos referentes à pessoal, material, finanças e outros cujo sigilo deva ser mantido por interesse das partes (informações sobre a atividade de pessoas e entidades; cartas, fotografias aéreas e negativos que indiquem instalações consideradas importantes para a segurança nacional; etc.)
	Reservado	Assuntos que não devam ser do conhecimento do público em geral. Recebem essa classificação, entre outros, partes de planos, programas e projetos e as suas respectivas ordens de execução; cartas, fotografias e negativos que indiquem instalações importantes

Fonte: Adaptado de Paes (2004).

Estes níveis de sigilo apresentados pela Paes (2004) podem ser submetidos à exceção. Schellenberg (2006) aponta que pode haver exceção ao grau de sigilo imposto as informações pessoais “quando as ações de um indivíduo comprometem seriamente o Estado, como no caso de atos criminosos” (Schellenberg, 2006, p.352). Como que chamando a atenção, o autor pontua que a regulamentação sobre a proteção dos dados pessoais

não deve impedir o acesso a documentos de serviços de administração de pessoal ou de serviços médicos, nem deve interceptar o uso de dados pessoais, tais como os contidos em tabelas de recenseamentos, se tais dados são utilizados no seu conjunto e não individualmente, nem deve aplicar-se por um período indefinido de tempo (Schellenberg, 2006, p.352).

Portanto, as normativas devem clarificar que os documentos sobre atividades oficiais dos servidores públicos, são distintos de documentos relativos à vida de cada

servidor, e por essa razão não devem ser excluídos de consulta sob alegação de que o acesso àqueles pode ferir a reputação dos servidores, pois esses servidores públicos (no serviço militar, diplomático, civil, etc.), devem prestar contas ao povo.

Portanto, os documentos de arquivo com tudo que representam, carregados de características específicas que os fazem diferentes de outros documentos, sujeitos a classificações de diversa ordem e que podem limitar o acesso a eles, são sujeitos a limitações muitas vezes objeto de normativas em diferentes ordenamentos jurídicos. Mas para que os aspectos levantados aqui, e outros, tenham lugar e sejam respeitados, é preciso que ocorra o processo de gestão desses documentos. Passemos então à discussão em torno da “gestão de documentos”, lembrando que, nesta tese, tal qual Troitiño (2015, p. 159) “[...] estamos a todo o momento nos referindo a documentos de arquivo, ou seja, documentos em contexto e estreita relação orgânica entre si”, mesmo que o termo “documento” não apareça acompanhado do termo “arquivo”.

3 DA GESTÃO DE DOCUMENTOS E POLÍTICA ARQUIVÍSTICA À PROTEÇÃO DE DADOS PESSOAIS

Nesta seção são discutidos os conceitos de gestão de documentos, de política arquivística adentrando, em termos gerais e de conceito, para a política arquivística nacional, assim como sistema de arquivos com enfoque em sistema de arquivos nacional, desembocando na noção de proteção de dados pessoais, dando-se aqui maior atenção aos princípios que norteiam esta proteção e que encontram fundamentos na gestão de documentos.

3.1 Gestão de documentos

Se acima vimos termos polissêmicos como “dado”, “documento” e “arquivo”, sobre a gestão de documentos (GD) não ocorre exatamente a mesma coisa, mas há diferentes percepções do que ela seja em diferentes cantos do mundo. Aliás, Schwaitzer, Nascimento e Costa (2021) constataram que sobre a GD a literatura mostra que não há uma compreensão universal devido às especificidades de cada país e de cada organização. Um exemplo na literatura é o texto da Indolfo (2007) em que a autora é categórica ao afirmar que “não se pode falar de gestão de documentos como um conceito único e de aplicação universal [...]”, e “não se pode falar [...] de um modelo de gestão de documentos, mas de diversidades que se produziram com as práticas em diferentes países” (Indolfo, 2007, p. 33-34).

As respostas as necessidades nascidas com a crise econômica, dos anos 1930, e com a Segunda Guerra Mundial, foram diferenciadas de acordo com os países, os governos, as tradições arquivísticas e os contextos históricos. Surgiram, a partir daí, vários modelos nacionais estreitamente ligados às condições culturais, econômicas, administrativas e históricas (Indolfo, 2007, p. 35).

Indolfo constata assim que, se as motivações forem de ordem econômico-administrativa, implantava-se o modelo americano e, se as motivações forem de ordem histórico-arquivística, seguia-se o modelo europeu (Indolfo, 2007). É desta forma que

Os Estados Unidos, entre outros países anglo-saxônicos, são considerados pioneiros, desde os anos 1940, na elaboração do conceito de gestão de documentos (*records management*) cuja ótica, inicialmente, era nitidamente mais administrativa e econômica do que arquivística, uma vez que se tratava,

essencialmente, de otimizar o funcionamento da administração, limitando a quantidade de documentos produzidos e o prazo de guarda (Indolfo, 2007, p. 30).

Em 2014, Heredia Herrera dava a indicação de que a gestão de documentos (GD) é uma expressão mais recente que tem origem não arquivística, embora tenha sido apropriada por arquivistas e arquivos. A GD começa antes da produção documental, envolvendo para além de arquivistas, gerentes administrativos e técnicos de informática (Heredia Herrera, 2014).

Jardim (2015) nos lembra que a associação da GD aos Estados Unidos, sobretudo no pós-II Guerra Mundial, emergindo em meados do século XX, com uma forte relação com o Estado, embora possa ser compreendida também fora deste contexto estatal norte-americano como campo científico. Este entendimento é similar ao da Rodrigues ao ter apontado que na segunda metade do séc. XX, registou-se uma reorientação da profissão dos arquivistas face ao volume documental, quando na América do Norte entrou em pauta a eliminação de documentos antes do recolhimento destes à guarda permanente (Rodrigues, 2006).

Considerando estas falas, entendemos, através de Schwaitzer, Nascimento e Costa (2021) que a GD tem como um dos propósitos separar documentos que devem passar pelo recolhimento daqueles que podem seguir para a eliminação de modo a garantir o controle e o direito individual de acesso à informação, observando as possíveis restrições para o seu acesso integral (Schwaitzer; Nascimento; Costa, 2021, p. 12).

Independentemente dos múltiplos modelos de GD ou ainda concepções diferenciadas, de orientações americanas ou europeias,

Administrar ou gerenciar documentos arquivísticos, a partir da aplicação de conceitos e teorias difundidas pela Arquivologia, garante às empresas públicas ou privadas obter maior controle sobre as informações que produzem e/ou recebem, racionalizar os espaços de guarda de documentos, desenvolver com mais eficiência e rapidez suas atividades, atender adequadamente clientes e cidadãos (Roncaglio; Szvarça; Bojanoski, 2004, p. 6).

Portanto, a GD “permite que os documentos sejam tratados, organizados e disseminados com eficácia e eficiência, considerando os valores que os mesmos possuem para a organização por meio da avaliação de documentos” (Schwaitzer; Nascimento; Costa, 2021, p. 11). Ou como fala Heredia Herrera (1991), a GD intimamente ligada à avaliação de documentos, compreende o planeamento,

controle, direção, organização, promoção e outras atividades de gestão relacionadas aos documentos antes de chegarem aos arquivos históricos. Logo, o termo “gestão de documentos” segundo Heredia Herrera (1991, p. 178) refere-se a “todas as medidas destinadas à economia e eficácia dos documentos”. No entanto,

não devemos perder de vista que este termo reflecte uma realidade e uma atividade levada a cabo pelos arquivistas. Todo o trabalho dos arquivistas não é mais do que a gestão dos documentos, antes e depois de chegarem ao arquivo, acrescida de novos aspectos e novas realidades, embora o nome e o conceito de gestão documental estejam ligados à fase pré-arquivística com uma projeção até aos arquivos intermédios onde se decide plenamente a conservação permanente e o início do verdadeiro arquivo (Heredia Herrera, 1991, p. 179, tradução nossa).

Alves *et al.* (1993, p. 53) definem GD como a “implementação de um conjunto de medidas que visam a racionalização e a eficácia na constituição, avaliação, aquisição, organização, conservação, e comunicação dos arquivos”. Para Bellotto (2006, p. 30) a GD resume-se no “acompanhamento da produção, no recebimento, na classificação, no controle da tramitação e na avaliação”. Cunha e Cavalcanti (2008) vêm a GD como conjunto de procedimentos e operações técnicas ligadas à produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, com vista à sua eliminação ou recolhimento.

É inevitável atentar ao “ciclo vital de documentos” quando falarmos da GD. Este conceito foi anunciado em 1940 por Brooks numa reunião da *Society of American Archivists* e teve impacto na operacionalização do sistema de gestão de documentos posteriormente desenvolvido pelo Arquivo Nacional dos Estados Unidos (Jardim, 2015). A ideia do ciclo vital também foi trabalhada por Schellenberg ao falar da “vida útil” de um documento de forma semelhante a um organismo biológico. Assim, os documentos nascem (produzidos ou recebidos), vivem e envelhecem (usados, distribuídos e preservados) e, finalmente, morrem (eliminação) (Beckles, 2014). Nesta senda, os documentos de arquivo passam por três estágios em seu ciclo de vida, “de um estágio corrente para um estágio semi-corrente e, finalmente, para um estágio não corrente” (Beckles, 2014, p. 239).

Beckles coloca muito bem ao entender que pelo ciclo de vida os documentos passam concomitantemente por três estágios e não ter colocado o ciclo e os estágios como sinónimos. Na verdade, a teoria das três idades (que abordaremos mais adiante) encontra suas bases no de ciclo de vida de documentos e essa pode ser a razão da frequente confusão entre esses termos. De forma sintética, a teoria das três idades

sustenta a ideia de que os documentos de arquivo, em razão do seu uso e do seu valor para a entidade que os produziu ou para terceiros, esses documentos podem sofrer intervenções em uma ou mais fases, a saber: corrente, intermediária e permanente (Jardim, 2015).

Rousseau e Couture (1998) percebem que

uma boa organização dos arquivos correntes gera uma quantidade importante de vantagens, tais como: o aumento da eliminação dos documentos na fonte e a diminuição do volume documental total; a aceleração e a sistematização da organização dos documentos; o aumento da proteção da informação (um documento bem classificado, ordenado e arrumado está relativamente em segurança); aceleração da pesquisa de informação e o facto de obter de forma mais rápida a informação pertinente, etc. (Rousseau; Couture, 1998, p. 119).

O clássico trabalho de Rhoads de 1989, *“La Función de la gestión de documentos y archivos en los sistemas nacionales de información: un estudio del RAMP”* traduzido para diferentes línguas, aponta as fases de gestão de documentos e que representam o ciclo de vida dos documentos, conforme o autor, fase de produção; fase de utilização e conservação; e, fase de eliminação.

A fase de produção de documentos abrange a concepção e gestão de formulários, preparação e gestão da correspondência, gestão de relatórios e orientações, aplicação de tecnologias modernas a estes processos etc. (Rhoads, 1989). A fase de utilização e conservação dos documentos cobre a criação e melhoria dos sistemas de arquivo e de recuperação, gestão do correio e das telecomunicações, seleção e funcionamento de fotocopiadoras, análise dos sistemas, funcionamento dos centros de documentação e aplicação, se for caso disso, da automatização e da reprografia a estes processos, etc. (Rhoads, 1989). Os sistemas de arquivo e de recuperação de informação aqui indicados devem ser ajustados às necessidades operacionais e antecipar a necessidade de proteger qualquer informação que o necessite em particular (Rhoads, 1989). A fase de eliminação inclui a identificação e a descrição das séries documentais, o estabelecimento de prazos de retenção, a avaliação e a eliminação dos documentos e o recolhimento dos documentos de valor permanente para os arquivos (Rhoads, 1989).

Retomando Beckles, notamos a autora assinalar que embora o conceito de ciclo vital dos documentos tenha sido contestado e tenha recebido sérias críticas, ele é amplamente aceito e utilizado em programas tradicionais de gestão de documentos

estabelecidos em todo o mundo, principalmente quando se lida com sistemas baseados em papel, em que há a movimentação física de documentos em papel, empregando processos manuais (Beckles, 2014). A autora avança apresentando uma versão contemporânea do conceito de “ciclo de vida” com cinco estágios principais: o estágio de produção; o estágio de distribuição e uso; o estágio de armazenamento e manutenção; o estágio de retenção e disposição; e, o estágio de preservação arquivística.

Beckles (2014) explica ainda que em cada um desses estágios, os documentos são fisicamente movidos do espaço ativo, que pode um escritório, para o armazenamento secundário onde são avaliados para destruição, retidos para revisão posterior ou considerados de valor permanente e enviados para um arquivo. Controles de privacidade/proteção de dados podem ser instituídos para proteger os dados pessoais encontrados nesses documentos por meio de um programa de gestão de documentos bem funcional e projetado para uma finalidade específica, usando o conceito de ciclo de vida (Beckles, 2014, p. 240).

Não apenas o conceito de ciclo vital de documentos ou as fases da gestão de documentos são importantes discutir neste trabalho, mas também são de elevada importância os instrumentos dessa gestão. Assim, como indicam Bernardes e Delatorre (2008, p. 10) o “Plano de Classificação e a Tabela de Temporalidade de Documentos de Arquivo são instrumentos eficazes de gestão documental”, eles garantem a simplificação e a racionalização dos procedimentos de gestão, proporcionando maior agilidade e precisão na recuperação da informação, autorizando a eliminação criteriosa de documentos sem valor que justifique a sua guarda e a preservação dos documentos permanente (Bernardes; Delatorre, 2008).

Bernardes e Delatorre explicam, o Plano de Classificação de Documentos “resulta da atividade de classificação que recupera o contexto de produção dos documentos de arquivo agrupando-os de acordo com o órgão produtor, a função, a subfunção e a atividade responsável por sua produção ou acumulação” e a Tabela de Temporalidade de Documentos “o resulta da atividade de avaliação, que define prazos de guarda para os documentos em razão de seus valores administrativo, fiscal, jurídico-legal, técnico, histórico, autoriza a sua eliminação ou determina a sua guarda permanente” (Bernardes; Delatorre, 2008, p. 11).

Schäfer, Martins e Silva (2024) ao falarem da *Gestão de documentos arquivísticos voltada à proteção de dados pessoais* concluem:

A gestão de documentos arquivísticos possui instrumentos e procedimentos que podem auxiliar no tratamento de dados pessoais, destacando-se o controle da produção de documentos, a aplicação do plano de classificação e da tabela de temporalidade e destinação de documentos, a efetivação da eliminação de documentos para garantir que dados pessoais que sirvam a obrigações legais já cumpridas sejam excluídos. Relevante, também, é a incorporação de procedimentos arquivísticos nos sistemas informatizados responsáveis pela produção e manutenção de documentos em meio nato digital. Assim, a definição de procedimentos, tarefas, fluxos e demais ações para o tratamento dos dados pessoais podem encontrar subsídios na gestão de documentos (Schäfer; Martins; Silva, 2024, p. 21).

Os instrumentos da GD, como vimos, são incontornáveis no âmbito de um programa de gestão de documentos. E um programa eficaz exige uma direção por parte de uma autoridade pública central, bem como a participação ativa de vários organismos na execução do programa onde os administradores principais desse organismo devem dar prioridade ao programa de gestão de documentos, compreendendo os seus objetivos e as suas vantagens (Rhoads, 1989). Esse programa de gestão de documentos pode ser aplicado de forma escalonada em 4 níveis: nível mínimo, nível mínimo ampliado, nível intermediário e nível máximo.

Portanto, foram identificados por Rhoads (1989) esses quatro níveis de aplicação, embora, segundo o autor, deva ser reconhecido que qualquer um dos primeiros três pode ser expandido através da incorporação de determinados serviços e sistemas num dos níveis superiores.

No que toca ao nível mínimo, não se pode dizer que um governo tem um programa de gestão de documentos se não conta, no mínimo, com sistemas para preparar listas de conservação e eliminação de documentos, eliminar documentos conforme ao indicado na lista e recolher os documentos de valor permanente aos arquivos nacionais. O nível mínimo ampliado abarca os sistemas do nível mínimo, bem como o uso de um ou mais centros de arquivo. Por sua vez o nível intermediário compreende os sistemas e serviços do nível anterior, como também outros subprogramas básicos, consistindo, em geral, na preparação e gestão de formulários, gestão de correspondência e relatórios, desenvolvimento de sistemas de arquivo e recuperação, gestão de arquivos e um programa de documentos essenciais, bem como planeamento de proteção contra desastres. O quarto nível, nível máximo toca os sistemas e serviços do nível anterior, mas igualmente a gestão de diretrizes,

correspondência e telecomunicações, copiadoras, tratamento de textos para a preparação de correspondência, relatórios, utilizam a análise de sistemas, a automatização e a tecnologia em diversas circunstâncias, etc. (Rhoads, 1989).

Ora, os programas de gestão de documentos são parte, em condições normais, de uma política arquivística. Ao se discutir uma política arquivística, identifica-se o programa de gestão de documentos, a ser implementado nos diferentes níveis vistos acima, como uma parte fundamental dessa política. Estas políticas arquivísticas podem ser desenhadas e implementadas em diferentes níveis da estruturação de um Estado. Aqui nos referimos aos níveis federal ou nacional, regional, estadual, provincial, municipal, local etc., conforme a estrutura desse Estado. A seguir, dado o interesse particular nesta tese, nos debruçamos sobre a política arquivística, com ênfase na de dimensão nacional.

3.2 Política arquivística

Parece justo antes de falarmos de política arquivística, ainda que de forma muito breve, revisitar o termo “política”. Portanto, este termo por ser polissêmico, carrega diferentes significados conforme sua aplicação. Estes significados ficam, em particular na língua portuguesa, escondidos pela invariabilidade da palavra “política”. Neste sentido e à semelhança de Jardim, Silva e Nharreluga (2009), recorreremos à língua inglesa para deixar mais visíveis os diferentes significados deste termo. Assim, nos deparamos com 3 significados do termo “política”, a saber:

Polity, para a esfera da política e para diferenciar o mundo da política do da sociedade civil; *politics*, como a atividade política na disputa por cargos políticos, o debate partidário etc.; *policies*, para a ação pública, ou seja, os processos que elaboram e implementam programas e projetos públicos (Muller; Sured, 2004, p. 13 *apud* Jardim; Silva; Nharreluga, 2009, p. 10).

Viegas, Santana e Noda (2020) recorreram a Palumbo (1994) para defender que política pública é o princípio orientador de regulamentos, leis, programas, e tem sua visibilidade nas estratégias adotadas pelo governo para responder aos problemas públicos. Aliás, Gomes em 2013, havia afirmado que as políticas públicas constituem uma realidade complexa que não se resume apenas a normas, nem apenas a atos administrativos, mas pela união e combinação deles, junto de ações concretas (Gomes, 2013). O autor explica melhor,

As políticas públicas apresentam-se como uma realidade complexa e formada não apenas por normas jurídicas, mas também por efetivas ações, tanto do poder público, como de agentes particulares, todos na busca por atingir metas constitucionalmente estabelecidas, podendo ser apreendidas em dois momentos principais: o normativo-hipotético e o concreto (ou de execução). Sem medo de incidir em equívoco, pode-se dizer que não há políticas públicas desprovidas de normas e, de forma paralela, sem o cumprimento mínimo do que fora hipoteticamente previsto (Gomes, 2013, p.137).

Consideradas as acepções de política e o conceito de política pública acima, importa esclarecer em que perspectiva de política levamos a cabo a nossa discussão sobre políticas arquivísticas, em particular, e mais largamente toda esta tese. Nesta senda, é na dimensão da política enquanto *policy* (*polícies*, no plural), política pública, que reside a nossa discussão atendendo o seu cunho para a formulação e implantação de programas e projetos públicos como podem ser os casos de política arquivística nacional; sistema nacional de arquivos; programas de gestão de documentos; proteção de dados pessoais; acesso à informação; etc.

A propósito, Heredia Herrera (1991) diz que falar de política de arquivos não é diferente de qualquer outro tipo de política. Para ela, a política arquivística é “a determinação sistemática dos meios administrativos, institucionais e económicos que permitirão atingir as finalidades e os objetivos dos arquivos em resposta às exigências da sociedade” (Heredia Herrera, 1991, p. 200, tradução nossa).

Ademais, “Uma política de arquivos estará também intimamente relacionada com o sistema organizacional do país” (Heredia Herrera, 1991, p. 200, tradução nossa). O mesmo entendimento tem Jardim (2006) defendendo que estas políticas podem ser setoriais e podem apresentar uma configuração nacional, regional ou local, esperando-se que elas se intersectem com outras políticas públicas (de saúde, de educação, etc.). Mas, chama atenção Jardim (2006), a política não deve ser confundida com legislação arquivística que é a fornecedora de elementos normalizadores à política. A legislação encontra viabilidade se for instrumento e objeto de uma política.

Heredia Herrera acrescenta que essa política não será uma boa política de arquivos se polarizar a sua ação e atuação em torno de determinados centros, “esquecendo outros setores menos favorecidos, que em quase todos os países tendem a ser a maioria” (Heredia Herrera, 1991, p. 200, tradução nossa). Ademais, exigirá “um sistema, uma legislação e meios, partindo do princípio de que teremos, na

melhor das hipóteses, arquivos e, na pior, depósitos de documentos” sendo ambos centrais na administração de arquivos em qualquer país (Heredia Herrera, 1991, p. 201, tradução nossa).

Jardim percebeu que se registava um crescente interesse sobre as “políticas públicas arquivísticas” devido à, pelo menos, 3 razões principais: o fracasso dos mega sistemas nacionais de informação; o fato de que sistemas, programas ou ações informacionais tenderem a ser melhor sucedidos quando precedidos pela formulação e implementação de políticas de informação; e, a ampliação de novos modos de produzir, conservar e usar a informação aliada às TIC’s (Jardim, 2006).

Cunha e Cavalcanti (2008) definem a política de arquivo como um documento formal que define a missão, os objetivos, tipos de serviços e demais informações pertinentes às atividades do arquivo. Esta é uma perspectiva bastante importante na discussão que fazemos, pois, a ausência de uma política formalizada em um documento pode significar o desnorreamento dos objetivos, da missão, dos serviços e instituições arquivísticas e acarretar violações de direitos aos cidadãos.

Jardim (2006, p. 6) entende política pública arquivística como o

conjunto de premissas, decisões e ações – produzidas pelo Estado e inseridas nas agendas governamentais em nome do interesse social – que contemplam os diversos aspectos (administrativo, legal, científico, cultural, tecnológico, etc.) relativos à produção, uso e preservação da informação arquivística de natureza pública e privada (Jardim, 2006, p. 6).

Considerando a transversalidade e outros aspectos apontados acima, Jardim (2006) considera que para formular políticas públicas arquivísticas, exige-se de seus formuladores, conhecimento político, gerencial e técnico-científico. Portanto, um conhecimento sobre a realidade onde o Estado pretende agir em relação aos arquivos, incluindo as formas de produção, uso e conservação dos arquivos públicos e privados, como também atores abrangidos pela política. Assim como um conhecimento multidisciplinar que emerge não apenas da Arquivologia, como também da Ciência Política, da Administração, entre outras.

Daí que diversos setores devem estar envolvidos na sua formulação, implantação e avaliação como: agentes públicos das áreas de ciência, tecnologia, administração, educação e cultura; agentes dos poderes executivo, legislativo e judiciário; agentes representantes dos diversos tipos de usuários dos arquivos, como

também dos arquivos privados, de instituições de ensino e pesquisa fora do aparelho do Estado e de organizações profissionais arquivísticas (Jardim, 2006).

Como vimos acima, uma política de arquivos tem relação íntima com o sistema organizacional do país e podem apresentar uma configuração nacional, regional ou local, conforme o caso (Heredia Herrera, 1991; Jardim, 2006). Assim, no nível nacional a “política nacional de arquivos compreende a definição e a adoção de um conjunto de normas e procedimentos técnicos e administrativos, para disciplinar as atividades relativas aos arquivos públicos e estimular a organização e a proteção aos arquivos privados” (Paes, 1998, p. 235).

Essa política nacional de arquivos ou política arquivística nacional, deve apresentar objetivos e objeto. Rodrigues (2012) aponta como sendo os objetivos de uma política nacional de arquivos:

A democratização e o aumento da qualidade do acesso à informação arquivística pública e à privada de interesse público; a promoção da boa governança; a promoção do *accountability*; a promoção da geração de conhecimento a partir das ações do poder público; a promoção da participação dos cidadãos nas decisões dos ocupantes dos cargos públicos, e; a construção da memória nacional (Rodrigues, 2012, p. 199).

Como podemos constatar, o acesso a informação de interesse público é um dos objetivos da política arquivística. Sobre este aspecto, Schellenberg (2006) apontou que se serve o interesse público evitando-se o acesso a documentos que contenham certos tipos de informações pessoais. O autor explica que se registra crescente quantidade de informação de natureza privada, uma vez que a esfera de ação dos governos modernos atinge cada vez mais a vida privada dos cidadãos. Certos tipos de documentos que contêm tais informações

são as tabelas de recenseamentos, os documentos de serviço militar, documentos de serviço público e prontuários médicos. Entre os de tipos especiais estão os relatórios de investigações de atividades criminais ou subversivas. Comumente não se deve dar divulgação a informação contida em tais documentos, prejudicial ao interesse do indivíduo ou a seus parentes próximos. Sem dúvida, serve-se o interesse público protegendo-se o que for de caráter reservado de cada cidadão (Schellenberg, 2006, p.352).

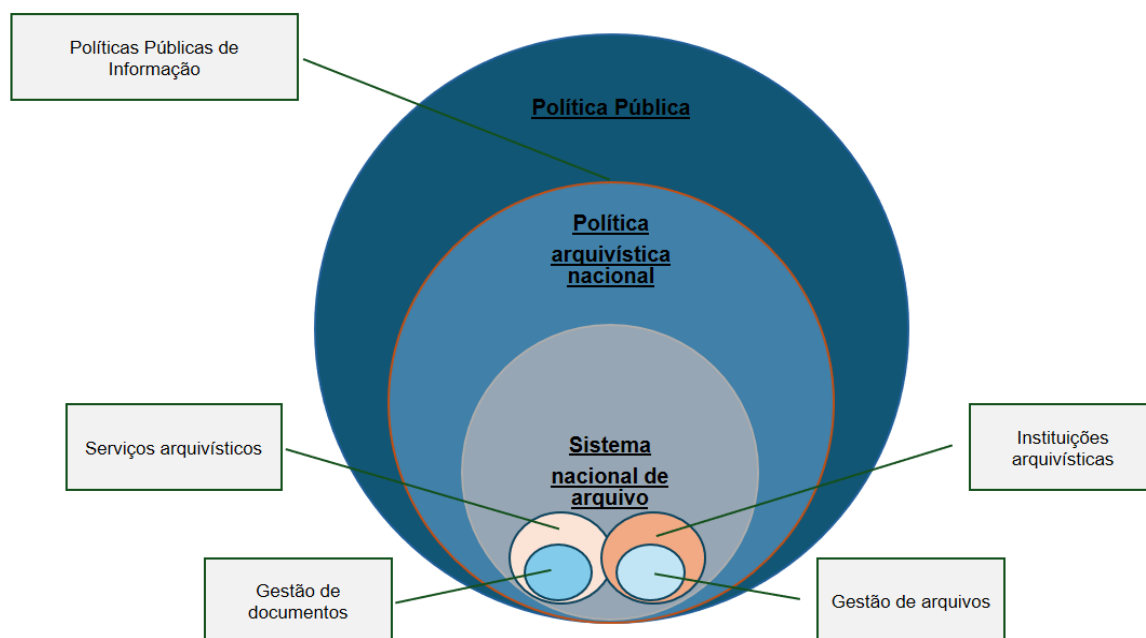
Em relação ao objeto de uma política arquivística nacional, Rodrigues (2012) compreende ser

a instituição arquivística pública; os documentos arquivísticos públicos e aqueles privados de interesse público; os órgãos e entidades que produzam esses documentos; os profissionais envolvidos; as entidades que ofereçam cursos e outros meios para a formação e capacitação do arquivista; os conselhos de arquivos e outras entidades de promoção e fiscalização da atividade arquivística; os órgãos e entidades implicados no processamento eletrônico da informação arquivística pública, e; aqueles órgãos implicados na comunicação e difusão da informação arquivística pública (Rodrigues, 2012, p. 199).

Tendo em conta estes aspectos, recorreremos à assertiva de Nharreluga (2021, p. 137) segundo a qual “a política arquivística, ainda que possa ser influenciada pelo sistema arquivístico, este prevalece como produto e não causa daquela”. Significa que o sistema nacional de arquivos é um mecanismo ou uma forma de operacionalização de uma política nacional de arquivos e por isso mesmo a política nacional de arquivos é um pré-requisito em relação ao sistema nacional de arquivos.

Achamos oportuno reproduzir, na figura que se segue, a posição e relação de *policy*, política arquivística (nacional) e sistema (nacional) de arquivo.

Figura 2- Relação de políticas públicas, política arquivística e sistema de arquivo



Fonte: Elaborado pela autora.

Da figura 2, percebe-se que uma política arquivística nacional, ela é antes de mais, uma política pública e, como tal, deve apresentar os diferentes aspectos gerais

de uma *policy*. A figura ilustra ainda que é decorrente da política arquivística nacional que deve funcionar o sistema nacional de arquivos que vai, por sua vez, dar conta dos serviços de arquivo e das instituições de arquivo, ou seja, a gestão de documentos e a gestão de arquivos conhecem aí melhor desenvolvimento.

3.2.1 Sistema nacional de arquivo

O sistema de arquivos é um conceito que responde à integração e à coordenação e que foi instrumentalizado através da legislação. A materialização de uma política arquivística deve traduzir-se numa programação arquivística (Heredia Herrera, 1991). E como nos alertam Nharreluga e Silva (2002), as noções de sistema de arquivos e de sistema nacional de arquivos possuem três facetas fundamentais: teórica, jurídica e operacional. Como sistemas abertos eles atuam sobre toda a organização arquivística, mantendo através do subsistema de arquivos, uma relação de interdependência com as estruturas administrativas.

O sistema de arquivos é, portanto, conforme Heredia Herrera (1991) a articulação lógica e fundamentada da rede de centros e, de recolhimento e depósito de documentos de arquivo, e requer uma gestão através de organismos e instituições competentes. Ou seja, sistema de arquivo é um conjunto de atividades articuladas através de uma rede de centros e serviços técnicos, para estruturar a recolha, transferência, depósito, organização, descrição e serviço dos documentos. É a legislação que define o sistema e estabelece as linhas do seu serviço e da sua eficácia. Contudo, há países que não dispõem de tal legislação e/ou que apenas dispõem de regulamentos ou disposições parciais. É o caso de Moçambique. No caso dos países que contam com algum marco legal, estes revelam diferentes pontos de vista ou perspectivas. Alguns países legislam apenas sobre os documentos conservados em arquivos públicos, enquanto outros países alargam o seu âmbito de aplicação. Outros países não consideram os documentos a não ser quando dão entrada nos arquivos.

Rhoads (1989) aponta em alguns países se distingue os arquivos nacionais propriamente ditos (que se ocupam principalmente dos documentos governamentais) e o sistema nacional de arquivos, que engloba o conjunto dos bens arquivísticos de

um país a fim de conservar e fazer acessíveis todos os arquivos de interesse para a investigação, e utilizar os recursos disponíveis para seus fins de maneira mais eficaz e económica possível (Rhoads, 1989, p. 37). Ressalta também que em muitos países, em particular nos que têm um sistema de governo muito centralizado, em certa medida, os arquivos nacionais são responsáveis pelos arquivos de organizações não governamentais incluindo de documentos privados de particulares (Rhoads, 1989).

Heredia Herrera apresenta a questão nos seguintes termos:

Nos países com uma administração centralizada, os arquivos públicos são geridos por uma única autoridade (ou por um pequeno número de autoridades). Nestes casos, existe uma hierarquia de arquivos centrais (arquivos nacionais), regionais (arquivos provinciais, departamentais ou distritais) e locais, bem como de repositórios especializados para arquivos audiovisuais, científicos, militares, etc., todos subordinados a uma direção central a nível governamental. Nestes casos, existem leis aplicáveis a todos os arquivos do país (Heredia Herrera, 1991, p. 207, tradução nossa).

Um sistema de arquivos dependerá, em primeiro lugar, da organização político-administrativa do país, podendo ser centralizado, federal, etc., sendo assim um sistema ou a soma de vários. Cada um será constituído por órgãos executivos e outros órgãos consultivos, cujo número e entidade vai depender do número de centros e do seu âmbito jurisdicional (Heredia Herrera, 1991).

Duchein (1980 *apud* Heredia Herrera, 1991, p. 211) considera um certo número de pontos indispensáveis a ter em conta em qualquer lei de arquivos de qualquer país, a saber:

definição de arquivos, tanto públicos como privados, e responsabilidade do Estado na sua salvaguarda para servir a Administração, os cidadãos e a ciência; descrição do sistema de arquivos; responsabilidade total dos serviços de arquivo na determinação dos expurgos; estabelecimento de normas de transferência, classificação e descrição; regras de acesso; estabelecimento dos deveres e obrigações dos arquivistas e da sua formação profissional; disposições relativas à proteção dos arquivos privados de interesse histórico (Duchein, 1980 *apud* Heredia Herrera, 1991, p. 211).

Depreende-se daqui que um sistema nacional de arquivos ou de outra dimensão, encontra de antemão, em normativas, a sua descrição. Para além destes pontos indispensáveis numa lei de arquivos, que incluem a descrição do sistema de arquivos, há medidas que se exigem para criação de um sistema nacional de arquivos. Rhoads (1989) elencou as seguintes medidas: estabelecimento de arquivos nacionais que constituam o órgão arquivístico da administração central; imposição, a todos os órgãos governamentais ou administrativos, assim como os organismos públicos e

semipúblicos de todo tipo, da obrigação regulamentar de tomar disposições para criar e administrar arquivos; proteção dos arquivos privados frente a toda destruição dolosa, deterioração, venda e exportação, e promoção de seu depósito em qualquer instituição arquivística adequada; estabelecimento de um mecanismo central que constitua um meio adequado de integração ou coordenação dos serviços arquivísticos.

Daí que Heredia Herrera (1991) nos diz que com base num sistema de arquivo, os diferentes conjuntos de documentos resultantes das diferentes administrações não podem ser considerados isoladamente, mas fazem parte do conjunto orgânico do país como um todo, o que joga um papel importante nas transferências e eliminação. A autora salienta que um sistema de arquivos apoia, de forma lógica e coerente, um sistema de informação nacional.

Dito de outro modo por Nharreluga (2021), os sistemas nacionais de arquivos são concebidos como um modelo de gestão de documentos e arquivos num contexto e âmbito marcado pela existência de uma estrutura constituída por entidades arquivísticas, consideradas no quadro de uma política de arquivo. Esta condição parece não ser atendida em Moçambique na sua, agora, terceira versão de um sistema nacional de arquivos, que é objeto de análise mais adiante.

Não menos importante para os sistemas de arquivo, os nacionais em particular, são as associações profissionais. Na área dos arquivos, a mais antiga, de 1891, é a holandesa. Estas associações, conforme Heredia Herrera (1991), constituem um fórum permanente para os arquivos e os arquivistas. Em condições normais e em teoria, deveriam ser as associações profissionais a se ocuparem do desenvolvimento de normas, da formação e da relação com outras associações. Na sua maioria cria uma publicação periódica. Mais adiante abordaremos sobre essas associações no contexto moçambicano.

3.3 Proteção de dados pessoais

Humbert Lesca e Elisabeth Lesca na segunda edição da sua obra *“Gestion de l’information: Qualité de l’information et performances de l’entreprise”*, começam relembando que as empresas ou organizações em geral, são frequentemente

comparadas à seres vivos, e como tais elas são suscetíveis de terem doenças. Entre tais, figuram as doenças que eles chamaram de “*Maladies de l’information*”. Portanto, na obra em referência, os autores mostram que as organizações podem ficar doentes de sua informação e essa doença pode comprometer seriamente sua performance econômica. Eles mostram ainda que a informação representa um capital suscetível de ser roubado ou destruído deliberadamente, seja por agentes externos ou mesmo pelo pessoal interno. Embora não seja algo novo, os autores apontam que esta questão tomou proporções que permitem falar de uma “ruptura” nos comportamentos, na deontologia e na ética (Lesca; Lesca, 2010). Entre diferentes *maladies de l’information* como sobrecarga informacional, anemia informacional, ambiguidade e incoerência informacional, perda de memória, etc., os autores apontam para as agressões como roubo, falsificação, destruição deliberada de informação, que inclui informação pessoal, o que demanda sua proteção levada à sério pelos dirigentes das empresas ou organizações em geral.

Garcia (2018) é categórico ao afirmar que a questão sobre os dados pessoais se amplia em importância em decorrência do avanço das TIC. Aliás, como é de comum entendimento, a noção de sociedade de informação, nasce na década de 1970, com a emergência das TIC.

Com o mesmo entendimento, Mendes (2019) defende que a proteção de dados pessoais desponta no contexto da sociedade de informação, “como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados *per se*, mas, sim, a pessoa que é titular desses dados” (Mendes, 2019, p. 35).

Os autores acima deixam nas entrelinhas que a questão da proteção de dados pessoais não é um assunto inteiramente novo, mas vem ganhando diferentes contornos conforme a sociedade avança e as TIC evoluem. Na verdade, a discussão remonta do século XIX em particular, com o artigo “*THE RIGHT TO PRIVACY*” de Warren e Brandeis, publicado na Harvard Law Review em 1890, com a tônica na privacidade, no direito a estar só. Doneda (2006) tem a mesma compreensão, apontando que uma crescente preocupação em relação à tutela da privacidade é própria de nosso tempo, mas a ideia de privacidade em si não é recente, podendo ser identificada noutras épocas e sociedades.

A privacidade esteve durante muito tempo reservada à elite e mesmo que hoje ela esteja consagrada como um direito fundamental na constituição de diferentes países, como o caso de Moçambique, traços do contexto individualista do qual é originária ainda se fazem notar (Doneda, 2006). Ora, com o aumento do fluxo e importância da informação, não é mais a “elite” que estava e está sujeita a ter sua privacidade violada. Nos dias que correm, pela internet todos podem se comunicar, bastando possuir um computador, um modem e uma linha telefônica. Ampliou-se a facilidade de acesso à informação (não mais apenas para a elite) armazenada em computadores, quer se trate de informações livremente disponíveis, quer se trate de informações e dados pessoais de ordem privada (Boff; Fortes, 2014, p. 110). De fato, como mostram Ferreira, Pinheiro e Marques (2021), com a expansão das TIC, ganham destaque alguns problemas, como a violação da privacidade de seus usuários diante do acesso e coleta de dados pessoais por meio dos artefatos tecnológicos.

A informação pessoal, como se refere Doneda (2006), assume importância por pressupostos diversos, com destaque para o controle e a eficiência, tendo a volta deles uma série de interesses envolvendo o Estado e o privado. Aliás, empregando um ponto de vista sócio-histórico, a noção de privacidade no capitalismo sofreu transformações ao dar novo significado ao conceito de vida privada e o limite entre o público e o privado (Ferreira; Pinheiro; Marques, 2021). Nesse espírito do capitalismo, a vida privada é passível de ser uma mercadoria. O acesso aos dados deste plano muito interessa, por exemplo, às empresas para fazerem ações de marketing direcionado de acordo com o comportamento individual do consumidor (Ferreira; Pinheiro; Marques, 2021). Em motores de busca, dados são rastreados por meio de cookies visando identificar o comportamento dos usuários e torná-los alvo de publicidade.

Amaral (2003) define assim, direito à privacidade como aquele que assegura aos indivíduos a não divulgação de informações contidas em documentos de carácter pessoal ou privado por um período previamente estabelecido, durante o qual o documento está sujeito a autorização especial de consulta. Para Alves *et al.* (1993) o direito à privacidade é a garantia de que os dados, informação e/ou documentos de carácter pessoal ou privado constantes dos arquivos estarão sujeitos a restrição de comunicabilidade por um período previamente estabelecido, durante o qual caberá ao(s) próprio(s) visado(s) ou aos seus legítimos sucessores qualquer autorização

especial de consulta. Fica claro que a privacidade e a proteção de dados pessoais andam de mãos dadas. Desta feita, o Arquivo Nacional (2005) define proteção de dados como procedimentos derivados de legislação específica, que objetivam impedir o acesso de pessoas não autorizadas a informações sigilosas ou relativas à privacidade de outrem.

Portanto, o direito à proteção de dados tornou-se, com a introdução desse direito na Constituição de vários países, um direito fundamental que protege os cidadãos contra o processamento ilegal e não consensual de dados pessoais por empresas e administrações públicas. Processamento que pode e geralmente ocorre no exercício das funções dessas instituições e, portanto, afeta os documentos de arquivo nos quais esse exercício é documentado (Cuesta, 2012).

Cuesta (2012) acrescenta que esses documentos são arquivados, onde continuam a ser processados para fornecer informações tanto à própria administração que os produziu quanto aos cidadãos e são mantidos como prova da atividade administrativa e do patrimônio documental. Diante disso, Cuesta considera os arquivos como grandes depósitos de dados pessoais e, portanto, sujeitos à legislação de proteção de dados. Assim, “os arquivos podem ser chamados a adquirir um peso importante como agentes destinados a proteger os dados pessoais processados pela administração” (Cuesta, 2012, p. 46).

Por meio da proteção de dados pessoais, avança Doneda (2011), garantias relacionadas à privacidade passam a ser vistas de forma mais alargada, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais.

Garcia (2018) recorre à João Carlos Zanon para pontuar o seu entendimento de que a proteção dos dados pessoais é um direito autônomo em relação ao direito à privacidade, indicando que o direito de proteção aos dados pessoais pode ser o agrupamento de outros direitos, como:

- a) Direitos à informação, compreendendo: direito de informação sobre a coleta (quando, o quê, como e por quem o dado pessoal foi coletado); direito de informação acerca dos responsáveis pelo banco de dados; direito de acesso ao banco de dados; direito de ciência da finalidade do tratamento dos dados pessoais; direito de informação sobre a divulgação dos dados pessoais a terceiros; direito de informação; direito de informação que acerca dos direitos que assistem o titular dos dados; e direito de informação sobre a existência do banco de dados;

- b) Direito de controle, abrangendo: direito de retificação; direito de anotação; direito de apagamento ou ao esquecimento; direito de bloqueio; e de direito de saída;
- c) Direitos à abstenção, compostos por: direito de oposição ao tratamento dos dados pessoais; direito de impedir o tratamento de dados sensíveis; direito de impedir e revistar decisões individuais automatizadas; direito ao tratamento confidencial dos dados pessoais;
- d) Direito de indenização: direito de ser indenizado por danos materiais e morais originados em razão da coleta, do tratamento ou de divulgação dos dados pessoais a terceiros, independentemente de culpa, em regime de responsabilidade civil aplicável para atividade potencialmente perigosa conforme previsto no Código Civil, art. 927, parágrafo único (Garcia, 2018, p. 21).

Como estamos a ver, para além de questões técnicas, tecnológicas, organizacionais e políticas, a proteção de dados pessoais acarreta aspectos legais. Deste modo, foram criados com o passar do tempo, em diferentes ordenamentos jurídicos, vários documentos de direito, com o propósito de proteger a vida privada dos indivíduos. Ferreira, Pinheiro e Marques (2021) apontam que o primeiro instrumento internacional a tratar do direito à privacidade foi a Declaração Americana dos Direitos e Deveres do Homem de 1948. Ela visava proteger os direitos essenciais da pessoa humana.

A Assembleia Geral das Nações Unidas aprovou, no mesmo ano, a Declaração Universal dos Direitos Humanos (DUDH), que estabelece em seu Artigo 12º que “Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques” (Nações Unidas, 1948). Sobre estes instrumentos e outros mais no mundo e no Brasil, assim como em Moçambique, nós abordaremos em maior detalhe mais adiante. Contudo, é oportuno apontar de forma geral, o que orienta as diferentes normativas que foram sendo sancionadas ao longo dos tempos.

Em geral as normativas identificam quatro cruciais atores na proteção de dados pessoais, o titular dos dados, agentes de tratamento (controlador de dados e operador de dados) e encarregado de dados. O titular de dados é “o sujeito de direito que cede dados ao controlador e ao operador” ou ainda “sujeito de direito produtor de dados” (Fornasier; Knebel, 2021, p. 1005). O controlador de dados é “quem toma as decisões relativas às operações de dados”, o operador de dados é “quem realiza o tratamento de dados” (Fornasier; Knebel, 2021, p. 1022). Ambos, o controlador e operador, são agentes de tratamento, pois são os que realizam a coleta, o uso, o compartilhamento

ou outra atividade com os dados pessoais. São pessoas naturais ou jurídicas, públicas ou privadas, que tratam dados pessoais (Autoridade Nacional de Proteção de Dados, s.d.). O encarregado de dados é “quem faz a comunicação entre controlador e operador” (Autoridade Nacional de Proteção de Dados, s.d.).

O modelo jurídico adotado por diversos países para a proteção dos dados pessoais consiste, como nos mostra Mendes (2019), em uma proteção constitucional, por meio da garantia de um direito fundamental e por meio de um regime legal de proteção de dados, na forma de uma lei geral. No Brasil, por exemplo, foi adotado o modelo de lei geral, a Lei Geral de Proteção de Dados. É, portanto, “o exercício do poder do Estado para intervir no processamento de dados, buscando estabelecer fluxos adequados de informação na sociedade, de modo a proteger tanto a coletividade como os direitos fundamentais dos cidadãos” (Mendes, 2019, p. 36).

Doneda (2011), considerando alguns instrumentos que orientam a proteção de dados pessoais e analisando uma série de legislação, sintetiza um conjunto de princípios a serem aplicados na proteção de dados pessoais. Como ele aponta, esses princípios formam a espinha dorsal das normativas em matéria de proteção de dados pessoais, formando o núcleo das questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema (Doneda, 2011).

O Princípio da publicidade ou da transparência obriga que a existência de um banco de dados com dados pessoais seja de conhecimento público; o princípio da exatidão orienta que os dados armazenados sejam fiéis à realidade, significando sua coleta e tratamento cuidadoso e possibilidade de correção, de como atualizações periódicas, conforme a necessidade; pelo princípio da finalidade qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. com base neste princípio são restringidas transferências de dados pessoais a terceiros, mas também serve para estruturar um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade; o princípio do livre acesso determina que o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, e igualmente controlar esses dados; pelo princípio da segurança física e lógica os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado (Doneda, 2011).

Beckles (2014) compreende que, de acordo com os princípios de proteção de dados, os documentos contendo dados pessoais devem ser processados de forma justa e legal, entendendo-se isto como a garantia de que todos os aspectos da normativa e do próprio titular dos dados estarão salvaguardados. Isto implica também que o design do documento em que as informações pessoais estarão registradas, não induzirá o usuário ao erro, de modo que ele saiba como os dados serão usados pelo controlador de dados e dê consentimento para qualquer compartilhamento dessas informações antes de serem colocadas no sistema. A autora compreende ainda que, de acordo com os princípios, é obrigação dos controladores de dados garantir que todas as informações em seus sistemas de gestão de documentos sejam atuais e/ou que as informações estejam atualizadas, podendo ser feito por meio da verificação periódica dos documentos nos sistemas, pois, informações imprecisas podem fazer com que a organização viole os direitos e prerrogativas de um titular de dados. Mas também “a organização será ineficaz na tomada de boas decisões ao usar dados imprecisos, o que resultaria em um gerenciamento deficiente dos assuntos de seus clientes” (Beckles, 2014, p. 242).

Atenta aos princípios, Beckles (2014) continua fazendo a sua leitura, entendendo que eles dizem respeito à garantia de medidas de segurança na manutenção de dados pessoais e por isso, devem ser consideradas as informações pessoais acessadas remotamente por meio de smartphones, tablets, laptops, etc. Ela considera que a criptografia desses dados seria uma medida útil para protegê-los em caso de furto ou roubo. A autora chama atenção para que os documentos com dados pessoais nunca sejam deixados sem supervisão em qualquer formato e que o pessoal que trabalha com esses documentos deve ser cuidadosamente selecionado, com seus contratos de confidencialidade assinados como uma medida adicional (Beckles, 2014).

Outro aspecto que Beckles denota considerando os princípios de proteção de dados, é que os documentos que contêm dados pessoais não devem ser mantidos por mais tempo do que o necessário. Isso significa que, desde o início, a gestão de documentos, em conjunto com os setores ou serviços em que são produzidos estes documentos, deve determinar por quanto tempo um documento com dados pessoais deve ser mantido no sistema com base no objetivo e na intenção declarados do documento. “Se os documentos forem de arquivo para a organização e forem retidos

para fins de pesquisa, outras medidas deverão ser tomadas para proteger os dados pessoais contidos neles” (Beckles, 2014, p. 243).

Também sem ignorar esses princípios, Mendes formula um modelo de aplicação da LGPD em três níveis:

- a) Qualquer tratamento de dados pessoais somente pode ser iniciado se atendidas as condições para a sua legitimidade (condições de legitimidade);
- b) Atendidas as condições de legitimidade, todo o tratamento de dados deve cumprir determinados procedimentos, que se encontram na Lei tanto na forma de direitos do titular como de obrigações dos agentes de tratamento (procedimentos para garantir a proteção de dados pessoais); e
- c) Em caso de violação a esse direito, são aplicáveis sanções administrativas e civis (sanções e reparação) (Mendes, 2019, p. 47).

Esse modelo, entre outros aspectos, deixa claro que, em caso de descumprimento das condições de legitimidade de tratamento ou dos procedimentos para a proteção dos dados pessoais, os agentes de tratamento ficam sujeitos às sanções administrativas e ao pagamento de indenização ao titular (Mendes, 2019).

Para além dos princípios que norteiam as normativas de proteção de dados pessoais, essas normativas, regra geral, atribuem direitos básicos aos titulares dos dados. Conforme Mendes (2019), esses direitos são conhecidos pela sigla ARCO, abreviação de Acesso, Retificação, Cancelamento e Oposição. Pois, entende-se que o titular deve ter livre acesso aos seus dados, deve poder corrigir dados equivocados e desatualizados e deve poder cancelar dados que foram indevidamente armazenados ou cujo consentimento tenha sido revogado por ele (Mendes, 2019, p. 50).

Na seção que se segue, são revisitados os conceitos de Arquivologia e de Arquivista, colocando-os, num primeiro momento, diante dos seus princípios e diante da ética profissional, respectivamente. E num segundo momento, procurando identificar o papel deste profissional de informação na proteção de dados pessoais.

4 A PROTEÇÃO DE DADOS PESSOAIS DESDE UMA PERSPECTIVA ARQUIVÍSTICA

Nesta seção, num primeiro momento revisitamos a definição de a Arquivologia e seus princípios, passando pela definição de arquivista (identificando o seu papel na e para a proteção de dados pessoais) e num segundo momento discutimos a proteção de dados pessoais face aos princípios arquivísticos.

4.1 A Arquivologia, seus principais princípios e teoria

A Arquivologia nascida da Europa do século XIX, chega ao século XXI como um campo de saber fortalecido por várias modificações teórico-práticas. Nos elementos que lhe fundam, a Arquivologia é marcada pelas características nacionais do Estado moderno europeu. Seus desdobramentos específicos têm lugar em contextos histórico-culturais diversos (Jardim, 2015).

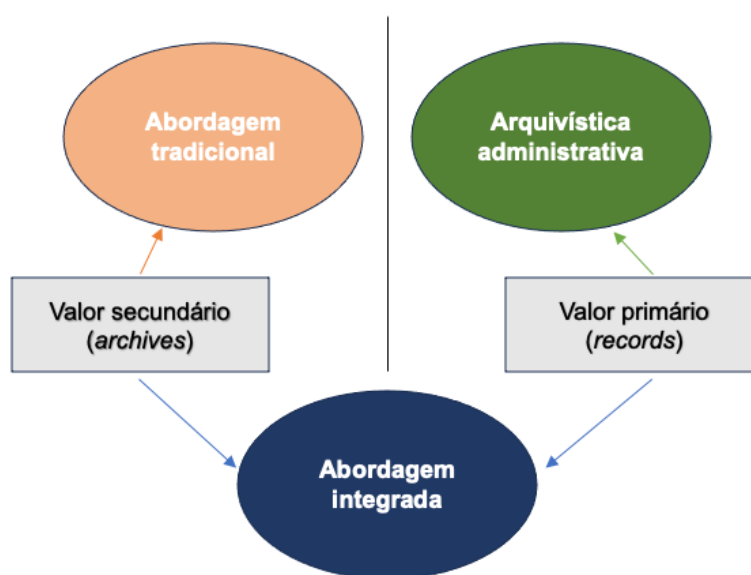
A prática da Arquivística, como apontam Rousseau e Couture (1998), está intimamente ligada à existência dos arquivos. Contudo, o trabalho em torno de um objeto e o aparecimento dos princípios arquivísticos, constituem um fenômeno contemporâneo, apontam os autores. Ou como diz Heredia Herrera (1991, p. 29, tradução nossa) “a Arquivística é a ciência dos arquivos, não dos documentos, embora, em última análise, os últimos sejam o produto integral dos primeiros”. A autora continua,

Ela lida com a criação, a história, a organização e o serviço dos arquivos para a Administração e para a História, em suma, para a Sociedade. É a ciência que estuda a natureza dos arquivos, os princípios de sua preservação e organização e os meios de sua utilização.” Seu objeto não é apenas o arquivo no singular, como algo concreto cujos limites estão em seu conteúdo e em seu recipiente, mas também o conjunto de arquivos integrados em um sistema com todos os problemas que isso implica (Heredia Herrera, 1991, p. 29-30, tradução nossa).

Segundo Cunha e Cavalcanti (2008), a Arquivística refere-se à princípios e técnicas a serem seguidos na constituição, organização, gerência, desenvolvimento e utilização de arquivo, abarcando aspectos legais e regulamentares dos arquivos, sendo que por sua natureza, responde às necessidades dos organismos e/ou dos indivíduos que criam os documentos.

As perspectivas apresentadas acima, levaram Rousseau e Couture (1998) a perceber que a Arquivística pode ser abordada de três maneiras: uma, unicamente administrativa, cuja principal preocupação é ter em conta valor primário do documento (*records management*); uma maneira tradicional que põe a tônica exclusivamente no valor secundário do documento; ou, por último, uma maneira integrada e englobante que se ocupa simultaneamente do valor primário e do valor secundário do documento, conforme a figura que se segue.

Figura 3 – Abordagens sobre Arquivística em Rousseau e Couture (1998)



Fonte: Adaptado de Rousseau e Couture (1998).

Atentas à figura 3 e à semelhança dos autores aqui citados, nós nos orientamos por esta terceira ótica, contudo no âmbito desta tese, colocamos maior enfoque nos documentos de valor primário. Rousseau e Couture (1998) defendem que a ótica da Arquivística Integrada é a que permite assegurar a unidade e a continuidade das intervenções no âmbito de uma política de arquivos, implicando o atingir de três objetivos essenciais à sua viabilidade:

garantir a unidade e a continuidade das intervenções do arquivista nos documentos de um organismo e permitir assim uma perspectiva do princípio das três idades e das noções de valor primário e de valor secundário; permitir a articulação e a estruturação das atividades arquivísticas numa política de arquivos; integrar o valor primário e o valor secundário numa definição alargada de arquivo (Rousseau; Couture, 1998, p. 70).

Heredia Herrera (1991) percebe que o escopo da Arquivística abrange muitos aspectos diferentes. Dentre eles destacamos: a elaboração, estudo e aplicação dos

princípios relacionados, em primeiro lugar, à organização em todos os seus estágios e, em segundo lugar, à descrição em todas as suas manifestações, abrangendo documentos textuais, bem como documentos cartográficos, audiovisuais, eletrônicos e/ou digitais, etc; a gestão de documentos e administração de arquivos, desde a racionalização da produção documental, transferências e expurgos, até serviços, acesso e controle de informações e usuários, e disseminação por todos os meios e em todos os aspectos, e; a história dos arquivos, da evolução da prática arquivística, da legislação em diferentes países e das instituições e organizações internacionais em relação ao desenvolvimento dos arquivos (Heredia Herrera, 1991).

Para além do escopo, a autora debruçou-se sobre o objeto da Arquivística. Para ela constitui objeto da Arquivística os arquivos, entendidos como um conjunto de documentos portadores de informação (conteúdo), que constituem o foco principal dela, tornando-os seu objeto, embora não se esqueça da materialidade do recipiente, ou seja, os edifícios, as instalações, na medida em que tenham a ver com sua conservação. A autora não perde de vista a tripla dimensão do objeto da Arquivística e sua ordem: arquivos, documentos de arquivo e informação (Heredia Herrera, 1991). Ela explica:

Os arquivos e as informações são inseparáveis, pois os arquivos são compostos de documentos e os documentos são portadores de informações. Não pode haver arquivos sem documentos, mas pode haver documentos sem arquivos. Os documentos fazem parte do patrimônio documental, fazem parte dos arquivos e repositórios documentais, podem estar soltos ou agrupados em fundos e coleções. A relação íntima entre arquivos, documentos e informações estabelece uma dimensão tripla no objeto da ciência arquivística (Heredia Herrera, 199, p. 121, tradução nossa).

Diante do objeto da Arquivística, importa, antes de mais, lembrar algumas características, ou propriedades, ou ainda qualidades de documentos de arquivo, identificadas por Duranti (1994). São elas: imparcialidade, autenticidade, naturalidade, inter-relacionamento e unicidade. A figura 4 na página seguinte, representa estas características.

Como se pode depreender, as propriedades ou qualidades dos documentos de arquivo, tem relação intrínseca com os princípios arquivísticos. Ora, a naturalidade e a unicidade, em particular, podem ocorrer noutros textos como princípios, tal é o caso de Fernal e Vechiat (2021).

Figura 4 – Características de documentos de arquivo em Duranti (1994)



Fonte: Elaborado pela autora

Esta ciência, a Arquivologia, tem objeto e também princípios. Estes princípios que se entrelaçam, orientam toda a *praxis* arquivística, desde os aspetos mais específicos da produção dos documentos de arquivo, passando pela proteção de dados pessoais, até ao acesso ou a eliminação destes documentos. Ora, cientes das nossas limitações para discutirmos todos os princípios arquivísticos e com a devida profundidade que demandam, nesta seção são discutidos àqueles que entendemos serem fulcrais para a compreensão da nossa tese.

Neste contexto, Rousseau e Couture (1998) apontam que existem três princípios que constituem o fundamento da Arquivística e que são utilizados desde o final do século XIX, o princípio de proveniência (que comporta duas vertentes, uma tida como princípio de ordem original), o princípio de territorialidade e o princípio, chamada também, abordagem ou teoria das três idades. Embora Rousseau e Couture (talvez por tomarem como uma característica) não apontem a organicidade com um dos principais princípios da Arquivologia, diferentes autores o fizeram.

Começaremos a nos debruçar sobre os princípios arquivísticos a partir deste último, o princípio da organicidade. Troitiño (2023) define organicidade como os vínculos que se estabelecem entre as unidades documentais e seus pares, numa relação que integra documentos, elementos estruturais e elementos funcionais, dentro de um arquivo. A organicidade, avança Troitiño (2023), está no núcleo do conceito de

proveniência e é somente possível identificar a relação orgânica entre documentos, quando se referem a unidades de um mesmo fundo. Troitiño (2023) entende igualmente que a organicidade é resultado da naturalidade na produção de documentos arquivísticos. Portanto, “consequência lógica das atividades de uma determinada entidade” (Troitiño, 2023, p. 52).

O princípio de proveniência é atribuído à Natalis de Wailly, chefe da seção administrativa dos arquivos departamentais do ministério do interior da França que, em 1841, inspirou a circular que promulgou que a partir daquela data, “os documentos que provenham de um corpo, de um estabelecimento, de uma família ou de um indivíduo deverão ser agrupados” e não misturados com outros que tenham provenham de corpo distinto (Rousseau; Couture, 1998, p. 52). Este princípio comporta dois níveis ou duas vertentes ou ainda dois graus, segundo Rousseau e Couture (1998) e define-se como o princípio segundo o qual os arquivos de uma mesma proveniência não devem ser misturados com os de outra e devem ser conservados conforme a sua ordem primitiva, ou define-se como “o princípio segundo o qual cada documento deve ser colocado no fundo donde provém, e nesse fundo, no seu lugar de origem” (Rousseau; Couture, 1998, p. 82).

Heredia Herrera o define como

O princípio segundo o qual cada documento deve ser localizado no acervo documental do qual se origina, e nesse acervo em seu local de origem. Além disso, todos os documentos são produzidos em uma ordem sequencial, lógica e natural. Essa origem e essa ordem não são outra coisa senão a consequência da natureza jurisdicional do arquivo e de seus fundos (Heredia Herrera, 1991, p. 34, tradução nossa).

As duas vertentes ou dois graus do princípio de proveniência indicados por Rousseau e Couture (1998) referem-se, primeiro “a considerar o fundo de arquivo como uma entidade distinta” e segundo, “exige que todos os documentos de um fundo de arquivo ocupem um determinado lugar que tem de ser respeitado ou restabelecido, caso a ordem primitiva ou a ordem original tenha sido modificada por qualquer razão” (Rousseau; Couture, 1998, p. 83).

Troitiño (2023) aponta que a concepção de ordem original abarca o entendimento de que a organização conferida pela entidade representada no fundo deve ser mantida, refletindo a acumulação de documentos durante a atuação de determinada administração. A autora explica:

sentido de ordem original vai além da simples manutenção das peças documentais nos lugares onde foram encontradas. Vincula-se a uma lógica muito mais profunda e essencial. Diz respeito à preservação do sentido fornecido pelas estruturas e funções, durante a produção e ao longo do uso dos documentos de arquivo, em dada administração (Troitiño, 2023, p.48)

Diante dos graus ou vertentes do princípio de proveniência, na perspectiva de Rousseau e Couture (1998), Troitiño (2023) entende que

[...]essa duplicidade de valores referenciais, representados pelo princípio da proveniência e pelo princípio da ordem original ou, simplesmente, princípio do respeito aos fundos, constitui questão-chave na Arquivologia. Entretanto, um ponto de intersecção [...], é a circunstância de a origem dos documentos de arquivo configurar eixo central e estruturante da proposição do conceito de fundo (Troitiño, 2023, p.44).

Duchein (1986) apontou exemplos interessantes no que toca a dificuldade de definir o fundo em relação à hierarquia dos organismos produtores. Ele considera fácil definir fundos de arquivo de uma abadia, de um hospital, ou de um tribunal. Mas considera complexa e difícil a definição de fundo de um Ministério, por exemplo, pois este é um todo grande corpo administrativo, está dividido em grandes setores de atividades, e têm cada um destes, suas próprias competências que correspondem a conjuntos de documentos mais ou menos individualizados. O autor questiona, neste contexto, se podemos falar de fundos de arquivo do Ministério ou de fundos das Direções ou dos fundos dos gabinetes? Para ajudar a responder as perguntas que ele próprio levanta, o autor alista 5 critérios para a definição de fundos, a saber:

- 1) [...] Um organismo que seja público ou privado deve possuir um nome e uma existência jurídica própria resultante de uma ata, lei, decreto etc. preciso e datado.
- 2) Deve possuir atribuições precisas e estáveis, definidas por um texto tendo valor legal e regulamentar.
- 3) A sua posição no seio da hierarquia administrativa deve ser definida com precisão pela ata que lhe deu origem em particular a sua subordinação a outro organismo de nível mais elevado deve ser claramente conhecido.
- 4) Deve ter chefe responsável, beneficiando do poder de decisão correspondente ao seu nível hierárquico, ou seja, ele deve tratar dos trabalhos da sua competência sem tê-los que submeter automaticamente por decisão a uma autoridade superior.
- 5) A sua organização interna deve, tanto quanto possível, ser conhecida e fixada num organograma (Duchein, 1986, s.p.)

Troitiño (2023, p.49) recorre a María Paz Martín-Pozuelo Campillos (1996) para apontar o nome defendido por esta autora como ideal para esse princípio, “*respeito à estrutura original dos fundos*” e à “*ordem natural dos documentos*”, (Campillos, 1996 *apud* Troitiño, 2023, p.49). Através desta autora, Troitiño aponta que este princípio contempla, por um lado, a finalidade de respeitar as estruturas e funções originadas

pelo titular do fundo, e por outro lado, contempla a finalidade de observar a acumulação dos documentos de uma mesma administração.

Rousseau e Couture (1998) entendem também que este princípio permite ter em conta a natureza dos documentos a tratar. Quer dizer, a decisão de conservar os documentos no meio que os viu nascer (primeiro grau do princípio) e no lugar exato que nesse momento lhe foi atribuído (segundo grau do princípio) tem muito mais em conta a natureza dos documentos e as particularidades de funcionamento do organismo a que eles dizem respeito (Rousseau; Couture, 1998).

O princípio de territorialidade “relewa do Direito aplicado à propriedade” e define-se como sendo o “princípio segundo o qual os arquivos públicos, próprios de um território, seguem o destino deste território” (Rousseau; Couture, 1998, p. 52).

Troitiño (2023) defende que a aplicação do princípio de territorialidade pode ser vista como a prática de colocar documentos com conteúdo relevante para uma região em um repositório, dentro da própria região e a importância do uso deste princípio, continua a autora, está intimamente ligada às funções operacionais e memoriais dos documentos de arquivo, inerente à localização geográfica do arquivo de origem, o que significa que, desfazer vínculos de territorialidade é desconectar o documento de suas funcionalidades primordiais.

À semelhança do princípio de proveniência que tem seu desdobramento, o princípio de territorialidade aplica-se a três níveis: nacional, regional e institucional. Segundo os autores

no nível nacional, os Estados soberanos servem de ponto de referência ao princípio de territorialidade, estes têm de proceder a intercâmbio de arquivos entre si, aquando de sucessões de Estados. No nível regional, a aplicação deste princípio difere pouco do nacional, estando eles assentes em entidades geográficas ou administrativas. Este nível difere-se do nacional pelo facto de delimitar melhor o lugar de produção de um fundo. O nível institucional é aquele que advoga que os arquivos sejam conservados o mais perto possível do lugar da sua criação e a sua aplicação significa que eles devem ser guardados pela instituição que os criou (Rousseau; Couture, 1998, p. 87-89).

Portanto, este princípio incide na capacidade de governança de uma Administração e reflete o conceito de domicílio legal do documento que é a condição jurídica específica, firmada em consonância ao princípio da proveniência, como coloca Troitiño (2023), ao levantar, neste contexto, a noção de jurisdição arquivística, definida por ela como a competência legal para a administração e gestão de documentos de

uma organização, pela entidade que lhe corresponda, em termos de propriedade ou custódia. A autora chama atenção a falta de clareza para a determinação do direito de propriedade, a partir do vínculo designativo da relação existente entre origem e custódia.

Apoiada ao termo pertinência territorial, Troitiño (2023) conclui que, refletir sobre a pertinência, relevância ou pertencimento dos documentos à sua origem leva a compreender sobre valores congênitos presentes nesses documentos, aos signos de identidade.

Por sua vez, a teoria das três idades nos leva a passar pelo entendimento da diferença entre *records* e *archives*. Como nos recorda Bittencourt (2022), ao longo da história os arquivos eram formados com enfoque no valor probatório associado à manutenção dos deveres dos subalternos e manutenção dos direitos e privilégios daqueles que detinham o poder. A autora relata que

no momento em que os arquivos deixam de servir somente aos seus produtores e são percebidos como fonte de conhecimento para a história da sociedade, cria-se uma separação que pode ser reconhecida como uma primeira base do que futuramente viria a ser as três idades nos arquivos. Esta separação, entre os documentos que serviam à administração e os arquivos que serviam à história, cumpriu o entendimento do que viriam, mais tarde, a ser dois dos três estágios, da teoria das três idades — o arquivo corrente que serve à administração e o arquivo permanente como o que serve à compreensão histórica, ou como se conhece na língua inglesa, os *records* e os *archives* (Bittencourt, 2022, p.175)

A teoria das três idades ganha, portanto, expressão nos Estados Unidos com raízes nas reflexões que os arquivistas e os *records managers* tiveram de fazer para resolver os problemas de massa documental, no início do séc. XX. Esta teoria assenta-se nas etapas de vida dos documentos, onde “na idade ativa, o documento serve regularmente para a administração; na idade semiativa, é utilizado ocasionalmente, e na idade inativa é destruído ou conservado de modo permanente” (Rousseau; Couture, 1998, p. 53).

Heredia Herrera (1991) debruçou-se sobre estas idades ou estágios. Para a autora, no primeiro estágio ou idade, os documentos fazem parte dos arquivos setoriais, correntes ou gerenciais. Estão próximos ao funcionário responsável por seu processamento (em sua mesa, armários de arquivo de fácil acesso para manuseio frequente, etc.). No segundo estágio ou idade, o documento que testemunhou a resposta ou solução da razão de sua produção deve continuar a ser mantido e pode

ser consultado ou mencionado como informação de base, sem a mesma frequência do primeiro estágio. Corresponde a um arquivamento intermediário no qual o valor primário diminui gradualmente e seu valor secundário se desenvolve. No terceiro estágio ou idade o documento assume um valor permanente e será consultado por seu valor cultural e informativo. Seu arquivamento e preservação serão definitivos (Heredia Herrera, 1991).

Bellotto (2006) traz um pouco mais de detalhe em relação às idades e indica, a primeira é a dos arquivos correntes, nos quais se abrigam os documentos durante seu uso funcional, administrativo, jurídico, sua tramitação legal, sua utilização ligada às razões pelas quais foram produzidos. A permanência de tais documentos nesse tipo de arquivo, pode ser generalizada em um ano e podem passar dali a um arquivo central do respectivo órgão produtor onde permanecerão de cinco à dez anos. A segunda idade, é a do arquivo intermediário, onde os documentos já ultrapassaram seu prazo de validade jurídico-administrativo, mas ainda podem ser utilizados pelo produtor. Permanecerão em um arquivo que já centraliza documentos de vários órgãos, porém sem misturá-los pelo prazo máximo de 20 anos. Assim, abre-se a terceira idade, geralmente aos 25 ou 30 anos, contados a partir da data de produção dos documentos ou do fim de sua tramitação. O recolhimento conduz aos arquivos permanentes (Bellotto, 2006). A autora acrescenta que a localização física dos arquivos correspondentes às três idades demonstra suas especificidades. O primeiro deve situar-se junto ao produtor, o segundo pode estar em local afastado, é um depósito onde os documentos aguardam seus prazos de vida ou seu recolhimento. O terceiro deve estar localizado junto às universidades ou aos centros culturais, deve situar-se em lugares de fácil acesso para seus usuários típicos.

É oportuno apresentar aqui uma recomendação feita por Paes em 2004. A autora apontou que o arquivo intermediário deve ser subordinado técnica e administrativamente ao arquivo permanente, de modo que se evite a criação descontrolada de depósitos e como forma de manter uniforme a política arquivística. Nessa ordem de ideia, a autora defende então que esse arquivo seja dirigido por arquivistas de alto nível que conhecem os métodos de classificação e elaboração de instrumentos de pesquisa.

Ao terminarmos, sem esgotar a discussão que se levanta nesta subseção, gostaríamos de esclarecer que os princípios de que tratamos aqui, eles atravessam

aquelas que são as funções arquivísticas: produção, avaliação, aquisição, conservação, classificação, descrição e difusão (Rousseau; Couture, 1998). Para maior clareza, observe o quadro a seguir.

Quadro 3 – Princípios e funções arquivísticas

Princípios arquivísticos	Funções arquivísticas	Finalidade
Organicidade Proveniência Territorialidade Teoria das Três Idades	Produção	Elaboração dos documentos
	Avaliação	Definição de prazos; identificação de valores; controle; tabela de temporalidade
	Aquisição	Transmissão da propriedade dos documentos; custódia
	Conservação	Manutenção dos documentos; preservação
	Classificação	Visualização das funções e atividades do produtor; plano de classificação
	Descrição	Estabelecimento de relações dos documentos; elaboração de instrumentos de pesquisa
	Difusão	Divulgação e acesso público

Fonte: Elaborado pela autora.

O quadro acima, ilustra que as sete funções arquivísticas, como as sete atividades no coração da Arquivologia, elas acontecem respeitando os princípios arquivísticos. Seja qual for a função, ela será permeada pelos princípios arquivísticos existentes, concomitantemente. Em conjunto, os princípios e as funções, tem bastante a subsidiar na proteção de dados pessoais, desde a produção dos documentos à difusão os mesmos.

A subseção que segue coloca no centro da discussão, o arquivista e a ética profissional, partindo do pressuposto de que esse arquivista é conhecedor e está munido dos princípios arquivísticos para lidar com a proteção de dados pessoais.

4.2 O Arquivista e a ética profissional

Do triângulo Arquivo-Arquivologia-Arquivista, já discutimos sobre os dois primeiros vértices com algum resquício do terceiro ou pelo menos, não discutido na especialidade. É, por isso, importante deixar às claras a quem nos referimos quando falamos deste profissional de informação. Paes (2004) apresentou na sua obra, uma seção sobre a terminologia arquivística, onde ela forneceu uma diversidade de termos

e dentre eles “arquivista”, definindo como “profissional de arquivo, de nível superior” (Paes, 2004, p. 24).

Para Cunha e Cavalcanti (2008) arquivista é um especialista encarregado de uma ou várias funções na gestão de arquivos. Também o definem como um profissional responsável por analisar e organizar documentos, públicos e/ou privados, organizando-os tendo em conta a sua origem e outros critérios, tratando-os tecnicamente e arquivando-os adequadamente, permitindo a sua recuperação eficiente, facilitando sua consulta e evitando sua deterioração (Cunha; Cavalcanti, 2008).

O trabalho do arquivista baseia-se em conhecimentos teóricos e práticos, como nos fala Heredia Herrera (1991), adquiridos ao longo de muitos anos de estudo e de aprendizagem, mas sempre suscetíveis de revisão. Heredia Herrera vê essa formação sob dois pontos de vista: “uma preparação geral para qualquer arquivista no momento da sua entrada e uma especialização” (Heredia Herrera, 1991, p. 217, tradução nossa).

Ao refletir sobre a ética, McGarry (1999), fala que as profissões surgiram com certas características substantivas, estruturais e filosóficas. As substantivas compõem o corpo específico de aptidões que a profissão alega possuir, dita competência exclusiva. Estas estão abertas à constante avaliação e adaptação às necessidades sociais em mudança; constitui também um currículo, que deve ser incisivo tanto para inculcar valores quanto ao capacitar no uso de técnicas e informação, para a formação de futuros profissionais. As estruturas são autónomas, coletivas e meritocráticas. Conferem a autoridade necessária para regulamentar seus procedimentos, impor disciplina e proporcionar o desenvolvimento intelectual de seus membros (McGarry, 1999, p. 183). As filosóficas compreendem a razão da existência da profissão. Sua orientação para a comunidade, ideias de serviço prestados à sociedade e sua relação com outros profissionais (McGarry, 1999, p. 183). Deste modo, quando pensamos na profissão do arquivista, percebemos sua competência exclusiva na gestão de documentos e como isto impacta a proteção de dados pessoais que por sua vez tem um enorme impacto para as organizações e para a sociedade em geral. Claro, o arquivista não trabalha sozinho nesta empreitada. A sua atuação é recheada de relações inter e multidisciplinares.

Heredia Herredia (1991) afirma também que não há formação sem investigação. E defende que é necessário centrar-se no trabalho quotidiano para extrair abordagens gerais de experiências concretas, que podem servir de orientações e modelos. Para ela o essencial é que “a arquivística seja confiada a instituições que disponham dos conhecimentos e dos meios para a ensinar” (Heredia Herrera, 1991, p. 219, tradução nossa). Nesta senda, “quase todos os países reconhecem dois níveis de formação equivalentes a diplomas de nível superior e intermédio: os arquivistas científicos e os arquivistas técnicos” (Heredia Herrera, 1991, p. 221, tradução nossa). Em Moçambique, pelo menos até janeiro de 2025, a formação de arquivistas estava confiada apenas à Universidade Eduardo Mondlane.

Independentemente do nível de formação, a evolução da arquivística exige a colaboração e o conhecimento de outras disciplinas (características filosóficas vistas em McGarry, 1999), sem, contudo, perder a sua personalidade específica. Arquivística, integrada e harmônica, permite a unidade das ações contínuas e sucessivas dos arquivistas, de acordo com as três idades; permite a elaboração de uma legislação que integre as atividades arquivísticas; permite a aceitação de uma definição suficientemente ampla que abranja a gestão, a administração e a investigação (Heredia Herrera, 1991).

É também olhando para a formação do arquivista e para a sua atuação profissional que as questões éticas sobressaem. Quando se analisam os códigos de ética das profissões, percebem-se incorporados neles, os fundamentos da respetiva área. Ora, os princípios que fundamentam o discurso ético são abstratos, mas as decisões éticas são concretas e práticas. (McGarry, 1999). A ética é “um campo muito complexo da filosofia, que imbrica com a religião, política, antropologia e psicologia. Permeia o pensamento em quase todas as áreas da atividade humana” (McGarry, 1999, p. 174).

McGarry (1999) aponta que existem dois pontos de vista que podem ser adotados na ética. A ética do dever ou a visão deontológica, que pode ser resumida como fazer o certo sem se importar com as consequências. E a visão teleológica onde se começa com as consequências e se avalia o valor moral de uma ação pelas consequências que pode causar a outras pessoas (McGarry, 1999). Nos parece que, no que toca às questões de proteção de dados pessoais, o arquivista deve orientar-

se pela visão deontológica, visto a severidade de consequências que podem advir de uma visão diferente.

Aliás, sobre as questões éticas e serviço de informação, o autor aponta que há quatro grandes áreas de interesse: privacidade, exatidão, propriedade e acesso. Ele define privacidade como “a situação em que se está protegido do acesso indesejável por parte de outrem, seja acesso psicológico ou físico, a informações pessoais ou observação indesejável” (McGarry, 1999, p. 184). Dentre diferentes características, aponta que a privacidade inclui a liberdade de não sofrer intromissão indesejável, e a liberdade de tomar decisões racionais sem coerção ou impedimento. Entende-o como um conceito territorial tanto no sentido psicológico como no sentido físico de controle espacial. E afirma que a privacidade é essencial para a preservação da identidade pessoal (McGarry, 1999).

Ora, a coleta de impostos; a destituição de benefícios sociais; segurança pública; o planejamento social e políticas governamentais, todas exigem a apresentação organizada de enorme quantidade de informações, em grande parte de natureza pessoal (McGarry, 1999) Isto quer dizer que, regra geral, as instituições públicas em sua grande maioria, estão repletas de dados pessoais, para ver a sua missão realizada. Contudo, estas mesmas instituições parecem não comunicar as razões da coleta desses dados. Nesta ordem de ideias, McGarry pontua

Se conhecemos quem sabe o quê a nosso respeito, temos uma chance remota de reparação; se desconhecemos quem sabe o quê a nosso respeito, então ficamos realmente muito vulneráveis. A informação pode até nem ser verdadeira. Esses problemas não foram criados pela tecnologia da informação, mas são certamente agravados pela sua capacidade ampliada de vigilância, comunicação, computação, armazenamento e recuperação (McGarry, 1999, p. 185).

O debate a respeito da privacidade tem estado centrado nas amplas possibilidades que existem de ela ser quebrada e invadida, inclusive intrusões no domicílio da pessoa por correspondência não solicitada, publicidade indesejável e o potencial dos computadores de armazenar e disseminar dados (McGarry, 1999). No que chamou de “crises informacionais”, Le Coadic (2019) identifica que um dos desafios nestes cenários é “Não esquecer as considerações éticas” e estima ser “útil perguntar onde traçar a linha entre transparência e privacidade e como integrá-la ao design de sistemas de informação e interfaces” (Le Coadic, 2019, p. 19). Aqui, aliando

a expertise e a ética, o arquivista tem um enorme papel a desempenhar, como veremos na subseção seguinte.

4.3 O arquivista na Proteção de Dados Pessoais

A Declaração Universal Sobre os Arquivos, aprovada na assembleia geral do Conselho Internacional de Arquivos (CIA) realizada em 17 de setembro de 2010, em Oslo e Aprovada na 36ª sessão da Conferência Geral da UNESCO, reconhece o papel dos arquivistas, como profissionais qualificados, com formação apropriada e contínua, que servem às suas sociedades, apoiando a produção, seleção e conservação dos documentos, e os tornam disponíveis para uso (Conselho Internacional de Arquivos – CIA, 2010). Não são apenas qualificados para tornar os documentos acessíveis, como também, em decorrência desse exercício, o arquivista é o profissional apropriado para identificar, junto do produtor dos documentos, aqueles documentos de arquivo que requerem alguma medida de sigilo para o seu acesso, como é o caso de documentos contendo dados e/ou informações pessoais.

Esse trabalho do arquivista recai sobre todo o ciclo vital dos documentos. Ao longo desse ciclo, há paralelamente, uma grande variedade de unidades de trabalho em Arquivística, como apontam Rousseau e Couture (1998). Algumas unidades de trabalho são próprias da Arquivística e revestem-se de um vocabulário consagrado como fundo, série, etc., aliás, como diz Heredia Herrera em seu texto traduzido por Rodriguez, “o vocabulário científico, em nosso caso, o arquivístico, é um importante instrumento quando se trata de definir nossa identidade” (Heredia Herrera; Rodriguez, 2022, p. 100). Outras unidades de trabalho advêm das várias disciplinas das Ciências da Informação, cobrindo realidades distintas. As unidades de trabalho baseiam-se todas na realidade arquivística e situam-se no coração dos seus próprios fundamentos. São elas: o património arquivístico comum; arquivos de Estado; Arquivos de um organismo; Grupo de arquivos; fundo; série; unidade de instalação; peça; documento e dado (Rousseau; Couture, 1998). Ou por outra, segundo Bellotto (2006, p. 30) “há toda uma gama de tarefas sucessivas que cabe ao arquivista

desempenhar ao longo de três fases bem definidas: o controlo dos arquivos em formação, a destinação e a custódia definitiva”.

Bellotto na sua famosa obra *“Arquivos Permanentes: tratamento documental”*, esmerou-se em falar, entre outros assuntos conexos, do arquivista na contemporaneidade. Nesse capítulo ela começou recordando ao arquivista que não poderia esquecer que vive e atua profissionalmente na dita “era da informação” onde as tecnologias de comunicação e informação são muito presentes. Recordá-lhes que os suportes documentais com os quais terá de lidar “exigem conhecimento, competência, métodos e meios de produção, utilização e conservação física especiais” (Bellotto, 2006, p. 299). Portanto, a sua tarefa em prol da proteção de dados pessoais não termina nos documentos ditos tradicionais, pelo contrário, em face das evoluções tecnológicas o arquivista deve estar atento e se reciclando para lidar com documentos de arquivo em diferentes formas e formatos, consequentemente dados pessoais registrados de múltiplas maneiras, devendo o arquivista ter habilidades para lidar com eles e protegê-los.

A autora esclarece que quando se fala do arquivista no século XXI, esperando-se que ele seja “o Senhor das TIC’s” (Bellotto, 2006, p. 301) para um eficiente desempenho de seu trabalho, não se deve esquecer daquelas qualidades esperadas do arquivista com ou sem tecnologia, em qualquer situação, tempo e lugar (Bellotto, 2006). Estas qualidades incluem: a capacidade de análise e síntese, justamente com uma aptidão particular para esclarecer situações complexas e ir ao essencial; capacidade de julgamento seguro; aptidão para tomar decisões sobre questões ligadas à memória da sociedade; abertura às TIC; bom senso para tomar resoluções; adaptação à realidade, às condições de seu tempo e lugar; pragmatismo; curiosidade intelectual; rigor; método; continuidade; capacidade de compreensão e de escuta relativamente ao produtor, ao pesquisador e ao cidadão. “O arquivista deverá estar capacitado profissionalmente para intervir em toda a cadeia do tratamento documental, qualquer que seja o suporte” (Bellotto, 2006, p. 301).

Mas é preciso ter ciência de que as incidências legais no tratamento de documentos são variadas e que sobre esses documentos é preciso agir em conformidade, como alertam Rousseau e Couture (1998). Daí que, por exemplo, o arquivista deverá certificar-se de que os documentos que devem ser produzidos, por

exigência de normativa, estão sendo produzidos de fato e em conformidade com a referida normativa. As normativas também podem exigir a conservação de determinados documentos por um período e prever mecanismos de eliminação. O arquivista deve proceder em conformidade com a normativa e velar para que a organização na qual exerce as suas funções faça o mesmo (Rousseau; Couture, 1998). Isto quer dizer que

O arquivista deve participar, através das suas intervenções, no respeito dos direitos da pessoa. Necessita efetivamente assumir a parte que lhe cabe na organização e tratamento de informação, respeitando as leis de acesso à informação e as que visam a proteção da vida privada (Rousseau; Couture, 1998, p. 263).

Em 1996, Jones-Evans afirmou que a proteção de dados, quer sob a forma informatizada ou manual, estava obviamente no centro da responsabilidade do arquivista e a introdução da legislação sobre proteção de dados tem um impacto na gestão de documentos que proporciona uma oportunidade para elevar o perfil da gestão de documentos como uma função fundamental para todas as organizações. Nestes termos, os arquivistas devem fazer uma avaliação mais detalhada do ambiente legal e regulamentar em que a sua organização opera.

Assim, a legislação pode assumir diferentes formas e os pormenores variam de um país para outro, pelo que, as organizações que operam a nível internacional devem ter em conta a legislação de cada país em causa. As obrigações de produzir ou conservar documentos podem ser impostas por leis ou regulamentos específicos de um determinado sector de emprego ou de uma determinada atividade, bem como pelo âmbito de aplicação como leis sobre a privacidade e leis sobre a liberdade de informação. Em muitos países, são também necessários procedimentos sistemáticos de conservação e destruição de documentos para cumprir a legislação relativa à privacidade ou à proteção de dados (Shepherd; Yeo, 2003).

Por exemplo, um dos objetivos da gestão de documentos é separar os documentos que devem ser colocados no arquivo permanente dos que podem ser eliminados, para garantir o controle e o direito individual de acesso à informação, respeitando as restrições eventuais e temporais para um acesso pleno (Schwaitzer *et al.*, 2021). Os documentos que não contenham dados pessoais ou material confidencial podem ser destruídos de forma menos segura. Jones-Evans (1996) aconselha, em caso de dúvida, a tratar o material como confidencial e a destruí-lo de

forma evidente e a não utilizar o lixo doméstico ou colocar os documentos num contentor de lixo para destruir material identificável e confidencial, uma vez que estes permanecem acessíveis a qualquer pessoa que os encontre.

Em suma, “o arquivista deve ser capaz de assegurar uma organização e um tratamento dos arquivos que tenham em conta normas legais suscitadas pelas leis referentes, direta ou indiretamente, aos arquivos” (Rousseau; Couture, 1998, p. 264). Outrossim, dentro da peculiaridade do documento arquivístico, “todo o processamento que se dê à informação arquivística não pode se afastar dos princípios teóricos básicos da arquivística” (Bellotto, 2006, p. 300). Como dizem Bagatini e Guimarães (2019), um arquivista, como profissional da informação comprometido com o bem-estar social, assume uma atitude preventiva, proativa e de constante alerta em relação às armadilhas que podem colocar em risco os dados pessoais.

Lowry (2020) refere que os arquivistas, pelo menos no seu próprio discurso profissional, podem ser encorajados a entender os dados como documentos. Encarar os dados de tal maneira, recorda-nos que os dados são moldados pelos seus contextos culturais e que a sua utilização e compreensão eficazes só serão possíveis se o conhecimento dos seus contextos for salvaguardado. Ou como referem Schwaitzer *et al.* (2021), reconhecer que os dados, enquanto unidades informacionais, precisam de ser organizados de forma significativa para serem transformados em informação; denota que a informação só é fiável, completa e autêntica quando é registada. Outro ponto relevante é que, após a legislação de proteção de dados, deve-se reconhecer que o arquivista é quem melhor pode compreender que os dados são um elemento intrínseco aos documentos, que requerem tratamento e devem ser eliminados após o término do período previsto em lei, e caso isso não ocorra, o profissional poderá sofrer as penalidades previstas.

Lowry (2020) defende também que a qualidade dos dados depende da qualidade dos documentos originais de onde são retirados. A fiabilidade, a exatidão e a fidedignidade dos documentos determinam a fiabilidade, a exatidão e a fidedignidade dos dados. Acrescenta ainda que documentos mal conservados resultam em dados imprecisos, incompletos ou não verificáveis, o que pode levar as organizações a desperdiçarem recursos na tentativa de processar ou analisar dados de má qualidade. Nestas situações, o governo pode ser induzido a erros e tomar

decisões com base em informações mal embasadas, com consequências potencialmente prejudiciais. Assim, os procedimentos utilizados pelo arquivista são essenciais para o controle e segurança dos dados pessoais detidos por quem oferece ou fornece bens ou serviços e a garantia dos direitos fundamentais resulta da eficácia de um programa de gestão de documentos e do desempenho eficaz do arquivista (Schwaitzer *et al.*, 2021).

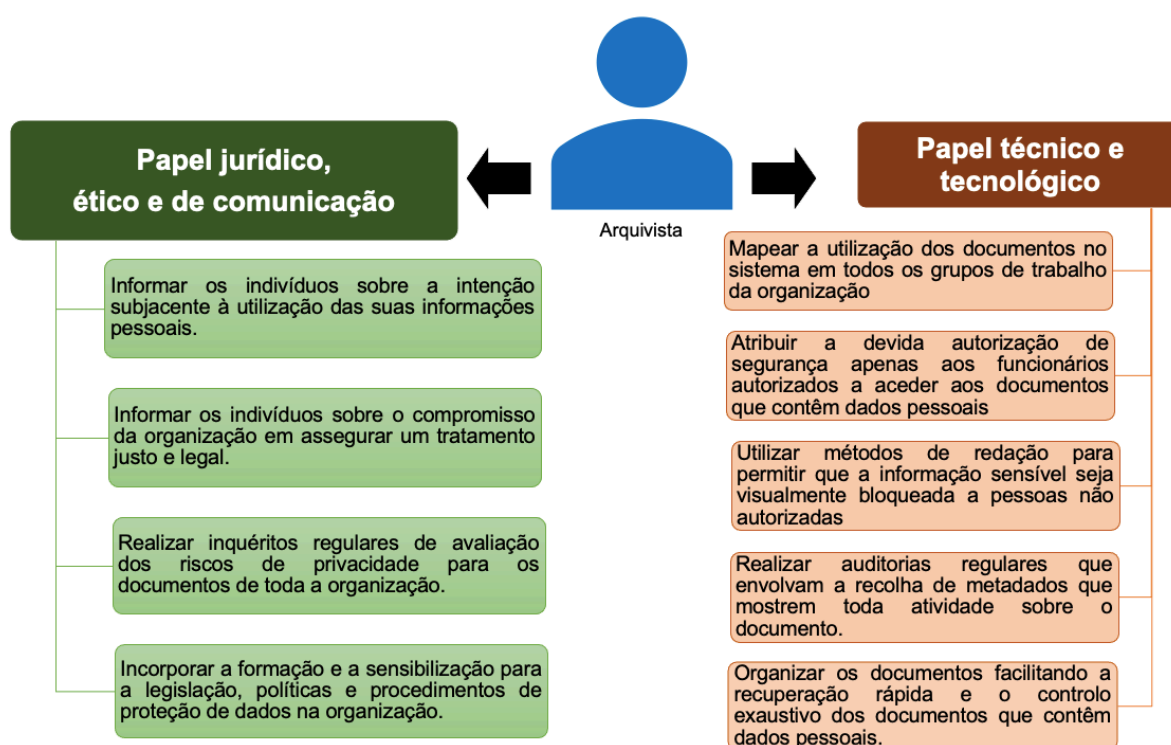
Analisando os trabalhos de Shepherd e Yeo (2003), Beckles (2014) e Schwaitzer *et al.* (2021), bem como os demais trabalhos apontados mais acima, pudemos identificar o papel do arquivista na proteção de dados pessoais. Assim, este profissional tem um papel jurídico, ético e de comunicação através do qual lhe cabe informar os indivíduos sobre a intenção subjacente à utilização das suas informações pessoais e o compromisso da organização em assegurar um tratamento justo e legal; realizar inquéritos regulares de avaliação dos riscos de privacidade para os documentos de toda a organização; e, incorporar a formação e a sensibilização para a legislação, políticas e procedimentos de proteção de dados nos programas de formação do pessoal a todos os níveis, tomando medidas proativas e preventivas.

O Arquivista tem também um papel técnico e tecnológico, pelo qual ele deve mapear a utilização dos documentos no sistema em todos os grupos de trabalho da organização e atribuir a devida autorização de segurança apenas aos funcionários autorizados a aceder aos documentos que contêm dados pessoais; utilizar métodos de redação para permitir que a informação sensível seja visualmente bloqueada a pessoas não autorizadas, permitindo-lhes visualizar a informação solicitada. Para esta tarefa são utilizados programas informáticos para documentos eletrônicos, mas no mundo analógico do papel, o arquivista teria de ocultar manualmente as informações pessoais sobre quaisquer dados sujeitos a proteção de dados antes de os fornecer ao requerente; anonimizar, pseudonimizar e utilizar cifragem, de modo que as pessoas deixem de ser identificáveis. A utilização da encriptação como medida de segurança para proteger dados sensíveis é altamente recomendada quando se armazenam eletronicamente documentos que contenham dados pessoais; estabelecer pistas de auditoria e realizar auditorias regulares que envolvam a recolha de metadados que mostrem quem viu o documento; quem o modificou; em que data foi acedido; quem o imprimiu; quem o retirou do sistema ou quem tentou destruir, alterar ou exportar ilegalmente dados pessoais do documento (eletrônico); deve procurar organizar os

documentos de modo a facilitar a recuperação rápida e o controlo exaustivo dos documentos que contêm dados pessoais, concebendo sistemas de classificação.

A figura 5 ilustra estes dois principais papeis do arquivista na proteção de dados pessoais.

Figura 5 – O arquivista na proteção de dados pessoais



Fonte: Elaborado pela autora.

Portanto, conforme ilustra a figura 5, o arquivista tem, *grosso modo*, duas categorias de papeis a desempenhar na esteira da proteção de dados pessoais. Estes papeis que ele desempenha e/ou deve desempenhar são aplicáveis a qualquer entorno, analógico ou digital.

5 A ARENA ARQUIVÍSTICA MOÇAMBICANA

A presente seção é dedicada à apresentação e análise do cenário arquivístico de Moçambique. Neste exercício iniciamos pela ilustração da estrutura político-administrativa daquele país, em seguida nos debruçamos sobre o sistema nacional de arquivos de Estado, a fim de identificar os principais atores da arena arquivística moçambicana e por fim buscamos conhecer o arquivista moçambicano.

5.1 Moçambique: da estrutura administrativa em direção à estrutura arquivística

Para entendermos a configuração dos arquivos em Moçambique, é importante antes fazer o exercício de reconhecimento do deste país e sobretudo da estruturação do seu Estado, aliás como Jardim nos lembra em vários escritos seus, o maior produtor de informação arquivística, em particular, é o Estado. Assim, faz-se aqui um breve périplo pelo Moçambique antes e depois da independência.

Diaz (2023) nos lembra que antes da ocupação colonial, coexistiam vários povos no território que hoje encerra Moçambique, a exemplo dos povos no Norte do território, os Macondes, os Macuas, os Yao, dentre muitos outros. Com a ocupação colonial Moçambique, antiga província ultramarina de Portugal, conheceu um longo período de colonização que contou com vários ingredientes, um deles, um sistema de informação ou documentação, fraco e desordenado. Adam (2014), nos conta, por exemplo, que trabalhou e morou por muitos anos em Moçambique e foi consultora de arquivos. Lhe impressionara que o colapso dos arquivos não tivera começado com a independência de Moçambique e consequente saída abrupta dos portugueses, deixando Moçambique sem equipe técnica e com 90% de analfabetismo em 1976, mas sim, percebera que a degradação dos arquivos moçambicanos começou nos anos 60. Adam (2014) relata

Em toda parte, pude perceber que os arquivos formados no início do século XX, até meados dos anos 50, estavam muito bem organizados, de acordo com princípios arquivísticos sólidos e métodos manuais simples, mas eficientes. Eles podem ter sido progressivamente desorganizados e deteriorados por falta de espaço, mas sua ordem original pode ser reconstruída em um piscar de olhos. As pastas e caixas eram bem identificadas. Havia os livros de registro da época e vários auxílios para a recuperação de informações na forma de cartões de registro de terras,

cartões de resumo etc., que começaram a faltar gradualmente na década de 1960, antes da independência (Adam, 2014, p. 66)

Moçambique conquistou a sua independência do jugo colonial em 1975, aos 25 dias do mês de junho, fruto de uma luta de libertação nacional sob liderança da Frente de Libertação de Moçambique (FRELIMO). Como um território independente, nasce então um país e começa a construção de um Estado nacional, a República Popular de Moçambique com constituição própria, a Constituição da República Popular de Moçambique (CRPM). Nessa sua primeira constituição, no Artigo 33° está plasmado que

As liberdades individuais são garantidas pelo Estado à todos os cidadãos da República Popular de Moçambique. Estas liberdades incluem a inviolabilidade de domicílio e segredo de correspondência, e não podem ser limitadas, a não ser nos casos especialmente previstos na lei (CRPM, 1975).

Pode-se notar através deste Artigo 33° da CRPM que algum espírito de respeito e/ou salvaguarda da privacidade dos cidadãos moçambicanos esteve presente desde o nascimento do país em 1975. Imaginamos, contudo, que a tônica era dada ao sigilo aliado ao segredo de Estado, de um Estado recém-nascido, frágil e vulnerável em várias frentes. Um Estado também caracterizado por um grande centralismo (Artigo 56°) para além de ter sido, pelo menos em termos práticos, um partido-Estado. Aliás, o Artigo 57° ilustra bem este último aspecto, “O mais alto órgão do Estado na província é o Governo Provincial, presidido pelo governador. O governador é o representante do Presidente da República e responde perante a FRELIMO e o Governo pelas suas actividades” (CRPM, 1975). Portanto, esta constituição definiu a organização administrativa do Estado, sendo conforme o Artigo 55°, “A República Popular de Moçambique está administrativamente organizada em províncias, distritos e localidades” (CRPM, 1975).

Moçambique passa por um período de cerca de 16 anos de guerra civil tendo como beligerantes a FRELIMO e a Resistência Nacional Moçambicana (RENAMO), encerrado pelos Acordos Gerais de Paz. Parte das reivindicações, se não a maior, do movimento beligerante contra o partido-Estado, era a implantação de um Estado democrático e de Direito em Moçambique. Assim, a Constituição de 1990 introduziu o Estado de Direito Democrático e levou Moçambique às primeiras eleições multipartidárias em 1994. Moçambique passou a designar-se República de Moçambique e não mais República Popular, como se denota pela Constituição da República de Moçambique (CRM) de 1990.

No que toca à organização territorial desta república, ela passa a se organizar territorialmente em províncias, distritos, postos administrativos, localidades e povoações, conforme o Artigo 7°. O Artigo 8° estabelece que “A República de Moçambique é um Estado unitário, que respeita na sua organização os princípios da autonomia das autarquias locais” (CRM, 1990).

Princípios que norteiam a proteção de dados pessoais, encontram mais alento na CRM 1990, através de alguns artigos, como o 41° segundo o qual “Todo o cidadão tem direito à honra, ao bom nome, à reputação, à defesa da sua imagem pública e à reserva da sua vida privada” (CRM, 1990). O Artigo 68° faz determinações mais detalhadas inerentes à “inviolabilidade do domicílio e da correspondência” pouco desenvolvida na constituição anterior. O Artigo 71° trouxe mais subsídios, olhando com particular atenção à “utilização da informática”. Neste artigo está determinado que

1. É proibida a utilização de meios informáticos para registo e tratamento de dados individualmente identificáveis relativos às convicções políticas, filosóficas ou ideológicas, à fé religiosa, à filiação partidária ou sindical e à vida privada.
2. A lei regula a protecção de dados pessoais constantes de registos informáticos, as condições de acesso aos bancos de dados, de constituição e utilização por autoridades públicas e entidades privadas destes bancos de dados ou de suportes informáticos.
3. Não é permitido o acesso a arquivos, ficheiros e registos informáticos ou de bancos de dados para conhecimento de dados pessoais relativos a terceiros, nem a transferência de dados pessoais de um para outro ficheiro informático pertencente a distintos serviços ou instituições, salvo nos casos estabelecidos na lei ou por decisão judicial.
4. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação (CRM, 1990).

Através do Artigo 48° (liberdades de expressão e informação), a questão do direito à informação passa a estar presente na CRM, embora nessa altura com uma perspectiva quase totalmente virada à comunicação social. Contudo, é oportuno visitar o n.º 6 deste artigo, segundo o qual “6. O exercício dos direitos e liberdades referidos neste artigo é regulado por lei com base nos imperativos do respeito pela Constituição e pela dignidade da pessoa humana” (CRM, 1990). Isto quer dizer que mesmo tratando-se do direito à informação, este exercício deve respeitar a privacidade, a proteção de dados pessoais.

Dado o amadurecimento do sistema democrático em Moçambique e a intenção de reafirmá-lo e afiná-lo, com alicerces no pluralismo introduzido em 1990, uma nova Constituição da República de Moçambique (CRM) é aprovada em 2004. Nesta

constituição a organização territorial da República de Moçambique não foi alterada em relação à de 1990 mantendo-se a organização em províncias, distritos, postos administrativos, localidades e povoações, conforme o Artigo 7°.

Também se manteve inalterado o Artigo 48° sobre “Liberdades de expressão e informação”. Adiantamos que da revisão constitucional feita em 2018, o Artigo ainda permaneceu nos atuais termos, que como já dissemos, tem uma forte e grande carga de comunicação social, como podemos ver na íntegra:

1. Todos os cidadãos têm direito à liberdade de expressão, à liberdade de imprensa, bem como o direito à informação.
2. O exercício da liberdade de expressão, que compreende nomeadamente, a faculdade de divulgar o próprio pensamento por todos os meios legais, e o exercício do direito à informação não podem ser limitados por censura.
3. A liberdade de imprensa compreende, nomeadamente, a liberdade de expressão e de criação dos jornalistas, o acesso às fontes de informação, a protecção da independência e do sigilo profissional e o direito de criar jornais, publicações e outros meios de difusão.
4. Nos meios de comunicação social do sector público são assegurados a expressão e o confronto de ideias das diversas correntes de opinião.
5. O Estado garante a isenção dos meios de comunicação social do sector público, bem como a independência dos jornalistas perante o Governo, a Administração e os demais poderes políticos.
6. O exercício dos direitos e liberdades referidos neste artigo é regulado por lei com base nos imperativos do respeito pela Constituição e pela dignidade da pessoa humana (CRM, 2004).

Queremos esclarecer que não vemos nada de errado com a comunicação social, mas pensamos que o direito à informação, o acesso à informação não se encerra no corpo da comunicação social, ou da imprensa. Entendemos que é um direito fundamental, aliás, um direito humano, que deve ser feito valer das mais elementares formas, nas diversas instituições e serviços de informação ou não, e, portanto, esta generalidade deve encontrar embasamento na dita, Lei-mãe.

Antes de fecharmos a leitura da CRM 2004, achamos importante partilhar os artigos 249° e 250°, do capítulo I sobre “administração pública”, do texto XII que versa sobre “Administração Pública, Polícia, Provedor de Justiça e Órgãos Locais do Estado”. O Artigo 249° apresenta os princípios fundamentais e em seu n.º 1 “A Administração Pública serve o interesse público e na sua actuação respeita os direitos e liberdades fundamentais dos cidadãos” (CRM, 2004). Quer dizer, de forma mais explícita para fins deste trabalho que, os órgãos e instituições da administração pública moçambicana, devem respeitar os direitos de protecção de dados pessoais dos

moçambicanos, bem como o seu direito de acesso à informação, inclusive sobre seus dados pessoais coligidos por esses órgãos e instituições.

No n.º 2 do Artigo 250º, está plasmado que “A Administração Pública promove a simplificação de procedimentos administrativos e a aproximação dos serviços aos cidadãos” (CRM, 2004). Entendemos que este ditame é possível havendo uma gestão de documentos implantada na administração pública moçambicana, que seja fruto de uma política arquivística nacional. Aliás, parece que, mesmo de forma tímida, nos anos que se seguiram, o aspecto arquivístico deste artigo foi considerado e assumido, tendo sido aprovada em 2006, a Estratégia para a Gestão de Documentos e Arquivos do Estado (EGDAE).

Conforme fizemos menção acima, a CRM foi revista, pontualmente, em 2018. A grande razão da revisão era de acomodar os interesses da descentralização e desconcentração do Estado ao mesmo tempo que se preparava o terreno para as eleições corridas em 2019. Note que o ano de 2018 coincide com o ano da revisão do chamado sistema nacional de arquivos do Estado, sobre o qual iremos discorrer mais adiante.

Moçambique tem como cidade capital a Cidade de Maputo. Este é um país que se localiza na região austral da África, concretamente na sua costa oriental e por isso é banhado pelo oceano Índico. A sua localização geográfica lhe permitiu ser um membro fundador da Comunidade de Desenvolvimento da África Austral (SADC), antiga Conferência de Coordenação do Desenvolvimento da África Austral (SADCC), constituída em Lusaka, Zâmbia, em 1980 (SADC, s.d.). Esta comunidade tem o objetivo de “alcançar o desenvolvimento económico, a paz e a segurança, o crescimento, reduzir a pobreza, elevar o nível e a qualidade de vida das populações da África Austral, e apoiar as camadas sociais desfavorecidas, mediante a integração regional” (SADC, s.d.).

Num plano continental, Moçambique é Estado membro da União Africana (UA) à qual aderiu em 18 de julho de 1975, quase um mês após a proclamação da independência. A UA é um órgão continental formado pelos 55 Estados que compõem os países do continente africano e surge da transformação da Organização da Unidade Africana (OUA), criada em 1963 (UA, s.d.). A UA atua sobre diferentes áreas-

chave, podemos destacar aqui “Resolução de conflitos, paz e segurança”; “Democracia, leis e direitos humanos”; “Educação, ciência e tecnologia”, etc.

Moçambique embora não sendo uma ex-colónia britânica, integrou a Commonwealth em 1995, depois das primeiras eleições democráticas multipartidárias de 1994. A Commonwealth é uma associação voluntária de países independentes, incluindo tanto economias avançadas quanto países em desenvolvimento. Esta organização tem como metas o desenvolvimento, a democracia e a paz (Commonwealth, s.d.).

Em 1996, Moçambique fez parte da criação da Comunidade dos Países de Língua Portuguesa (CPLP), junto de outros países, a destacar o Brasil que teve atores e foi palco bastante decisivo para a criação desta comunidade, como a realização do primeiro encontro dos Chefes de Estado e de Governo dos países de língua portuguesa, em São Luís do Maranhão, em 1989. Para além da “materialização de projetos de promoção e difusão da língua portuguesa”, esta comunidade prossegue diferentes objetivos e tem “cooperação em todos os domínios, inclusive os da educação, saúde, ciência e tecnologia, defesa, agricultura, administração pública, comunicações, justiça, segurança pública, cultura, desporto e comunicação social” (CPLP, s.d.).

O Relatório sobre o Desenvolvimento Humano 2023/2024 do Programa das Nações Unidas para o Desenvolvimento (PNUD), intitulado “Acabar com o impasse: Reinventar a cooperação num mundo polarizado”, mostra Moçambique na posição 183, apenas 10 lugares acima de Somália, o último país na categoria de países de desenvolvimento humano baixo (PNUD, 2024).

Ora, olhando para as normativas moçambicanas ordinárias, vemos que poucos anos depois da proclamação da independência, é aprovada pela Comissão Permanente da Assembleia Popular, a Lei n.º 12/79, de 12 de dezembro, que visa proteger o segredo estatal relativamente a todos os documentos contendo dados e informações classificados. Na introdução desta lei pode-se ler

A República Popular de Moçambique é o produto dos sacrifícios consentidos pelo Povo e constitui a materialização da vitória do povo moçambicano contra a dominação colonial portuguesa e o imperialismo. [...] Na sua acção, o inimigo tenta obter informação de carácter secreto para utilizá-la na perpetração de novos crimes e atentados contra o nosso Povo, Partido e Estado. Urge assim, intensificar o processo de criação de instrumentos legais

que permitam consolidar o exercício da ditadura democrática popular. (Moçambique, 1979).

Este trecho ilustra diferentes aspectos daquele Estado moçambicano, dentre eles seu carácter monopartidário e tendencialmente socialista, bem como as sementes do secretismo que veio a caracterizar a administração pública moçambicana desde essa altura. Contudo, o espírito para a concepção de normativas atinentes à dados e/ou informações de acesso não público está presente.

Para esta lei documento é “qualquer objecto físico capaz de conter registada uma informação que pode ser transmitida de uma pessoa para outra” (Artigo 3). No artigo seguinte a lei aponta que esses documentos se dividem em: “Documentos classificados”, sendo “aqueles que contêm dados ou informações militares, políticas, económicas, comerciais, científicas, técnicas ou quaisquer outras cuja divulgação ponha em causa, prejudique, contrarie ou perturbe a Segurança do Estado e do Povo ou a economia nacional” E em “Documentos não classificados”, sendo os que não possuem nenhuma das características dos documentos classificados. Ora, o Artigo 5 esclarece que os dados ou informações contidas nos documentos classificados dividem-se em Segredo de Estado; Secreto; Confidencial; e, Restrito.

Para o controlo de informações, “a Comissão para Implementação do Segredo Estatal define as estruturas em que devem ser designados responsáveis pelo controlo da informação classificada” (n.º1 do Artigo 8º) e “Compete aos dirigentes das estruturas a que se refere o número 1 designar as pessoas que podem ter acesso a documentos classificados” (n.º4 do Artigo 8º), entendendo que estes podem conter dados pessoais.

A Comissão para Implementação do Segredo Estatal (CPISE), acima referida, foi criada pelo Decreto Presidencial n.º 9/93, de 29 de dezembro de 1993. Conforme o Artigo 2 deste decreto presidencial, a CPISE é presidida pelo Director-Geral do Serviço de Informações e Segurança do Estado (SISE), coadjuvado por um vice-presidente, e composta por subcomissões que funcionam junto do Ministério da Defesa Nacional; Ministério do Interior; Ministério da Administração Estatal⁵; e, SISE (Artigo 3).

⁵ Atual Ministério da Administração Estatal e Função Pública, de acordo com a designação vigente até ao momento que submetemos este trabalho à avaliação.

A CPISE tem papel de relevo no cenário arquivístico de Moçambique. Tem seu lugar no Sistema Nacional de Arquivo de Estado (SNAE) de 2018, incluindo no Conselho Nacional de Arquivos (CNA) e na Comissão Nacional de Avaliação de Documentos (CNAD), bem como no projeto de Sistema Nacional De Gestão Documental (e-SNGD). No âmbito do SNAE 2018 a CPISE joga o papel de Órgão de gestão de informação classificada e tem, entre outras funções, a função de centralizar e orientar a implementação das normas do Segredo do Estado; emitir instruções que definam os princípios básicos e as normas destinadas a garantir a segurança das matérias classificadas; garantir o controlo e o cumprimento das instruções adotadas; e, capacitar e apoiar metodologicamente as diferentes instituições na elaboração dos classificadores de informação classificada (Moçambique, 2018a).

Em 1997 foi aprovada a Resolução n.º. 12/97, de 10 de Junho, que aprova a Política Cultural e Estratégia de sua Implementação. Essa política é um instrumento que regula a atividade do Governo na sua articulação com os demais intervenientes na promoção e desenvolvimento da cultura. Conforme o instrumento, a política cultural visa nortear a atuação de todos, no contributo para a coesão e equilíbrio psicológico e social das comunidades, assim como para a integração dos seus membros. A política cultural do Governo constitui uma contribuição para a definição dos contornos da moçambicanidade que corporizam o património de todos os cidadãos.

Ela tem como um dos seus princípios norteadores que “Todos os cidadãos têm igual direito de participação na vida cultural e de acesso à fruição dos benefícios da cultura e arte” (Moçambique, 1997a). E para o desenvolvimento cultural, foi elencado, pelo Governo, como umas das prioridades o domínio dos arquivos, sendo considerado que estes têm por função a recolha, tratamento, conservação e difusão de documentos, essencialmente primários, em diferentes tipos de suporte e que o Governo apoia as atividades dos arquivos existentes e encoraja a criação de outros de âmbito nacional e local, gerais e especializados. Olhando para estes dizeres, reabre-se o questionamento sobre a criação de arquivos públicos em Moçambique, passados praticamente 33 anos depois das primeiras indicações de necessidade de criação dos mesmos. Aliás, pode-se ver mesmo através desta resolução, na componente “estratégia de implementação”, em particular no que concerne às “competências do Estado” que no âmbito da implementação da política cultural, entre outras atribuições, compete ao Estado “Criar instituições culturais como museus,

bibliotecas, Casas de Cultura, escolas artísticas, galerias e teatros” (Moçambique, 1997a). Como se vê, parece que os arquivos ficaram esquecidos desde logo no próprio instrumento, uma situação que não acontece apenas neste dispositivo legal.

A Política e Estratégias da Informação são aprovadas pela Resolução n.º 3/97, de 25 fevereiro de 1997, referindo-se “ao conjunto de medidas ou atividades baseadas no Programa do Governo, visando impulsionar o desenvolvimento da comunicação social” (Moçambique, 1997b). Sem precisar de ir ao mais profundo desta suposta política de informação, percebe-se pela definição dada pelo Governo de Moçambique, que não se trata de uma política, nos termos de Jardim, Silva e Nharreluga (2009), como conjunto de premissas, decisões e ações, produzidas pelo Estado e inseridas nas agendas dos governos em nome do interesse social, contemplando, entre outros, os aspectos administrativo, legal, científico, cultural e tecnológico, relativos à produção, uso e preservação da informação de natureza pública e privada, mas sim trata-se de uma política de comunicação social.

Nharreluga (2009) teceu críticas sobre como os arquivos foram e/ou são recorrentemente tomados em Moçambique. O autor percebe que eles não são concebidos em sua dimensão informacional em que possam assumir a liderança na gestão da informação e na definição de políticas de informação arquivística, por exemplo. Pelo contrário, os arquivos são concebidos em seu sentido cultural apenas, exprimindo a preservação da memória institucional e ações de pesquisa histórica. Essa maneira de tomar o arquivo está patente nos dois instrumentos 1997 que acabamos de ver.

Aparentemente alguma coisa deste cenário poderia vir a ser alterada com a criação da Comissão Interministerial da Reforma do Sector Público – CIRESP, pelo Decreto Presidencial n.º 5/2000 de 4 de abril de 2000. Conforme o texto introdutório deste dispositivo, foi reconhecendo a necessidade de garantir a coordenação dos diversos programas setoriais no âmbito da reforma do sector público, em função de um mesmo objetivo que é o da racionalização e modernização da administração pública com vista à melhoria contínua da qualidade de serviços prestados ao cidadão, que foi criada a Comissão Interministerial da Reforma do Sector Público, também designada por CIRESP, subordinada ao Conselho de Ministros (Artigo 1). A CIRESP tem como objetivos:

- a) Elaborar e propor a política global da reforma do sector público;
- b) Assegurar a coordenação, gestão e implementação da reforma, nomeadamente facilitando a articulação e harmonização dos diversos programas sectoriais;
- c) Promover e garantir a participação integrada de todos os serviços e da sociedade civil na desburocratização, simplificação, modernização e profissionalização da Administração Pública (Moçambique, 2000a).

Sem precisar de muito esforço, é perceptível que estes objetivos são alcançáveis com a área de arquivos em condições de servir ao sector público. Os objetivos definidos para esta comissão, requerem, antes de mais, uma gestão de documentos ao rubro.

A comissão é presidida pelo Primeiro-Ministro e conta com o Ministro da Administração Estatal como seu vice-presidente. O vice-presidente tem as funções de:

- a) Coadjuvar o Presidente no exercício das suas funções;
- b) Assegurar o monitoramento e assistência necessária ao desenvolvimento das actividades inerentes ao programa da reforma, velando pelo cumprimento das decisões da CIRES;
- c) Garantir a supervisão dos trabalhos da Unidade Técnica da Reforma do Sector Público, orientando e decidindo atempadamente sobre as questões de gestão corrente do processo da reforma (Moçambique, 2000a).

A referida Unidade Técnica da Reforma do Sector Público (UTRESP), foi criada pelo Decreto n.º 6/2000, de 4 de abril, para apoiar os trabalhos da CIRES. Ele é, portanto, um órgão técnico permanente de execução corrente do programa da reforma do sector público que tem como objetivos apoiar o funcionamento da CIRES e assegurar a planificação integrada, a coordenação, articulação e acompanhamento dos programas e projetos da reforma (Artigo 1). São algumas funções da UTRESP:

- c) Garantir a implementação das políticas e estratégias integradas da reforma do sector público e garantir a integração dos programas sectoriais de reforma em curso na estratégia global do Governo;
- f) Organizar e assegurar o funcionamento de um Centro de Informação da Reforma do Sector Público e garantir a sua crescente actualidade;
- h) Propor medidas integradas visando a promoção do profissionalismo e a mudança de atitudes com vista à melhoria da qualidade dos serviços prestados ao cidadão (Moçambique, 2000b).

Parece-nos que, para o desempenho pleno destas funções, a UTRESP deve ter conhecimento teórico e prático da gestão de documentos, dito de outro modo, esta unidade, em condições normais, deve estar composta por recursos humanos capacitados em gestão de documentos.

Em 2001 o Governo de Moçambique concebeu a “Estratégia Global da Reforma do Sector Público -EGRSP- (2001-2011)”. Sob responsabilidade da CIRESPP, com a reforma e sua estratégia, se “pretende que os serviços públicos sejam mais operacionais, orientados para resultados e com enfoque no cidadão. Este, deverá estar no centro das atenções, pelo que o sector público deverá estar mais voltado para fora e não para dentro de si mesma” (CIRESPP, 2001a, p. 9). Neste contexto, a reforma, que é implementada pelos sectores, é concebida pelo Governo de Moçambique como o conjunto de ações de carácter transversal ou horizontal e processos de mudanças que devem ser empreendidos de modo que os serviços públicos sejam melhorados (CIRESPP, 2001a.).

No diagnóstico do sector público feito no âmbito da EGRSP, foram identificados alguns problemas. Relativamente à gestão dos processos de políticas públicas, podem ser destacados problemas como:

A definição de políticas públicas ainda não é concebida e coordenada em função de objectivos e princípios que permitam a sua gestão efectiva (viabilidade, coordenação, monitoria e avaliação de objectivos e resultados/impacto); as políticas públicas e as suas estratégias nem sempre estão, como regra, compatibilizadas com os recursos necessários à sua viabilização, em particular os previstos nos planos e orçamentos do Estado; não há um sistema e processo definidos de formulação de políticas públicas, pelo que as práticas de formulação são díspares; não há um fluxo de informação organizado de suporte à tomada, monitoria e avaliação das decisões do Conselho de Ministros; a análise de políticas públicas ainda não constitui uma actividade técnica específica institucionalizada e praticada; ainda não é obrigatória a consulta a entidades que sejam ou possam vir a ser afectadas por uma determinada política pública e que, por esse facto, devem ser consideradas interessadas nessa política; etc. (CIRESPP, 2001a, p. 15-16).

Este cenário diz muito quando pensamos na área da informação, de forma mais concreta, quando pensamos nos arquivos e suas políticas em Moçambique. Ainda que exista legislação sobre arquivos, elas não fazem parte de uma política arquivística nacional formalizada em algum documento. Aliás, mesmo os sistemas de arquivos que foram sendo aprovados e alterados, não se consubstanciam como parte de alguma política de arquivos, daí compreende-se, com alguma facilidade o seu (des)funcionamento. Ora, o que não se compreende é por que razão alguns problemas prevalecem tendo sido identificados. Vejamos que este documento é de 2001 e a versão de sistema nacional de arquivos em vigor é de 2018, um sistema que não veio corrigir o que não esteve bom em 2007, que aliás teve uma estratégia específica em 2006 para, supostamente, melhorar o sistema que, se foi implementado

de fato, vigorava desde 1992. Um dos indicadores gerais para a verificação dos resultados da estratégia, é ter, conforme CIRES, “os mecanismos de informação e prestação de contas pelo Governo e objecto da reforma em pleno funcionamento, sendo a informação respectiva disseminada e acessível para o conhecimento público” (CIRES, 2001a, p. 21). Parece-nos que este indicador é bastante forte para que, até a esta parte, ainda não tenhamos, mesmo em moldes tradicionais (uma vez que os portais existentes não funcionam na plenitude ou estão sempre inacessíveis) as instituições não só não disponibilizam informações de interesse público de maneira voluntária como também continuam amarradas ao sigilo exacerbado o que lhes leva a recusar os pedidos de informação.

Ainda em 2001, o Conselho de Ministros aprovou o Decreto n.º 30/2001, de 15 de outubro de 2001, que aprova Normas de Funcionamento dos Serviços da Administração Pública. Este é um dos instrumentos incontornáveis na arena arquivística moçambicana. A sua importância se mostra desde logo no texto introdutório desta normativa, onde se lê que

A criação duma Administração Pública ao serviço do desenvolvimento harmonioso do País, das necessidades dos cidadãos e da sociedade em geral deve ser uma das preocupações permanentes da modernização administrativa, preconizada no programa do Governo, consubstanciada pela aproximação da administração aos utentes, pela prestação de melhores serviços, pela simplificação dos procedimentos e ao aumento da qualidade da gestão e funcionamento do aparelho administrativo do Estado (Moçambique, 2001b).

Como se pode depreender, para servir melhor aos utentes dos serviços da administração pública, o que significa igualmente que ela tenha melhores serviços, implica uma gestão de documentos efetiva, possibilitando o acesso à informação não só aos utentes, mas aos próprios produtores da informação, no caso vertente as instituições da administração pública. Possibilitará também melhor gestão do sigilo, como nos casos em que há dados pessoais contidos em documentos solicitados para acesso.

Conforme o decreto n.º 30/2001, a Administração Pública é regida pelos princípios da legalidade; princípio da prossecução do interesse público e proteção dos direitos e interesse dos cidadãos; princípio da justiça e da imparcialidade; princípio da transparência da administração pública; princípio da colaboração da administração com os particulares; princípio da participação dos particulares; princípio da decisão; princípio da celeridade do procedimento administrativo; princípio da fundamentação

dos atos administrativos; princípio da responsabilidade da administração pública; e, princípio da igualdade e da proporcionalidade.

O princípio da transparência da administração pública, de acordo com o plasmado no n.º1 do Artigo 7º, “implica a publicidade da actividade administrativa”. Combinado com o Artigo 8º, princípio da colaboração da administração pública com os particulares, onde está determinado que

1. No desempenho das suas funções, os órgãos e instituições da administração pública colaboram com os particulares, devendo designadamente:
 - a) Prestar as informações orais ou escritas, bem como os esclarecimentos que os particulares lhes solicitem;
 - b) Apoiar e estimular as iniciativas dos particulares, receber as suas informações e considerar as suas sugestões
2. A administração pública é responsável pelas informações prestadas por escrito aos particulares, ainda que não obrigatórias (Moçambique, 2001b).

Percebe-se o dever das instituições em informar aos cidadãos sobre os seus dados pessoais, como também pautar pelo acolhimento das possíveis correções apontadas pelos cidadãos titulares dos dados pessoais. Portanto, sem ignorar outros princípios, estes dois conseguem aliar a gestão de documentos e a proteção de dados pessoais na dimensão em que o cidadão/utente/titular de dados tem o direito de ser informado e de se informar acerca dos seus dados pessoais.

O decreto reserva a seção V, do capítulo VII (formalidades do procedimento administrativo) para determinar aspectos inerentes à “arquivo”. O Artigo 90º estabelece que para além de apontar que os meios eletrônicos podem ser utilizados sem prejuízo do sistema manual de arquivo, também apresenta a distinção de arquivo corrente e arquivo intermediário, para além de indicar no seu n.º 4 que “o arquivo intermediário, com regulamento próprio, será criado por diploma conjunto do Ministério da Administração Estatal e do ministério respectivo” (Moçambique, 2001b). Disposições são feitas sobre informação classificada (Artigo 92º), responsabilidade e utilização do arquivo (Artigo 94º), bem como indicações gerais de temporalidade para os documentos em fase intermediária, enquanto o dispositivo mobiliza o AHM como parte de comissões técnicas de avaliação de documentos, mas também para determinar que “os documentos anteriores à data da independência nacional devem ser remetidos para o Arquivo histórico de Moçambique” (Moçambique, 2001b).

A CIRESPP assistida pela UTRESPP sofreu algumas alterações em 2007 e em 2016 é profundamente alterada pelo Decreto Presidencial n.º 2/2016, de 20 de maio, através do qual é criada a Comissão Interministerial da Reforma da Administração Pública, abreviadamente designada por CIRAP e revogado o Decreto Presidencial n.º 2/2007, de 8 de março, e o Decreto Presidencial n.º 3/2015, de 20 de fevereiro. Portanto, a CIRESPP passa a ser CIRAP. O seu regulamento interno é aprovado em 2016 e atualizado em 2021 pelo Decreto n.º 98/2021, 31 de dezembro, onde a CIRAP é definida como o “órgão de coordenação das actividades a desenvolver na Administração Pública, que assegura a implementação dos objectivos no âmbito da aplicação da Estratégia da Reforma e Desenvolvimento da Administração Pública” (Moçambique, 2021a). Voltaremos para a CIRAP, mas antes é interessante olhar algum detalhe dessa Estratégia da Reforma e Desenvolvimento da Administração Pública – ERDAP (2012-2025), aprovada pelo Conselho de Ministros na sua 29ª Sessão Ordinária, de 14 de agosto de 2012.

Conforme a CIRESPP (2012) a Estratégia da Reforma e Desenvolvimento da Administração Pública 2012-2025 (ERDAP) surge da necessidade de responder ao Programa Quinquenal do Governo (PQG), na sequência dos resultados conseguidos com a implementação dos Programas de Governação e da EGRSP, alinhados com os objetivos estabelecidos na Agenda 2025, Plano de Acção para Redução da Pobreza (PARP) e Objectivos de Desenvolvimento do Milénio na área da Governação.

Na ERDAP são identificados sete objetivos estratégicos a serem prosseguidos de forma transversal e integrada pelos vários sectores da Administração Pública em Moçambique, destacamos aqui o objetivo de “Fortalecer a organização da Administração Pública” (CIRESPP, 2012, p. 8). Estes objetivos tomam corpo nas chamadas “componentes” de desenvolvimento. São cinco principais componentes, a saber: profissionalização dos funcionários e agentes do Estado (componente 1); descentralização e desconcentração (componente 2); melhoria da prestação de serviços (componente 3); consolidação e coordenação das estruturas da administração pública (componente 4); e, reforço da integridade na administração pública (componente 5) (CIRESPP, 2012).

Ao nosso estudo interessa a componente 4, que se alinha ao objetivo “Fortalecer a organização da Administração Pública”. Assim, na ERDAP são elencadas áreas de atuação desta componente estratégica. São elas:

4.1. Promover a continuidade do serviço público: Assegurar a existência de uma Administração Pública profissionalizada com uma base regulamentar, funcional e humana estável, que seja o garante da capacidade de prestação de serviços, independentemente de mudanças de titulares de cargos públicos.

4.2. Assegurar a preservação da memória institucional: Consolidar a implementação dos sistemas de gestão de documentos e arquivos na Administração Pública e criar condições para a sua modernização, promovendo a gestão do conhecimento e o acesso à informação por parte dos funcionários e agentes do Estado e da sociedade em geral.

4.3. Melhorar a coordenação da planificação e execução entre sectores: Reforçar os mecanismos de articulação e integração das políticas sectoriais, nas fases de planificação e execução, assumindo as várias componentes da Administração Pública como fazendo parte de uma entidade única que existe para um propósito comum (CIRES, 2012, p. 56).

Face à estas áreas de atuação, foram definidos indicadores de desempenho da componente em questão. Desta feita para cada área há um indicador correspondente, ou seja, para “Promover a continuidade do serviço público” o indicador é “Lei de Bases de Organização da Administração Pública aprovada”; para “Assegurar a preservação da memória institucional” o indicador é “Percentagem de organismos que implementam o SNAE” e para a área “Melhorar a coordenação da planificação e execução entre sectores” o indicador é “Aprovação e Implementação da Estratégia de Desenvolvimento Nacional”. Como se pode notar mais especificamente, a área 4.2, junto do seu indicador, são aspectos que não só nos interessam, mas também devem ser acautelados no escopo de uma política arquivística (nacional). Cogitamos assim que, pelo menos até 2025, o cenário arquivístico moçambicano em que o grande ausente é uma política arquivística nacional formalizada em um documento, prevaleça. Importa referir também que no documento da ERDAP não ocorrem, em nenhum momento e nem por sinónimos os termos “privacidade” ou “dados pessoais”.

De volta à CIRAP, importam as suas diversas funções, das quais podemos destacar no domínio das políticas de desenvolvimento das TIC:

- a) acompanhar e avaliar a implementação das políticas atinentes ao desenvolvimento das tecnologias de informação e comunicação e suas estratégias de implementação;
- b) assegurar a padronização de informatização dos serviços do Estado e de uso de sistemas e tecnologias de informação e comunicação na Administração Pública;
- c) avaliar periodicamente a implementação da Estratégia de Governo Electrónico a nível nacional;
- d) assegurar a expansão e consolidação da infra-estrutura nacional das telecomunicações; e
- e) recomendar sobre as normas e os processos de formação e certificação dos técnicos de informática (Moçambique, 2021a).

As funções da CIRAP nesse domínio, são claramente conexas à gestão de documentos, às questões arquivísticas, mas até aqui estes aspectos não foram colocados de forma explícita nos instrumentos que as regulam, o que pode significar desconhecimento e provável insucesso na implementação destes dispositivos. Da mesma comissão, são algumas das competências no domínio da Reforma da Administração Pública:

- a) definir objectivos gerais metodológicos e prioridades da organização, modernização, gestão e implementação da reforma da administração pública;
- b) garantir a harmonização do quadro legal e das políticas sectoriais da reforma da Administração Pública de modo a contribuir para a racionalização dos recursos humanos, materiais e financeiros;
- d) promover acções concentradas na desburocratização, simplificação de procedimentos, descentralização e de modernização administrativa, para melhorar a qualidade de serviços e boa governação;
- g) orientar a gestão e implementação da reforma, facilitando a articulação e harmonização dos diversos programas sectoriais" (Moçambique, 2021a).

Compreendemos que toda a reforma da administração pública que se pretenda imprimir, visa acima de tudo, a melhoria na prestação dos serviços das diferentes instituições, o que significa igualmente o traçar e a prossecução desta competência. Nós nos questionamos como, em particular, esta competência da CIRAP pode ser cumprida sem a devida consideração dos arquivos, dos documentos, da gestão de documentos?

5.2 O Sistema Nacional de Arquivos do Estado e sua (des)estrutura arquivística

Moçambique conta atualmente com a sua terceira versão do chamado sistema nacional de arquivo de Estado. Para sermos mais rigorosos e respeitarmos os nomes dados pelo Governo de Moçambique, atualmente vigora a segunda versão do Sistema Nacional de Arquivos do Estado (SNAE) depois de ter vigorado, antes da sua primeira versão, o Sistema Nacional de Arquivos (SNA), que teve versão única. Começamos, então, revisitando este sistema antes de desembocar no sistema em implementação.

O Decreto n.º 33/92, de 26 de outubro de 1992, institui o Sistema Nacional de Arquivos (SNA) (Moçambique, 1992). Na introdução deste decreto, o Conselho de Ministros escreveu:

Os arquivos constituem um instrumento importante para preservar e valorizar o património histórico e cultural da nação moçambicana, para a tomada de decisões dos órgãos do [E]stado e também para comprovar os direitos dos cidadãos. A fim de assegurar a protecção do património arquivístico, é necessário desenvolver um sistema nacional de arquivos que discipline a custódia dos documentos e o acesso às informações neles contidas, desde a sua produção até ao destino final, não se dissociando o seu valor histórico da importância que os acervos assumem enquanto instrumentos de administração. Para imprimir maior racionalidade e operacionalidade aos serviços de arquivo, há que manter integradas as fases corrente, intermediária e permanente por que passam os documentos, segundo as normas gerais de procedimento (Moçambique, 1992).

A introdução do decreto enche de esperança num contexto arquivístico desolador. No Artigo 1 define-se que são arquivos, consideram-lhes os conjuntos de documentos que, independentemente da natureza ou do suporte da informação, são reunidos por processo de acumulação ao longo das atividades de pessoas físicas ou jurídicas, públicas ou privadas, e conservados em razão do seu valor (Moçambique, 1992)

Integravam o SNA, o Arquivo Histórico de Moçambique (AHM), os arquivos centrais, os arquivos correntes nos diferentes órgãos do Estado, e outras entidades e os arquivos especiais existentes ou a serem criados (Moçambique, 1992). O AHM, desempenhava as funções de órgão central, quer dizer, conforme o Artigo 8, cabia ao AHM: formular diretrizes gerais e fazer a supervisão metodológica do funcionamento do sistema; fazer a supervisão do processo de avaliação de documentos de arquivo, presidindo as comissões que se formassem para esse fim; participar no estabelecimento de programas de racionalização da produção documental; propor a política geral de acesso aos arquivos, respeitando as normas de confidencialidade; promover ações de formação de recursos humanos em matéria de arquivo; manter um cadastro geral atualizado das unidades que desempenhavam atividades de arquivo no âmbito do sistema (Moçambique, 1992) Portanto, nesta versão do sistema, tem-se a na figura de órgão central, um arquivo nacional (e igualmente histórico), à *priori* com capacidade técnico-científico para a gestão do sistema. Sobre este sistema, Nharreluga percebe que

Esta versão é relevante na medida em que sua estrutura compreende ou prevê domínios arquivísticos. Contudo, além da falta de harmonia entre os supostos arquivos indicados como parte da estrutura do sistema, os arquivos referidos como integrantes do sistema, excepto o AHM, não foram instituídos durante toda a vigência da mesma versão, de 1992 até sua extinção em 2007 (Nharreluga, 2021, p. 139).

Embora imbuída de considerável lógica arquivística, o SNA apresentava diversas carências na sua formulação em si (a ausência de instrumentos de gestão de documentos, por exemplo), mas também pela conjuntura que a envolvia (falta de profissionais arquivistas, legislação fraca etc.). É assim que em 2006 foi aprovada a estratégia para a gestão de documentos e arquivos do Estado (EGDAE), pela Resolução n.º 46/2006, de 26 de dezembro. Na sua introdução está plasmado que

A gestão documental e a protecção especial de documentos e arquivos são da responsabilidade do Governo, enquanto instrumento chave de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação. Ao longo das últimas décadas, a gestão de documentos e arquivos nas instituições do Estado não acompanhou a rápida evolução e introdução das novas tecnologias que, actualmente, são usadas em muitos países do Mundo (EGDAE, 2006, p. 1).

Com estas palavras parece que o Governo de Moçambique, dessa altura, estava bastante sensibilizado com as questões arquivísticas e disposto a estabelecer as condições de base para a um cenário arquivístico melhor desenhado e funcional, ciente dos desafios de diversa ordem que constituíam (e ainda o são) a situação daquela altura.

Portanto, para a elaboração da estratégia, foi realizado um levantamento a nível central, provincial e distrital das instituições da Administração Pública e constataram-se irregularidades ligadas ao enquadramento institucional; ao desenvolvimento de recursos humanos; a capacidade institucional; ao acesso à Informação; e, a Legislação (EGDAE, 2006). São, portanto, constatações que partem desde a ausência dos arquivos nos organogramas das instituições a que pertencem e seus objetivos e/ou atribuições claramente definidos, passando pelo secretismo na disponibilização de documentos, desaguando no desajuste dos instrumentos legais com destaque para o decreto n.º 33/92, que acima apresentamos.

Esta estratégia orienta-se pelos princípios de uniformização de métodos, através do qual, considerando as especificidades de cada setor, orienta que a gestão de documentos nas instituições públicas deve obedecer a normas e métodos de trabalho comuns e prossecução de fins comuns. O princípio de profissionalização do setor, orienta promover a formação profissional e recrutamento de pessoal qualificado em matérias de gestão de documentos como forma de elevar as capacidades técnicas na área. Com o princípio de modernização há orientação para a promoção do uso das tecnologias de comunicação e informação durante o ciclo vital da informação. No que

toca ao princípio de preservação e salvaguarda definitiva de documentos, este é adotado de forma a garantir a conservação em arquivos permanentes, assegurar a acessibilidade e inteligibilidade (EGDAE, 2006).

O texto da estratégia considera a diversidade e natureza das instituições do Estado e define as instituições da Administração Pública como sectores-alvo no domínio da gestão documental. Ainda avança que as instituições autónomas e independentes só poderão desenvolver os seus subsistemas de gestão de documentos e arquivos, desde que observem os princípios que guiam a estratégia.

Três etapas de implementação do EGDAE foram programadas. A primeira faz referência à realização de programas de curto prazo no ano de 2006. Tais programas incluem a divulgação da própria estratégia; a revisão do decreto n.º 33/92 e aprovação de instrumentos de gestão de documentos, entre outros programas. A segunda se refere à realização de ações e programas de médio prazo nos anos de 2007 à 2008. Nesta etapa previu-se a implantação do decreto revisto; a institucionalização das unidades de gestão de documentos, como forma de fazer frente ao desafio referente ao enquadramento institucional; introdução de sistemas de gestão eletrônica de documentos, entre outras ações. Importa assinalar que algum sinal de institucionalização de tais sistemas começamos a notar no ano de 2022 com o desenvolvimento do chamado Sistema Nacional De Gestão Documental (e-SNGD), sobre o qual iremos abordar mais adiante. A derradeira etapa é de implementação dos programas e projetos de desenvolvimento da área de arquivos no ano de 2009, tendo em vista a sua modernização.

Contudo, mesmo equacionados nessa estratégia, os problemas da área, não encontraram uma solução, conclui Nharreluga (2021). O autor percebe que os problemas identificados e apresentados pela EGDAE são estruturais e exigem a conceção de políticas arquivísticas para a sua resolução, o que significa que

a conceção de arquivos públicos (que contempla a dimensão institucionalizada, no caso de um Estado unitário como Moçambique, do Arquivo Nacional, dos arquivos provinciais, dos arquivos distritais ou municipais) tem sua maior realização no âmbito de uma política arquivística, que antecede a conceção e operacionalização de qualquer modelo, seja ele sistémico ou não, voltado para o seu gerenciamento (Nharreluga, 2021, p. 146).

Portanto, diante do exposto desta estratégia, podemos inferir que diferentes aspectos assistidos em Moçambique na área dos arquivos desde o ano 2007, tiveram

a sua razão, não só na insustentabilidade da situação arquivística que caracteriza(va) a administração pública em particular, mas sobretudo nas linhas orientadoras emanadas da EGDAE. Entendemos, por exemplo, que a criação do curso de graduação em Ciência da Informação com especialidade em Arquivística (e em Biblioteconomia) na Universidade Eduardo Mondlane (UEM) em 2009 e em 2016 a criação do curso de graduação em Arquivística, bem como a criação do curso de graduação em Biblioteconomia e Documentação na Escola Superior de Jornalismo em 2010, tiveram fundamentação nesta estratégia. Não menos importante, foi a aprovação do Sistema Nacional de Arquivos do Estado (SNAE) pelo decreto n.º 36 /2007, fruto da revisão do SNA, como indicamos acima.

O decreto que aprova o Sistema Nacional de Arquivos do Estado (SNAE) de 2007, para além de revogar o SNA de 1992, aprova também, como se lê no n.º 1 do artigo 2, o Plano de Classificação de Documentos para as Actividades Meio, a Tabela de Temporalidade e Destinação de Documentos para as Actividades Meio da Administração Pública e o Classificador de Informações Classificadas. Portanto, esta versão, diferente da anterior, já veio acompanhada de instrumentos de gestão de documentos. O SNAE 2007 institui também, o Conselho Nacional de Arquivos (CNA) e a Comissão Nacional de Avaliação de Documentos (CNAD), importantes atores na cena arquivística. Estes serão objeto de apresentação mais abaixo (Moçambique, 2007).

O SNAE 2007 define Arquivo como sendo o conjunto de documentos de qualquer época e forma que, independentemente da natureza ou do suporte da informação, são acumulados e conservados em razão do seu valor ao longo das atividades de pessoas físicas ou jurídicas, públicas ou privadas, para servir de referência, prova, informação ou fonte de pesquisa (Moçambique, 2007).

Foram definidos como objetivos do SNAE 2007, através do artigo 4: harmonizar as diversas fases da gestão de documentos, atendendo às especificidades dos órgãos geradores e acumuladores dos acervos; assegurar a proteção e preservação dos documentos gerados e recebidos no exercício de funções dos órgãos e instituições públicos e privados, revestidos de valor administrativo, histórico e científico; facilitar o acesso público ao património arquivístico nacional de acordo com as necessidades de informação, respeitando o disposto nas normas de Segredo de Estado e demais leis que regem o acesso à informação; etc. (Moçambique, 2007) Com estes objetivos

podemos inferir uma tendência integrada da arquivística que se pretende instaurar em Moçambique. Também consegue-se inferir o cuidado que se previu dar aos documentos face às questões sigilosas, como podem ser o caso de documentos contendo dados pessoais.

Sobre a composição desta versão do sistema, pode ser visto no seu artigo 5 que ele integra os seguintes órgãos: “Art. 5, [...] órgão director central; órgãos centrais; órgãos provinciais; e, órgãos distritais” (Moçambique, 2007). Importa notar que não se faz referência a arquivos desses órgãos ou a arquivos públicos nos diferentes níveis da estruturação e administração do Estado moçambicano. Nem mesmo os indicados órgãos centrais, provinciais e distritais, são de competência arquivística.

O n.º 2 do Artigo 5 estabelece que “a entidade que superintende na administração pública é o órgão director central do sistema.” (Moçambique, 2007). Chamamos atenção para a formulação deste número. Ele denota uma ambiguidade e gravidade pela falta de clareza, objetividade e coerência. Exercícios de substituição de preposições ou de acréscimos de palavras não ajudam muito, pois no bom rigor, não cabe ao leitor “preencher as frases das normativas”.

Ainda no mesmo Artigo, no n.º 3, apontam que os órgãos centrais, provinciais e distritais compreendem, cada um e a seu nível, arquivos correntes; unidades de gestão de documentos dos arquivos intermediários; e, comissões de avaliação de documentos.

No n.º 4, AHM é indicado como “o órgão de gestão de documentos na fase permanente e de assessoria ao órgão director central do Sistema” (Moçambique, 2007). Este número parece-nos problemático pois, atendendo que o AHM acomoda os documentos da fase ou idade permanente, ou ainda de valor secundário, e considerando o conceito de gestão de documentos sobre o qual discorreremos na esteira da nossa fundamentação teórica, há uma contradição clara. Isto denota uma provável falta de auscultação à especialistas da área arquivística para a conceção desta normativa. O que parece demonstrar que os problemas identificados pela EGRSP de 2001, continua(ra)m a serem ignorados.

No que concerne às funções dos órgãos do SNAE 2007, no Artigo 6 estão arroladas as funções do órgão director central, que são:

- a) dirigir e coordenar centralmente as actividades de gestão de documentos desenvolvidas pelos órgãos centrais, provinciais e distritais do Sistema;
- b) coordenar a implantação e implementação do Sistema Nacional de Arquivos do Estado;
- c) normar e orientar tecnicamente as actividades de gestão de documentos de arquivo;
- d) acompanhar, supervisionar e monitorar a aplicação de normas técnicas e tecnologias de gestão de documentos de arquivo;
- e) promover a disseminação de normas técnicas e informações de interesse, junto dos outros órgãos do sistema;
- f) propor normas de acesso aos documentos dos arquivos públicos, respeitando as normas de acesso à informação e Segredo Estatal;
- g) promover a capacitação dos funcionários responsáveis pela gestão de documentos;
- h) promover e manter o intercâmbio de cooperação técnica com instituições congêneres nacionais e internacionais;
- i) manter um cadastro geral actualizado das unidades que desempenham actividades de arquivo no âmbito do Sistema (Moçambique, 2007).

Fizemos questão de apresentar todas as funções arroladas na normativa para podermos inferir que o SNAE 2007 deixa de lado uma das funções do órgão central, uma função que nos parece de capital importância, a de “Propor a política geral de acesso aos arquivos, respeitadas as normas de confidencialidade a que estão sujeitos determinados documentos”, nos termos do SNA 1992.

O Artigo 13 que versa sobre “custódia”, dispõe que as instituições detentora de custódia de documentos das fases corrente e intermediária devem assegurar: a proteção e conservação da integridade, fidedignidade e autenticidade desses documentos; o acesso público às informações contidas nesses documentos; a preservação do sigilo dos documentos que dizem respeito à ordem nacional e à segurança pública, ao resguardo da inviolabilidade da intimidade e da vida privada, entre outros relativos aos segredos protegidos por lei; a eliminação dos documentos que, depois de esgotado o seu valor corrente, estejam desprovidos de valor permanente. Compreende-se neste artigo que as diversas instituições públicas, em particular, devem proteger os dados pessoais que estão contidos nos diferentes documentos que corporizam essas instituições.

Um outro aspecto inaugurado pelo SNAE 2007 é a previsão de sanções em caso de infrações, conforme o Artigo 19, “os funcionários dos órgãos, que integram o presente Sistema, respondem disciplinar, criminal e civilmente, pelas infracções que cometerem no exercício das suas funções, nos termos da lei” (Moçambique, 2007). Podemos incluir nessas infrações, não detalhadas pelo SNAE 2007, a preservação do carácter sigiloso dos documentos que dizem respeito à intimidade e à vida privada.

McGarry (1999) confessou que “a privacidade possui uma incômoda relação com o acesso” (McGarry, 1999, p. 184). De fato, alguns olham como dois aspectos totalmente antagônicos e nós os percebemos como duas faces da mesma moeda. O SNAE 2007 decretou no Artigo 16, sobre o acesso aos arquivos, que

1. É permitido o acesso aos documentos depositados em arquivos públicos a todos os interessados, salvaguardando-se os princípios que regulam o segredo estatal e a inviolabilidade da vida privada.
2. Os arquivos de acesso condicionado no roteiro do segredo estatal poderão ser livremente consultados pelos utentes, após a sua desclassificação ou término do prazo de validade do acto de classificação (Moçambique, 2007).

Na esteira da questão do acesso à informação ou direito à informação, e que significa igualmente direito de acesso à documentos (de arquivo), pensamos que é relevante pontuarmos aqui a Lei do Direito à Informação, Lei n.º 34/2014, 31 de dezembro de 2014, antes de nos esmerarmos sobre a versão em vigor do sistema nacional de arquivos, o SNAE 2018.

Gostaríamos de começar olhando para o glossário desta lei e perceber qual é a conceção de alguns termos-chave utilizados nesta normativa. Assim, sem necessariamente nos atermos a ordem alfabética, no âmbito desta lei considera-se

arquivo [o] conjunto de documentos de qualquer época e forma que, independentemente da natureza ou suporte de informação, são acumulados e conservados em razão do seu valor ao longo das actividades de pessoas físicas ou jurídicas, públicas ou privadas, para servirem de referência, prova, informação ou fonte de pesquisa (Moçambique, 2014).

São “dados pessoais [as] informações relativas a pessoas físicas identificadas ou identificáveis, registada manual ou informaticamente” e “Informação pessoal [é aquela] informação contendo dados identificativos de uma determinada pessoa e dados sobre o universo da sua vida privada e pública” (Moçambique, 2014).

Informação de interesse público é no âmbito desta lei,

a que se encontra na posse das entidades referidas no Artigo 3 da presente Lei que contribua para o exercício da cidadania, ou na manutenção ou construção de valores na sociedade, que promova o bem-estar pessoal ou social do cidadão, que contribua para o bem comum, em conformidade com as restrições previstas na presente Lei (Moçambique, 2014).

Pensamos que cada cidadão moçambicano tem, no acesso aos seus dados e/ou na comunicação do tratamento dos seus dados pelas entidades citadas acima, informação que contribui para o seu bem-estar pessoal, portanto, informação de interesse público.

A informação classificada é, no âmbito desta Lei, aquela que reporta dados de natureza considerada segredo de Estado, secreta, confidencial ou restrita. O documento classificado é definido, por sua vez, como aquele que

contém dados ou informações militares, políticas, económicas, comerciais, científicas, técnicas ou quaisquer outras, cuja divulgação ponha em causa, prejudique, contrarie ou perturbe a segurança do Estado e do povo ou a economia nacional (Moçambique, 2014).

Temos a percepção que de algum modo, esta lei não coloca no mesmo patamar o documento classificado e a informação classificada, sendo que nenhum destes termos apresenta na sua definição, uma menção clara dos dados pessoais.

Tendo visitado a semântica dos termos em uso nesta lei, é oportuno mobilizarmos os princípios que a orientam. Conforme o Artigo 4, em Moçambique o exercício do direito à informação rege-se, entre outros, pelos princípios de respeito à dignidade da pessoa humana; transparência da atividade das entidades públicas e privadas; e, respeito pela informação classificada. Nos termos do Artigo 5, o respeito pela dignidade significa que “o exercício do direito à informação deve salvaguardar outros direitos e interesses protegidos pela Constituição, nomeadamente, o direito à honra, ao bom-nome, à reputação, à defesa da imagem pública e à reserva da vida privada” (Moçambique, 2014). Este princípio não deixa dúvidas que ele é inerente à proteção de dados pessoais.

Se visitarmos o Artigo 7, princípio da transparência, segundo o qual “as entidades públicas e privadas investidas de poder público, por lei ou por contrato, exercem as respectivas actividades no interesse da sociedade, devendo, por isso, as mesmas serem de conhecimento dos cidadãos” (Moçambique, 2014), percebemos que as instituições têm o dever de comunicar ao titular de dados pessoais, toda a atividade que recai sobre esses dados, desde a coleta à eliminação. Até porque, conforme o Artigo 13, “o exercício do direito à informação compreende a faculdade de solicitar, procurar, consultar, receber e divulgar a informação de interesse público na posse das entidades [...]” (Moçambique, 2014).

Sobre o acesso à informação, o n.º 1 do Artigo 15, estabelece que “o pedido de informação é dirigido ao dirigente ou servidor com competências no domínio de gestão de documentos, informação e arquivos, devendo o requerente identificar-se devidamente, apresentando o tipo de informação que solicita”. Isto é interessante

particularmente se questionarmos qual é o perfil desses servidores e/ou dirigentes, incluindo sua formação superior.

O Artigo 17 estabelece que “a disponibilização da informação é gratuita, excepto se implicar a reprodução, a declaração autenticada e a passagem de certidão, casos em que está sujeita a taxas” (Moçambique, 2014). Parece que esta regra é contrariada pela alínea b) (em particular, para não falar de todo o número ou mesmo toda a normativa), do n.º 6 do Artigo 63 da Lei das Transações Electrónicas, onde está plasmado que toda a pessoa tem o direito de “ser comunicado a respeito de seus dados dentro de um período razoável, mediante pagamento de uma taxa” (Moçambique, 2017).

A Lei do Direito à Informação indica suas restrições e limites no Artigo 20. Conforme o seu n.º 1, “o direito à informação pode ser restringido, condicionado ou limitado quando a informação solicitada tenha sido classificada como segredo de Estado, secreta, restrita e confidencial” (Moçambique, 2014). Estas restrições são aplicadas quando se tratar de, entre outros casos, “dados pessoais constantes de ficheiros electrónicos em poder de autoridades públicas ou privadas” e “informação referente à vida e intimidade privada dos cidadãos” (Moçambique, 2014).

Portanto, se estas e outras restrições e limites estabelecidos por esta lei forem violadas, já estão previstas sanções, no capítulo IV. No que toca à violação da dignidade humana, o Artigo 38 prevê que “a violação dos direitos de personalidade é passível de punição nos termos do regime dos crimes contra a honra, previsto na legislação penal” (Moçambique, 2014).

Acabamos de apreciar a Lei do Direito à Informação, onde conseguimos identificar sua profunda relação com a proteção de dados pessoais e a gestão de documentos, como estamos a ver também através dos chamados sistema nacional de arquivos do Estado. Assim, como havíamos apontado anteriormente, passamos a seguir, a olhar para a versão de 2018, aprovada pelo Decreto n.º 84/2018, de 26 de dezembro.

Esta versão aponta, de forma explícita, os seus subsistemas. Vale lembrar que esta questão foi recomendada através do EGDAE em 2006, como vimos mais acima. Contudo, ela aparece ostentando este nome, não imediatamente no SNAE 2007, mas sim 12 anos depois. O Artigo 2 (subsistemas do SNAE) aponta que “o SNAE integra,

entre outros, os seguintes subsistemas: Arquivos dos órgãos centrais; arquivos dos órgãos da província; Arquivos dos órgãos do distrito; Arquivos das autarquias locais” (Moçambique, 2018a). Ainda assim, os subsistemas do SNAE 2018, parecem contrários à lógica prevista pela EGDAE de 2006, que entendemos ser um instrumento orientador de toda a ação na área arquivística pós-2006. A estratégia aponta que “as instituições autónomas e independentes do poder executivo poderão desenvolver os seus subsistemas de gestão de documentos e arquivos [...]” (EGDAE, 2006, p. 4).

Quanto a estrutura do sistema, no Artigo 6, são apontados como órgãos de gestão do SNAE: órgão diretor central; órgão coordenador (Centro Nacional de Documentação e Informação de Moçambique – CEDIMO); órgão de assessoria e gestão de documentos na fase permanente (AHM); órgão de gestão de informação classificada (CPISE); órgãos centrais (órgãos de soberania, ministérios e demais instituições de nível central); órgãos da província (secretarias provinciais, direções, delegações provinciais e demais instituições de nível provincial); órgãos do distrito (secretarias distritais, serviços, delegações distritais e demais instituições de nível distrital); autarquias locais. Nota-se aqui, à semelhança do SNAE 2007, que não se referem aos arquivos dos órgãos centrais, arquivos provinciais, arquivos, distritais ou ainda arquivos municipais ou arquivos das autarquias locais. Uma perspectiva nessa linha de ideia é, nessa versão do SNAE, colocada em termos de subsistemas, como apresentamos acima. Depreende-se assim que o SNAE 2018 não é composto por arquivos, nas perspectivas que podemos aventar. Nharreluga entende que

O projeto de Sistema Nacional de Arquivos, reiterado ao longo do tempo, persiste nesta terceira versão desprovida de entidades arquivísticas em sua composição, numa perspectiva em que, se a prática arquivística nacional não é pautada por uma política nacional de arquivos, tampouco as leis que instituíram as sucessivas versões daquele projeto de sistema apontam parâmetros de uma possível política nacional de arquivos (Nharreluga, 2021, p. 147).

Conforme o n.º 3 do Artigo 8, a gestão dos arquivos correntes e intermediários é feita sob a coordenação do CEDIMO. Uma instituição não arquivística. Aliás o órgão diretor central, nos termos atuais, Ministério da Administração Estatal e Função Pública, também não é uma instituição arquivística. As suas funções estão expostas no Artigo 10. São elas: Garantir a implementação correta do SNAE; Promover e controlar a aplicação das regras de documentação, publicação e arquivo do Estado; Promover a observância das regras de Segredo do Estado; Promover a preservação da memória institucional Aprovar normas e homologar políticas sobre gestão de

documentos de arquivo; Aprovar os Planos de classificação e Tabelas de Temporalidade de Documentos das Atividades-fim, bem como os Classificadores de informação Classificada Setoriais Promover a construção de edifícios para guarda de documentos na fase permanente; Manter o cadastro geral atualizado dos órgãos e instituições que implementam o SNAE; e, Promover e manter intercâmbio e cooperação técnica com instituições congêneres nacionais e internacionais.

As “políticas” voltam a fazer parte das funções do órgão central do sistema, desta vez com a atribuição para homologá-las. Aparecem, pela primeira vez de forma explícita, a função de “promover a construção de edifícios para guarda de documentos na fase permanente” e de “promover a preservação da memória institucional”. Por outro lado, a “capacitação e/ou formação, de recursos humanos” desaparece das funções do órgão central (Moçambique, 2018a).

Sobre o acesso aos arquivos, o n.º 1 do Artigo 28 aponta que podem ser acessados os documentos em arquivos públicos por todos os interessados, respeitando-se os princípios que regem o segredo do Estado e inviolabilidade da vida privada. Nos perguntamos quais são os arquivos públicos (em plural mesmo, e em vários níveis da estrutura estatal) existentes em Moçambique?

O SNAE 2018, introduz um aspecto interessante através do seu Artigo 32, onde aponta que “a gestão de documentos electrónicos de arquivo será objeto de legislação específica” (Moçambique, 2018a).

À semelhança do SNAE 2007, o SNAE 2018 no seu Artigo 33 fala da responsabilização disciplinar, criminal ou civil à que incorrem os funcionários e agentes do Estado pelas infrações que cometerem no exercício das duas funções. Isto significa que se estes violarem a privacidade do cidadão ou ainda se desprotegerem os dados pessoais contidos nos documentos, poderão ser sancionados.

Achamos bastante curioso o glossário do SNAE 2018, ao encontrarmos definidos os termos “arquivo provincial”, “arquivo distrital” e “arquivo autárquico”, termos que não ocorreram no corpo do texto da normativa. Aliás são termos que contrastam com as noções por trás dos termos “órgãos da província”, “órgãos do distrito” e “autarquias locais”.

Tomando os aspectos apresentados aqui e outros do SNAE 2018, Nharreluga (2021) conclui que

se o que se pretende em Moçambique é a gestão de documentos e arquivos, então se torna urgente abandonar o projeto de Sistema Nacional de Arquivos nesse país para se tomar medidas condizentes à gestão de documentos e arquivos, em uma iniciativa de construção do campo arquivístico nacional, norteado pela formulação e implementação de políticas públicas arquivísticas em termos mais incisivos que no projeto atual (Nharreluga, 2021, p. 151).

O autor não para por aí e vai mais longe, fazendo uma reflexão em torno de algumas instituições que compõem o SNAE 2018 e a configuração que devem ter no cômputo de uma política arquivística nacional. Fazemos a seguir, uma longa citação das falas deste autor.

Enquanto única instituição arquivística em nível nacional, a refundação do AHM em todas as suas dimensões é urgente para adequá-la à atual exigência de organização e gestão arquivísticas em nível nacional. Caso essa visão não seja oportuna, seria o caso de transformar o CEDIMO – sem descurar da experiência do AHM –, de uma instituição com funções mistas para uma instituição arquivística e reorientar as suas competências, dotando-o de capacidade técnico-científica para além de suas atuais competências político-administrativas. Se nenhuma dessas opções se mostrar viável, abre-se espaço para a criação de uma instituição arquivística pública de âmbito nacional – independente das duas instituições –, aglutinando o que há de melhor nas duas, na definição das suas atribuições. Entretanto, qualquer que seja a opção, ela deve ocorrer dentro da perspectiva de uma política nacional de arquivos, diferentemente dos termos atuais de busca por um projeto que não contribui para a organização e desenvolvimento da área (Nharreluga, 2021, p. 153).

Comparamos, no quadro abaixo, algumas definições (in)existentes nas normativas que instituem as diferentes versões do chamado sistema nacional de arquivos em Moçambique.

Quadro 4 – Definições nas versões do Sistema Nacional de Arquivos (de Estado)

Definições	SNA 1992	SNAE 2007	SNAE 2018
Acesso aos documentos	O acesso público aos documentos depositados em arquivos centrais só poderá ocorrer mediante autorização prévia dos órgãos a que se subordinam.	É permitido o acesso aos documentos depositados em arquivos públicos a todos os interessados, salvaguardando-se os princípios que regulam o segredo estatal e a inviolabilidade da vida privada.	É permitido o acesso aos documentos depositados em arquivos públicos a todos os interessados, salvaguardando-se os princípios que regulam o segredo estatal e inviolabilidade da vida privada
Arquivo(s)	Os conjuntos de documentos que, independentemente da natureza ou do suporte da informação, são reunidos por processo	o conjunto de documentos de qualquer época e forma que, independentemente da natureza ou do suporte da informação, são acumulados e conservados	O conjunto de documentos de qualquer época e forma que, independentemente da natureza ou do suporte

	de acumulação ao longo das actividades de pessoas físicas ou jurídicas, públicas ou privadas, e conservados em razão do seu valor.	em razão do seu valor ao longo das actividades de pessoas físicas ou jurídicas, públicas ou privadas, para servir de referência, prova, informação ou fonte de pesquisa	da informação, são acumulados e conservados em razão do seu valor ao longo das actividades de pessoas singulares ou colectivas, públicas ou privadas, para servir de referência, prova, informação ou fonte de pesquisa.
Dado(s)	Nada consta	Nada consta	Nada consta
Dados pessoais	Nada consta	Nada consta	Nada consta
Documento	Nada consta	Nada consta	Unidade de registo de informações qualquer que seja o suporte ou formato.
Órgão central	Arquivo Histórico de Moçambique	A entidade que superintende na administração pública é o órgão director central do sistema.	O órgão director central do SNAE é a entidade que superintende a área de gestão de documentos e arquivos do Estado.
Privacidade	Nada consta	Nada consta	Nada consta
Sistema de arquivo	Nada consta	conjunto de elementos (entidades, meios, procedimentos) que funcionam de modo articulado, tendo em vista a gestão dos documentos produzidos ou recebidos por um organismo no exercício das suas actividades.	Conjunto de arquivos que, independentemente da posição que ocupam nas respectivas estruturas administrativas funcionam de modo integrado e articulado na prossecução de objectivos comuns.

Fonte: Elaborado pela autora

O quadro que acabamos de apresentar, ilustra como, em pelo menos três versões do chamado sistema nacional de arquivos, alguns termos não fazem parte do arcabouço de suas palavras-chave. Notamos que nada consta definido sobre o que é considerado privacidade, dados e dados pessoais, no âmbito dos três decretos, respectivamente. Quanto ao acesso aos documentos, se na versão de 1992, para além de uma tendência maior de inaccessibilidade, nada constava sobre a vida privada dos cidadãos, nas versões subsequentes, infere-se uma maior abertura ao acesso e a previsão do respeito à inviolabilidade da vida privada. Ora, pressupõe-se que a integração de alguns termos que levantamos aqui seja acautelada pelo e-SNGD.

5.3 O Sistema Nacional de Gestão Documental (e-SNGD): um projeto

O Ministério da Administração Estatal e Função Pública (MAEFP) e o Ministério da Ciência, Tecnologia e Ensino Superior (MICTES) produziram, em 2022, a “Informação sobre o desenvolvimento do Sistema Nacional De Gestão Documental (e-SNGD)”. O e-SNGD é “uma plataforma desenvolvida em uma arquitetura atualizada, utilizando as tecnologias mais avançadas disponíveis no mercado. Seguindo essa tendência, a aplicação é desenvolvida em plataforma web” (MAEFP; MICTES, 2022, p. 4), sendo seu principal objetivo dotar a Administração Pública de mecanismos tecnológicos de acompanhamento dos processos de gestão de documentos e arquivos do Estado usando meios tecnológicos (MAEFP; MICTES, 2022, p. 3).

O e-SNGD contempla a CloudGov e o e-Doc como seus dois subsistemas. A CloudGov é um subsistema de gestão de ficheiros armazenados que funciona como um arquivo permanente. Ela permite carregamento e descarregamento de arquivos e diretórios; partilhas; visualização e edição colaborativa de documentos; e, controlo de atividades sobre os arquivos e diretórios. O eDoc é um subsistema de gestão de documentos orientado a processos internos de cada instituição e visa essencialmente a interação entre os utentes (cidadãos ou instituições) e os provedores de serviços (instituições públicas). Ele permite ao provedor de serviços, entre outras ações, classificar os documentos por assunto, grau de sigilo e quanto à brevidade; preservar os documentos no arquivo intermediário e permanente, acautelando a questão de segurança e da transparência; definir níveis de acesso aos documentos nas diversas fases. E permite ao utente fazer o seu auto-registro para acessar a Plataforma; requisitar serviços; submeter pedidos de serviços e informação; acompanhar a tramitação dos seus pedidos; acessar informação conforme a Lei do Direito à Informação, entre outras ações (MAEFP; MICTES, 2022).

Conforme o documento, são intervenientes na conceção do e-SNGD: o Órgão Diretor Central do SNAE, através do Órgão Coordenador do SNAE; o MICTES, através do Instituto Nacional de Governo Electrónico (INAGE), órgão coordenar e fornecedor de serviços de Governo eletrónico; o AHM; e, a CPISE (MAEFP; MICTES, 2022, p. 3).

5.4 Principais atores da arena arquivística moçambicana

Esta subseção é reservada a apresentação e análise dos principais atores no cenário arquivístico moçambicano, entidades que são referenciadas na principal legislação arquivística daquele país. Como indicamos acima, o SNAE 2007 instituiu, para além de outros aspectos, o Conselho Nacional de Arquivos (CNA) e a Comissão Nacional de Avaliação de Documentos (CNAD). O SNAE 2018 destaca o Centro Nacional de Documentação e Informação de Moçambique (CEDIMO), o Arquivo Histórico de Moçambique (AHM, que é igualmente destaque no SNA 1992 como órgão central) e a Comissão Nacional para Implementação das Normas de Segredo do Estado (CPISE). Assim, estes constituem os principais atores neste contexto. Com a exceção de CPISE que foi abordado mais acima, a seguir passamos a nos debruçar sobre estes atores ao detalhe.

5.4.1 Arquivo Histórico de Moçambique (AHM)

O AHM é uma unidade orgânica da UEM. Tem sob sua custódia um universo diversificado de património arquivístico constituído por fundos e coleções, nos mais variados tipos e suportes, desde o séc. XVIII até à atualidade.

A ideia de se criar o AHM surgiu num contexto em que o Governo Colonial não tinha recursos necessários para o efeito. Deste modo, decidiu, através da Portaria 2.264, de 27 de junho de 1934, incumbir à Repartição de Estatística as tarefas do futuro AHM e da futura Biblioteca da Colónia. E em 1939, através do Diploma Legislativo 635, de 19 de abril, foi atribuída ao AHM a dupla tarefa de Instrumento de Cultura Histórica e de Arquivo do Governo da Colónia.

Em 1957 o AHM foi transferido da Repartição de Estatística para os Serviços de Instrução e incorporado na sua estrutura administrativa o Museu Histórico Militar da Fortaleza de Nossa Senhora da Conceição, de Lourenço Marques, em consequência do Decreto-Lei 41:472, de 23 de dezembro. No ano seguinte, o Decreto 42:030, de 31 de dezembro, reafirma sua importância como arquivo geral e depósito legal da província e, nomeia o primeiro diretor do AHM.

Em 1943 o AHM inaugurou o edifício construído especificamente para albergar os vários acervos sob sua custódia de onde foi desalojado através do Diploma-Legislativo 2.632, de 7 de agosto de 1965, passando a ocupar parte do edifício onde tinha sido instalada a Biblioteca Nacional.

Em 1976 o AHM foi desligado dos Serviços de Instrução e integrado na estrutura administrativa da UEM. A nova tutela permitiu a esta instituição criar infraestruturas indispensáveis e levar a cabo o projeto de recolha de documentação colonial que até à data da independência encontrava-se dispersa em todo o país e, de documentos sobre Moçambique existentes em Portugal e Itália. Foi igualmente feito um investimento na formação de quadros e capacitação de técnicos internos e externos, em matérias de documentação.

Criado em 1934 e, desde 1976, dependendo administrativamente da Universidade Eduardo Mondlane, “o AHM é considerado um dos melhores arquivos da África ao sul do Sahara”. Para a documentação dos sécs. XV a XIX, desde 1978 que o AHM, por acordos firmados com Portugal, iniciou um programa de microfilmagem dos arquivos históricos de Portugal, com interesse para Moçambique (Amaral, 1994, p. 8-9).

Para complementar as fontes escritas e permitir a reconstituição histórica de certos períodos ou processos sociais, o AHM deu início ao projeto de recolha de fontes orais para a história de Moçambique, em 1980.

Dez anos depois de intenso trabalho de recolha, tratamento e organização dos acervos documentais, seguiu-se a fase de divulgação. Neste contexto inicia-se a produção da Revista Arquivo, que tinha por objetivo divulgar a informação de interesse para o ensino e a investigação.

Na tentativa de assegurar a proteção do património arquivístico nacional, disciplinar a custódia e o acesso à informação, o governo aprovou o Decreto n.º 33/92, de 26 de outubro, que cria o Sistema Nacional de Arquivos (SNA) e atribui ao AHM a função de órgão central (Moçambique, 1992). Este sistema não avançou devido a problemas estruturais e carência de recursos humanos qualificados. Quinze anos mais tarde o Decreto n.º 36/2007, de 27 de agosto, altera o SNA passando a denominar-se Sistema Nacional de Arquivos de Estado (SNAE) e transfere a função de órgão central do AHM para a entidade que superintende na administração pública, Ministério da Administração Estatal e Função Pública, e atribui ao AHM a função de órgão de assessoria (Moçambique, 2007). Em 2018 o governo aprova a revisão do

SNAE e revoga o Decreto n.º 36/2007, através do Decreto n.º 84/2018, de 26 de dezembro, onde o AHM é designado “órgão de assessoria e gestão de documentos na fase permanente” (Moçambique, 2018a).

5.4.2 Centro Nacional de Documentação e Informação de Moçambique (CEDIMO)

O Centro Nacional de Documentação e Informação de Moçambique (CEDIMO) tem suas origens na estrutura do Banco Central de Moçambique, o Banco de Moçambique (BM), onde funcionou como seu centro de documentação e informação. Há também indicações de que essa origem na estrutura do BM está aliada à penhora de uma biblioteca particular anos 1970 (Nharreluga, 2014). Nharreluga conta que

[...] o Centro Nacional de Documentação e Informação de Moçambique – assim batizado em 1977 quando foi determinada a alteração de sua designação pelo Decreto 40/77, de 27 de setembro, e designado, abreviadamente, daí em diante, por CEDIMO – emerge na estrutura da administração direta do Estado, em 1977, da “necessidade de dispor [o governo] de uma estrutura de documentação e informação classificada [...] nacional, como primeiro passo para a planificação e implementação do Sistema Nacional de Documentação (Nharreluga, 2014, p. 210).

Antes de falarmos com mais detalhes sobre o CEDIMO, vamos rapidamente revisitar o estatuto orgânico do Ministério da Administração Estatal e Função Pública (MAEFP), que é o órgão central do aparelho do Estado responsável pela organização, funcionamento e inspeção da Administração Pública, prevenção e gestão de calamidades, bem como pela gestão estratégica dos recursos humanos do Estado (Artigo 1). Mas também é a instituição que superintende a área da informação e documentação em Moçambique e que, sobretudo, é a instituição à que se subordina o CEDIMO, conforme o Artigo 5º da Resolução n.º 2/2015, de 24 de junho.

Desta feita, citamos aqui algumas das atribuições do MAEFP: “direcção Central da Administração Local do Estado; gestão da reforma do sector público; coordenação do processo de descentralização; organização do sistema de informação, documentação e arquivos do Estado; formação e capacitação dos recursos humanos do Estado” (Moçambique, 2015). Assim, para a concretização destas e outras atribuições, o MAEFP tem como competências na área da “Gestão da documentação e arquivo do Estado” (Artigo 8): “coordenar a implementação do Sistema Nacional de Arquivos do Estado; promover e controlar a aplicação das regras de documentação,

publicação e arquivos do Estado; promover observância das regras de segredo do Estado; e promover a preservação da memória institucional” (Moçambique, 2015).

Estas competências são postas em marcha através do CEDIMO, como fizemos indicação anteriormente. O estatuto orgânico do CEDIMO foi revisto em 2023 e aprovado pela Resolução n.º 8/2023, de 9 de maio de 2023. O Artigo 1º desta resolução define a natureza do CEDIMO como sendo “instituto público, [...] responsável pela organização do sistema de documentação, de registo, de arquivos do Estado e de informação da Administração Pública, de categoria B, dotada de personalidade jurídica e autonomia administrativa” (Moçambique, 2023). Conforme o Artigo 4º, são atribuições do CEDIMO:

- a) elaboração de propostas de normas para a implantação e desenvolvimento do sistema de documentação, registo e arquivos do Estado;
- b) divulgação e promoção da aplicação do sistema de documentação, registo e arquivos do Estado;
- c) divulgação das normas que regem o funcionalismo público;
- d) recolha, sistematização, divulgação e arquivamento da informação de interesse da Administração Pública;
- e) realização de estudos e pesquisas sobre a gestão documental e acesso à informação na Administração Pública;
- f) monitoria e assistência técnica aos órgãos e instituições da Administração Pública, no âmbito da gestão de documentos e arquivos e acesso à informação;
- g) divulgação e coordenação de acções de implementação da Lei do Direito à Informação e legislação complementar; e
- h) promoção e realização de intercâmbio com instituições congéneres nacionais e estrangeiras da área de gestão documental e arquivos do Estado e acesso à informação (Moçambique, 2023).

O Artigo 5º, apresenta as competências do CEDIMO. No que toca à gestão de documentos, compete ao CEDIMO:

- a) elaborar propostas de políticas e estratégias de gestão de documentos e arquivos do Estado;
- b) dirigir normativa e metodologicamente o sistema de documentação, registo e arquivo do Estado;
- c) investigar e desenvolver técnicas de gestão de documentos e arquivos aplicáveis na Administração Pública;
- d) assegurar a gestão do sistema de documentação, registo e arquivos do Estado em coordenação com outras unidades, organismos e agências especializadas;
- e) promover a criação de unidades de gestão de documentos nos órgãos e instituições da Administração Pública;
- f) garantir a criação das comissões de avaliação de documentos nos órgãos e instituições da Administração Pública;
- g) promover a formação e valorização profissional dos funcionários da área de gestão documental e arquivos do Estado;
- h) assistir tecnicamente aos órgãos e instituições da Administração Pública na elaboração dos planos de classificação e tabelas de temporalidade das actividades-fim;

- i) pronunciar-se sobre as propostas de classificadores de informações classificadas sectoriais;
- j) promover a cultura de avaliação de documentos nos órgãos e instituições da Administração Pública; e
- k) pronunciar-se sobre as propostas de eliminação de documentos da Administração Pública e das Entidades Descentralizadas (Moçambique, 2023).

Esperamos que com as competências adquiridas por este estatuto de 2023, venha a ser elaborada, formalizada e aprovada uma política arquivística nacional que há muito Moçambique carece. Ainda assim, continuamos a estranhar que estas, competências típicas de um arquivo nacional, sejam atribuídas a uma instituição não arquivística e que, como vimos, coordena o sistema nacional de arquivos do estado em Moçambique.

A estrutura do CEDIMO obedece, como estabelecido no Artigo 13º, Serviços Centrais de Documentação e Arquivos do Estado; Serviços Centrais de Informação; Gabinete Jurídico; Departamento de Administração e Finanças; Departamento de Recursos Humanos; Departamento de Planificação e Cooperação; e, Departamento de Aquisições.

São funções dos Serviços Centrais de Documentação e Arquivos do Estado (Artigo 14º)

- a) propor normas de funcionamento e actualização do sistema de documentação, registo e arquivo do Estado;
- b) promover, divulgar e realizar estudos e pesquisas sobre gestão de documentos e arquivos na Administração Pública;
- c) propor políticas e estratégias de gestão, registo e arquivo de Documentos do Estado;
- d) coordenar, monitorar e avaliar a implementação do sistema de documentação, registo e arquivo do Estado;
- e) assistir tecnicamente os órgãos e instituições da Administração Pública na organização e gestão de documentos e arquivos;
- f) disseminar, monitorar e controlar a aplicação das normas e técnicas de gestão de documentos;
- g) promover e realizar actividades de formação e capacitação de funcionários e agentes do Estado em matérias de gestão de documentos e arquivos, em coordenação com instituições da Administração Pública;
- h) promover a modernização dos sistemas de gestão de documentos e arquivos do Estado, através da adopção de novas tecnologias de comunicação e informação;
- i) organizar, gerir e avaliar os documentos do arquivo intermediário do CEDIMO, IP;
- j) pronunciar-se sobre as propostas de eliminação de documentos dos órgãos e instituições da Administração Pública;
- k) promover a criação de unidades de gestão de documentos nos órgãos e instituições da Administração Pública;
- l) garantir a criação de comissões de avaliação de documentos dos órgãos e instituições da Administração Pública;

m) realizar outras actividades que lhe sejam superiormente determinadas, nos termos do presente Estatuto e demais legislação aplicável (Moçambique, 2023).

São funções dos Serviços Centrais de Informação (Artigo 15º):

- a) recolher, sistematizar e publicar informação de interesse da Administração Pública;
- b) promover, divulgar e assegurar a aplicação de normas e estratégias de promoção do acesso à informação de interesse na Administração Pública;
- c) promover e monitorar a implementação da Lei do Direito à Informação e demais instrumentos legais que regulam o acesso à informação;
- d) fiscalizar as condições de consulta de informação nas instituições públicas e privadas abrangidas pelas normas que regulam o direito à informação;
- e) incentivar as instituições abrangidas pela Lei para o uso massivo dos meios de divulgação de informação de interesse público;
- f) pronunciar-se sobre as propostas de classificadores de informações classificadas das actividades-fim sectoriais;
- g) elaborar pareceres sobre o carácter público ou privado da informação na posse de entidades públicas ou privadas abrangidas pela Lei do Direito à Informação;
- h) elaborar o relatório anual sobre a implementação da Lei do Direito à Informação que é submetido ao Órgão Director Central do Sistema Nacional de Arquivos do Estado (SNAE);
- i) promover e realizar actividades de formação e capacitação de funcionários e agentes do Estado em matérias de acesso à informação;
- j) propor estratégias de comunicação e imagem da instituição;
- k) garantir a assistência e manutenção do equipamento informático e gráfico, bem assim a rede intranet do CEDIMO, IP;
- l) gerir a página oficial de internet do CEDIMO, IP;
- m) promover o uso de novas tecnologias de informação e comunicação no CEDIMO, IP;
- n) criar e gerir uma base de dados de informação de interesse público; o) realizar outras actividades que lhe sejam superiormente determinadas, nos termos do presente Estatuto e demais legislação aplicável (Moçambique, 2023).

O CEDIMO faz-se, ou deve se fazer representar ao nível provincial em Moçambique, pelas “delegações provinciais”, que são dirigidas por Delegados Provinciais nomeados pelo Director-Geral do CEDIMO, como se lê no n.º 2 do Artigo 21. Ora, “as Delegações Provinciais subordinam-se ao Director-Geral e atuam em coordenação com o Secretário do Estado na Província” (Moçambique, 2023). Essas delegações devem:

- a) assegurar e coordenar todas as acções operativas a nível da respectiva área de jurisdição;
- b) garantir a aplicação das normas e regulamentos sob tutela do CEDIMO, IP, e implementação dos projectos a nível local;
- c) acompanhar, apoiar e fiscalizar todas as actividades do CEDIMO, IP, na área da sua jurisdição;
- d) propor e gerir os meios materiais, humanos e financeiros necessários ao seu funcionamento;
- e) elaborar inventários periódicos e anuais dos bens patrimoniais e zelar pelo cumprimento do Regulamento do Património do Estado; e

f) elaborar relatórios e submetê-los à apreciação do Conselho de Direcção. (Moçambique, 2023).

5.4.3 Conselho Nacional de Arquivos (CNA)

Embora o Conselho tenha sido instituído em 2007 com o SNAE, foi através do Diploma Ministerial n.º 35/2010, 16 de fevereiro de 2010, que ele foi criado, vista a necessidade de munir o órgão diretor central do SNAE (desde a versão de 2007 e, posteriormente com a revisão desta, na versão de 2018) de mecanismos de consulta para o exercício das suas atividades, por isso, o Artigo 2 deste diploma ministerial, define o CNA como o órgão de consulta do órgão diretor central do SNAE, na definição da política nacional de arquivos públicos e privados e na orientação técnico-normativa da gestão de documentos.

Este conselho é composto por um presidente, o Director Nacional de Estudos e Procedimentos Administrativos do Ministério da Função Pública; um vice-presidente o Director do AHM; pelo Director do CEDIMO; pelo Director-Geral do Instituto Superior de Administração Pública; pelo Secretário Executivo da CPISE; por um representante do Ministério da Educação e Cultura; e, por um representante do Ministério da Ciência e Tecnologia (Artigo 3).

As funções deste conselho são arroladas no Artigo 4. São elas: velar pelo funcionamento do Sistema Nacional e subsistemas de Arquivos do Estado; analisar as propostas de declaração do interesse público de arquivos privados; velar pelos programas nacionais de gestão e modernização de arquivos públicos e privados; analisar os estudos e propostas de revisão do Plano de Classificação, da Tabela de Temporalidade de Documentos das Atividades-Meio e do Classificador de Informações Classificadas⁶; velar pelo funcionamento e o acesso aos arquivos públicos; debruçar-se sobre outros assuntos que se mostrem pertinentes para o Órgão Diretor Central do SNAE.

⁶ A possível redundância vem do próprio nome do instrumento, conforme mencionado.

5.4.4 Comissão Nacional de Avaliação de Documentos (CNAD)

A semelhança do CNA, essa comissão foi instituída pelo SNAE 2007 e criada através do Diploma Ministerial n.º 36/2010, 16 de fevereiro de 2010. É, conforme o Artigo 2, um órgão de assessoria do Órgão Diretor Central SNAE em matérias de avaliação de documentos. Em 2017, este diploma foi alterado, tendo sido aprovado o Diploma Ministerial n.º 45/2017, de 21 de junho, alterando os Artigos 3, 4 e 6 do Diploma Ministerial n.º 36/2010, de 16 de fevereiro, que estabelecem a composição, as funções e o apoio técnico administrativo à Comissão Nacional de Avaliação de Documentos.

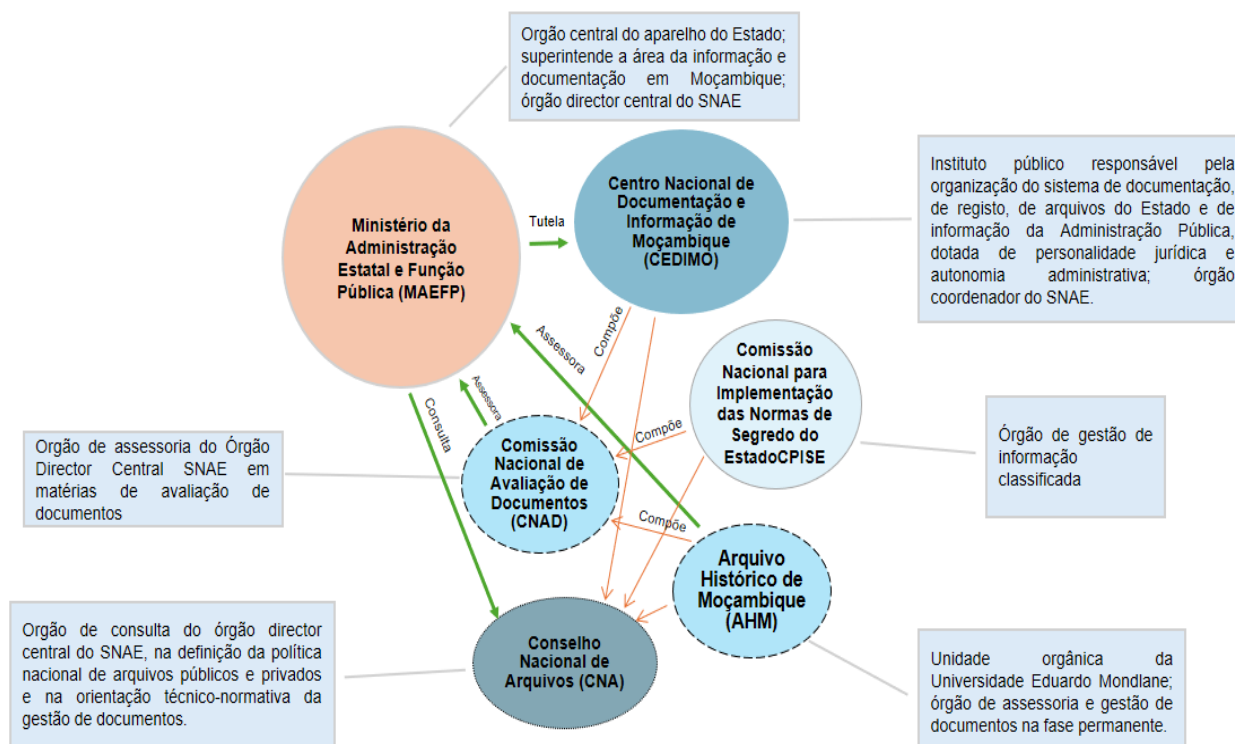
Assim, o Artigo 3 aponta a que

1. A CNAD tem a seguinte composição:
 - a) Director do Centro Nacional de Documentação e Informação de Moçambique (CEDIMO), que a preside;
 - b) Um representante do Arquivo Histórico de Moçambique (AHM);
 - c) Um representante do Fundo Bibliográfico de Língua Portuguesa (FBLP);
 - d) Um representante da Comissão Nacional Para Implementação das Normas do Segredo Estatal (CPISE). (Moçambique, 2017a).

A CNAD tem como funções, ao abrigo do Artigo 4: analisar e emitir pareceres sobre matérias de avaliação de documentos e propostas de planos de classificação e de tabelas de temporalidade de documentos das atividades-fim submetidas ao Órgão Diretor Central do SNAE; assistir técnica e metodologicamente as comissões de avaliação de documentos no exercício das suas atividades; supervisionar os processos de transferência, recolhimento e eliminação de documentos de arquivos; elaborar estudos que permitam avaliar a eficácia do Plano de Classificação e da Tabela de Temporalidade de Documentos das Atividades-Meio da Administração Pública e propor a sua revisão sempre que for necessário; e, avaliar regularmente o funcionamento do SNAE e propor medidas para sua atualização (Moçambique, 2010)

Considerando a descrição feita acima, abaixo representamos estes atores da arena arquivística moçambicana e a relação que estabelecem entre si.

Figura 6 - Principais atores da arena arquivística moçambicana



Fonte: Elaborado pela autora.

5.5 O arquivista moçambicano face à proteção de dados pessoais

Nesta subsecção damos ênfase a dois aspectos que consideramos bastante importantes para a atuação do arquivista moçambicano, em particular, face à questão cada dia mais urgente da proteção de dados pessoais. O primeiro aspecto ligado à formação deste arquivista em que o quadro curricular deve abranger elementos que o dotem de habilidades e competências contemplando o seu papel para proteger os dados pessoais. O segundo aspecto diz respeito às associações profissionais que têm um papel bastante importante na orientação do fazer de seus profissionais membros.

5.5.1 Formação

Para falar da formação do arquivista em Moçambique, é preciso visitar a configuração do ensino superior deste país para que se perceba também qual é o

nível de oferta do curso de arquivologia no nível superior em Moçambique. Porém, para chegar lá é preciso passar pelo Sistema Nacional de Educação, do qual o Ensino Superior é seu Subsistema.

A Lei n.º 18/2018, de 28 de dezembro, estabelece o regime jurídico do Sistema Nacional de Educação (SNE) na República de Moçambique e revoga a Lei n.º 6/92 de 6 de maio, Lei do Sistema Nacional de Educação, indica no seu Artigo 9, que o ensino superior se constitui num dos seus subsistemas. A este, conforme a mesma lei no seu Artigo 17, compete assegurar a formação ao nível mais alto nos diversos domínios de conhecimento técnico, científico e tecnológico necessários ao desenvolvimento do país.

A Lei n.º 1/2023, 17 de março de 2023, Lei que estabelece o regime jurídico do Subsistema do Ensino Superior e revoga a Lei n.º 27/2009, de 29 de setembro, aponta no seu Artigo 2 que ela se aplica às Instituições do Ensino Superior, abreviadamente designadas por IES, públicas e privadas. No Artigo 31, a lei classifica as IES quanto à tipologia, e elas podem ser a) classe A - Universidades e Academias Militares e Paramilitares; b) classe B - Institutos Superiores Politécnicos; c) classe C - Institutos Superiores, e; d) classe D - Escolas Superiores.

O país conta atualmente com cerca de 56 IES, sendo que dessas, apenas duas lecionam os cursos de graduação que formam profissionais de informação, sendo a UEM com os cursos de graduação em Arquivística e graduação em Biblioteconomia e, a ESJ com o curso de Biblioteconomia e Documentação (BD).

Quer dizer, somente a UEM em Moçambique, é que oferece um curso de graduação em Arquivologia. E importa referir que este curso é apenas oferecido na Escola de Comunicação e Artes, na cidade de Maputo, a capital de Moçambique, não estando representado noutras partes de Moçambique. Mas quando é que foi introduzido este curso na UEM? De onde vêm as discussões para a implantação de um curso de arquivologia nesta universidade? Vamos olhar para os Antecedentes da formação de arquivistas em Moçambique.

Só nos anos 90 é que Moçambique, no que tange ao campo de informação, começa a sair do estado de inércia no qual estava mergulhado. Nesta década dá-se início a um processo de formação de quadros moçambicanos, como um dos resultados da capacitação dos primeiros arquivistas e bibliotecários, mas que foram

formados fora de Moçambique em países com alguma tradição nesta área. E que mais tarde estes moçambicanos foram contribuir para que a formação em Arquivologia, Biblioteconomia e Ciência da Informação ocorresse no território moçambicano. Entre os países estão Botswana, Espanha, Brasil e mais tarde Inglaterra, Portugal entre outros (Mangue *et al.*, 2022).

Neste mesmo período, mais concretamente em 1998, é criado o Instituto Médio de Ciências Documentais (CIDOC), que, embora não estivesse a formar arquivistas como tal, foi somando esforços, junto dos esforços do AHM que ia dando cursos de curta duração, para dotar de alguma competência os profissionais que atuavam na área da informação e documentação.

Em 2004, o Departamento de História da UEM fez uma reforma curricular no curso de História de 1989. Com essa reforma foi introduzido um tronco comum e três (3) linhas de opção no curso de graduação em História: História Social, Ensino e Documentação. Contudo, ainda não estavam sendo formados arquivistas em Moçambique. Na linha de Documentação atuaram como docentes alguns dos moçambicanos que tinham estado no Brasil para se formar em Arquivologia e Biblioteconomia.

Em 2008, fruto de um Estudo de Viabilidade para a Implantação do Curso de Ciência da Informação em Moçambique, desenvolvido em parceria entre a Universidade Federal de Minas Gerais (UFMG) e o Fundo Bibliográfico de Língua Portuguesa (que é a instituição que superintende o CIDOC), com o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) do Brasil, é aprovado o curso de graduação em Ciência da Informação em Moçambique que inicia formalmente em 2009 na Escola de Comunicação e Artes da Universidade Eduardo Mondlane (ECA), com especialidades em Biblioteconomia e em Arquivística. Na sequência, em 2010, a Escola Superior de Jornalismo (ESJ) criou o curso de graduação em Biblioteconomia e Documentação.

Um outro elemento que pode ter contribuído para a criação destes cursos e com tais configurações, é a EGDAE, visto mais acima, em que se apontava como “Situação Atual” (naquela altura) da Área de Documentação e Arquivo, em relação ao desenvolvimento de recursos humanos, que

A área de documentação e arquivos é assegurada por poucos profissionais qualificados e sem formação técnica específica desta área, o que é agravado pela sua subvalorização, afectando consequentemente os funcionários da área devido a ausência de carreiras específicas no quadro do Sistema de Carreiras e Remunerações. Tendo, desta forma, como uma das ações estratégicas o desenvolvimento de recursos humanos e é “em face disso que a estratégia adopta como um dos princípios fundamentais a profissionalização dos técnicos afectos nas unidades documentais e arquivísticas (EGDAE, 2006).

Como podemos ver, até esta altura e durante os anos que o currículo da UEM vigorou, não estavam sendo formados, digamos, arquivistas de raiz. O que só veio a suceder como resultado de um processo de reforma curricular do curso de graduação em Ciência da Informação, fruto de auscultação interna de 2011. Assim, o curso de graduação em Arquivística (assim denomina-se), começa a ser operacionalizado em 2016 com a duração de 4 anos. Podemos dizer que os primeiros arquivistas formados em Moçambique começam a ser lançados para o mercado de trabalho a partir de 2020. Será que no quadro curricular da formação destes arquivistas cabem questões de proteção de dados pessoais? Procuramos conhecer o currículo deste curso para responder à nossa inquietação.

Lecionado tanto no período diurno (manhã e tarde) assim como noturno, o curso de graduação em Arquivística, conforme a UEM (2014) aponta, forma profissionais especializados nos âmbitos teórico, prático, ético e deontológico, em Arquivos para os sectores público e privado. Portanto é objetivo geral do curso

Formar arquivistas com uma visão crítica e interdisciplinar, dotados de competências e habilidades e com consciência do seu papel, tanto institucional no apoio ao processo de tomada de decisão e à constituição do património arquivístico nacional. quanto social na eliminação de barreiras de acesso à informação (UEM, 2014, p. 7).

Na estrutura do curso, fazem parte disciplinas nucleares; disciplinas complementares, disciplinas opcionais; estágios curriculares e Trabalho de conclusão de Curso. Vamos, no quadro que se segue, dar maior destaque para as disciplinas nucleares, apontando para cada uma delas a sua carga horária e o período em que são ministradas.

Quadro 5 – Disciplinas nucleares do curso de Arquivística da UEM

Disciplina nuclear	Carga horária	Período
Análise e Representação da Informação	184	V
Arquivos Permanentes	184	VI
Arquivos, Memória e Património	184	VIII
Avaliação e Seleção de Documentos	184	V

Direito Notarial	184	VI
Estágio Curricular em Arquivística I	248	VII
Estágio Curricular em Arquivística II	248	VIII
Estatística Básica	111	IV
Ética e Informação	184	VIII
Fontes de Informação	111	IV
Fundamentos Arquivísticos I	248	I
Fundamentos Arquivísticos II;	248	II
Fundamentos Teóricos da Informação	184	II
Gestão de Bases de Dados	184	V
Gestão de Documentos I	248	III
Gestão de Documentos II;	248	IV
Gestão de Serviços e Instituições Arquivísticas	184	VII
Gestão Electrónica de Documentos (GED)	184	VI
História das Instituições (Moçambique)	184	VII
Informação, Cultura e Cidadania	184	I
Informática Aplicada	148	I
Linguagens Documentais	184	III
Políticas de Informação	148	V
Preservação e Conservação de Acervos Documentais	111	VI
Seminário de Pesquisa em Arquivística I	184	VI
Seminário de Pesquisa em Arquivística II	248	VII
Serviços de Referência em Unidades de Informação	148	V
Tecnologias de Informação e Comunicação em Unidades de Informação	184	IV
Trabalho de Conclusão de Curso	248	VIII

Fonte: Elaborado pela autora

Tendo identificado as disciplinas nucleares do curso de graduação em Arquivística, achamos oportuno identificar igualmente, em quais disciplinas estão previstos tópicos, de forma explícita, sobre a proteção de dados pessoais em seus planos temáticos, partindo de princípio de que as questões gerais da gestão de documentos e de política arquivística, em suas diferentes dimensões, são de base. Neste contexto, partimos para a análise dos planos de estudo destas disciplinas, que são parte integrante do currículo em apreciação.

Da leitura e análise aos planos temáticos, nenhuma ocorrência de tópico ou tema específico sobre a proteção de dados pessoais foi identificado. Estamos conscientes de que os planos temáticos são moldados e desenvolvidos em planos analíticos pelos docentes, o que pode significar que eles abordem esta questão em sala de aulas (com maior ou menor profundidade). Contudo, achamos que tendo o tema “proteção de dados pessoais” patente no plano temático, obriga o docente a desenvolvê-lo em sala de aulas, não se tornando “facultativo”, conforme a afinidade ou não do docente à temática, domínio etc. Entendemos que nos moldes atuais, essa temática da proteção de dados pessoais pode ser negligenciada, ou o mais provável, não discutida em profundidade, o que nos leva a inferir que os arquivistas que estão sendo formados dentro deste quadro curricular podem apresentar algum

desconhecimento e/ou despreparo para lidar, de forma mais profissional com a proteção de dados pessoais, seja no setor público ou privado, olhando para aspectos técnicos e legais.

5.5.2 Atuação profissional e associativismo

É importante começarmos esta subseção, trazendo um histórico e panorama do profissional de informação em Moçambique. E iniciamos colocando propositalmente esta expressão abrangente porque, conforme se constata pela história da Arquivística em Moçambique (se assim podemos falar), este profissional de fato, aparece muito mais tarde.

Wanda de Amaral, uma das pioneiras da área de documentação em Moçambique, escreveu em 1994, sobre “Sistemas e serviços de informação em Moçambique”. Neste texto a autora aponta que até à Independência de Moçambique não havia um estatuto da profissão de informação e na maior parte dos quadros de pessoal que existiam, praticamente era inexistente a possibilidade de progressão, de tal forma que nem sequer dava para falar de uma carreira profissional de profissional de informação. Do período que ela faz referência, apresenta exemplos de quadros de pessoal da Biblioteca Nacional de Moçambique e do Arquivo Histórico de Moçambique que contavam com “Catalogador”, a Universidade de Lourenço Marques (atual Universidade Eduardo Mondlane) que contava com “1º Bibliotecário; Encarregado de Biblioteca; Catalogador; e Auxiliar de Biblioteca”. A autora nota também que pelo número ínfimo de lugares desses quadros nessas unidades de informação, as pessoas que trabalhavam na área da documentação tinham títulos de categorias profissionais como escriturário-datilógrafo, preparador de laboratório, telefonista, entre outros (Amaral, 1994). Um cenário que nos parece ainda prevalecer em algum grau, mesmo passados 30 anos depois das observações de Amaral.

Amaral relata que o cenário começa a ser alterado quando é aprovado o qualificador de ocupações comuns de técnicos, na segunda metade da década 1980, a nível nacional, embora abrangendo apenas os técnicos de documentação de nível básico (9ª classe) e médio (11ª classe). A partir de 1990 o qualificador profissional começa a incluir a carreira da base ao topo, quer dizer, do auxiliar técnico (7ª classe)

ao técnico especialista (doutorado na área). Neste momento já se pode começar a falar de carreira profissional, porém ela apresentava ainda alguns problemas como a falta de um qualificador profissional comum para arquivos, bibliotecas e centros de documentação.

Em 2004, Tembe e Waete escreveram “A sociedade da informação e o profissional de informação em Moçambique”, um texto através do qual os fazem recomendações dada às constatações feitas naquele contexto. Dentre diferentes perspectivas e recomendações, Tembe e Waete (2004) pontuaram que o profissional de informação, para encarar as mudanças que chamaram de “agressivas” da sociedade, precisam de saber implantar programas de gerenciamento de informação e de informatização de unidades de informação; preparar, resumir e editar informações de natureza científica e técnica; administrar unidades de informação e; organizar e distribuir informação em sua forma original ou como produtos elaborados a partir dela. Os autores constataram que, naquela altura, o setor de informação ainda não tinha sido devidamente “apresentado” em Moçambique, o que significava que o próprio profissional de informação não tinha formação para fazer esse papel de divulgador de sua área de atuação. De fato, nessa altura ainda não haviam sido criados, em Moçambique, cursos superiores de Arquivística, Biblioteconomia ou Ciência da Informação, o que veio acontecer poucos anos depois, como resultado, não só da EGDAE de que falamos mais acima, como resultado também de reflexões como esta realizada por Tembe e Waete, entre outros trabalhos científico de moçambicanos da área das ciências da informação.

Dez anos depois da publicação do texto de Tembe e Waete, foi realizada uma pesquisa, pela Universidade Carlos III de Madrid (UC3M) e pela UEM na qual o “propósito é actualizar o referencial existente e, ao mesmo tempo, traçar um prospecto sobre o perfil do profissional que atua na área de Informação em Moçambique” (González; Mangué, 2014, p. 2). Essa pesquisa teve as bibliotecas, arquivos e centros de documentação da Cidade de Maputo⁷ como seu campo empírico, ainda assim os autores apresentam no final um catálogo de unidades de informação em Moçambique.

Da pesquisa realizada, ficou concluído que as bibliotecas e os arquivos continuavam sendo os espaços de maior atuação dos profissionais de informação,

⁷ Capital, política e económica, de Moçambique.

com uma boa parte deles atuando em bibliotecas universitárias, e as instituições públicas se destacavam como as maiores empregadoras. Com esta pesquisa notou-se que houve uma evolução nos graus académicos dos funcionários, isto é, mais funcionários ostentavam o grau de licenciados, cenário que era muito diferente nas décadas anteriores (González; Mangué, 2014).

Alguns problemas parecem terem persistido, de tal forma que González e Mangué (2014) assinalaram que “a aplicação e gestão de bases de dados, a gestão de unidades de informação, a criação e manutenção de sítios *web* destacam-se entre as necessidades de formação” daqueles que atuam na área e notaram a persistência da “falta de reconhecimento e de um estatuto profissional próprio” (González; Mangué, 2014, p. 2).

Um dado interessante de ver através deste estudo é que, a maioria dos profissionais de informação, cerca de 93,7%, concluiu a sua formação superior em Moçambique e, em segundo lugar, Brasil representa o país onde mais profissionais moçambicanos foram formados em Arquivologia, Biblioteconomia ou Ciência da Informação, com cerca de 3,8% (González; Mangué, 2014, p. 37). Na verdade, o Brasil continua formando número considerável de profissionais de informação moçambicanos incluindo na pós-graduação. Num estudo realizado por Cabsela *et al.* em 2024, onde procuravam compreender a contribuição de Brasil e de Portugal na formação de moçambicanos em Ciência da Informação, as autoras identificaram no Brasil, 11 dissertações e 8 teses. Elas constataram ainda que a maioria dos formados nesses programas, atuam como docentes universitários em Moçambique (Cabsela *et al.*, 2024).

Em Moçambique, a Resolução nº 42/2015 de 31 de dezembro, cria as carreiras de Informação e Documentação e aprova os respectivos qualificadores profissionais. Portanto, nossa compreensão é que o arquivista é enquadrado na carreira de técnico superior de informação e documentação N1. Para ingressar nesta carreira, o indivíduo deve possuir o nível de graduação na área de informação, documentação e ser aprovado em avaliação curricular acompanhada de entrevista profissional e ter participado na capacitação sobre o segredo do Estado .

Esse enquadramento que é dado ao arquivista nas carreiras de informação e documentação, pode ser parte dos entraves para a existência efetiva de uma

“associação de arquivistas moçambicanos”. Procuramos nos inteirar sobre a (in)existência de uma associação neste sentido. A pesquisa documental nos levou a um despacho datado de 28 de maio de 2018, do Ministério da Justiça, Assuntos Constitucionais e Religiosos (MJACR) que reconhece a “Associação dos Arquivistas de Moçambique” como pessoa jurídica. Do estatuto desta associação anexada ao despacho, conseguimos identificar quais são os seus objetivos, sendo alguns deles:

a) contribuir para o desenvolvimento técnico e científico da arquivística; b) congregar profissionais que defendem os interesses da arquivística do ponto de vista científico, ético, social e económico; c) cooperar com entidades públicas e privadas, nacionais e estrangeiras, na solução de problemas relacionados à gestão e preservação de arquivos; d) organizar congressos, conferências, palestras, simpósios, mesas redondas, seminários, reuniões, encontros e outros eventos que contribuam para o desenvolvimento e o aperfeiçoamento no campo da Arquivologia, além de colaborar, quando solicitada e na medida de suas possibilidades, nos eventos promovidos por entidades afins; h) promover cursos na área dos Arquivos, contribuindo para capacitação, actualização e aprimoramento técnico dos associados e dos demais interessados; k) mobilizar a sociedade para reivindicar políticas públicas em defesa da preservação do património arquivístico nacional; l) articular e firmar parceria com instituições de ensino técnico e superior para garantir o ensino e a profissionalização da arquivologia em todos os níveis a nível nacional (Artigo 3º do Estatuto da Associação dos Arquivistas de Moçambique).

Conseguimos notar, através destes e outros objetivos da associação, que caso ela tivesse a sua atuação em curso e/ou venha a ter, alguns aspectos como a reciclagem dos arquivistas, incluindo o debate de assuntos prementes da área, poderão ser observados. Inferimos, todavia, que, esta associação seria/será, aparentemente fraca na proposição de uma política arquivística nacional, visto o objetivo da alínea k) acima.

Ora, tudo indica que o estatuto da associação não foi publicado no Boletim da República (BR), que é a publicação oficial da República de Moçambique, onde a publicação obrigatória dos atos sujeitos a registo é oficiosamente promovida pelos serviços do Registo de Entidades Legais, como é o caso do estatuto desta associação. Cogitamos que não teve lugar o procedimento necessário para a sua publicação pois, tivemos acesso a outro despacho do MJACR, de 13 de fevereiro de 2020, em que é concedida a alteração parcial dos estatutos e a denominação da “Associação dos Arquivistas de Moçambique” passando para “Associação Moçambicana de Arquivistas, Bibliotecários e Documentalistas- ARBIDOC”.

Entendemos que esta alteração é resultado da reunião realizada em fevereiro de 2019, em que membros da comissão instaladora da Associação Moçambicana de

Arquivistas e Bibliotecários (AMOABI, da qual não temos mais informações) convidaram os fundadores da Associação dos Arquivistas de Moçambique e outras entidades para discutirem, entre outros assuntos, a criação da Associação Moçambicana de Arquivistas e Bibliotecários e analisarem o apoio da Associação Africana das Bibliotecas e Instituições de Informação, compreendendo que este último justifica a necessidade de agregação de bibliotecários, pois esta instituição presta(ria) apoios se for nestes termos.

À semelhança da Associação dos Arquivistas de Moçambique, não vimos o estatuto da ARBIDOC publicado no BR, o que nos leva a pensar que esta associação ainda não começou a operar em pleno. Este cenário nos leva a dizer que ainda não existe efetivamente uma associação moçambicana de arquivistas, com este nome ou outros e que a frente do associativismo na área arquivística representa uma fraqueza nesta arena. Imaginamos que essa associação, em condições normais, teria um papel atuante na questão da proteção de dados pessoais e seu alinhamento na gestão de documentos, ou mais amplamente, essa associação que imaginamos poderia ser uma voz a ser ouvida, sem exceção, na formulação e formalização de uma política arquivística nacional.

Posto isto, nas seções adiante, estaremos discutindo com maior detalhe o quadro legal da proteção de dados pessoais, no Brasil, no espaço internacional com incidência para o ocidente, no espaço internacional com incidência para a África (exceto Moçambique) e finalmente um olhar particular para a legislação de proteção de dados pessoais em Moçambique.

6 PANORAMA INTERNACIONAL E BRASILEIRO DA PROTEÇÃO DE DADOS PESSOAIS

Esta seção é dedicada ao mapeando legal atinente à proteção de dados pessoais ao nível internacional (exceto Moçambique pois lhe dedicamos a seção 7) e ao nível nacional brasileiro. Assim, nas subseções seguintes começamos com um olhar à legislação internacional, em seguida, a brasileira e finalizamos com um olhar geral à proteção de dados pessoais em África (exceto Moçambique).

6.1 Legislação internacional

Nesta subseção é nosso objetivo fazer o levantamento dos principais instrumentos legais internacionais sobre proteção de dados pessoais, exceto de África para a qual reservamos uma subseção mais abaixo. Deste levantamento, o maior enfoque é dado à instrumentos das Nações Unidas e do Parlamento Europeu, partindo da Declaração Universal dos Direitos Humanos (DUDH) de 1948 à Convenção 108+ de 2018, passando pelo Regulamento Geral de Proteção de Dados (RGPD) de 2016, evidentemente.

A DUDH estabelece em seu artigo 12º que “Art. 12º, ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.” (DUDH, 1948). Portanto, a questão da proteção de dados pessoais é parte integrante de um dos mais importantes instrumentos legais do mundo desde meados do séc. XX.

Em 1950 foi concebida na Europa, a Convenção para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, conhecida também como Convenção Europeia dos Direitos Humanos. Neste instrumento, o Artigo 8º estabelece nos seus n.º 1 e 2 que

1. Toda pessoa tem direito ao respeito de sua vida privada e familiar, de seu domicílio e de sua correspondência;
2. Não haverá interferência de uma autoridade pública no exercício desse direito, exceto se estiver de acordo com a lei e for necessário em uma sociedade democrática, no interesse da segurança nacional, da segurança pública ou do bem-estar econômico do país, para a prevenção de desordem

ou crime, para a proteção da saúde ou da moral, ou para a proteção dos direitos e liberdades de terceiros (Conselho da Europa, 1950, p. 5).

Dezesseis anos depois da adoção da Convenção Europeia dos Direitos Humanos, o Pacto Internacional dos Direitos Civis e Políticos foi adotado em 1966 pelas Nações Unidas. O n.º 1 do seu artigo determina que “ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação.” (Nações Unidas, 1966).

Em 2001, a Europa volta a ser palco de concepção de uma importante convenção, a Convenção sobre a cibercriminalidade, também conhecida como Convenção de Budapeste. Esta convenção abarca a criminalização do acesso ilegal, interferência em dados, fraudes envolvendo sistemas informáticos, disseminação de material de abuso infantil, entre outros.

As Nações Unidas adotaram mais recentemente, em 2015, a Agenda 2030 para o Desenvolvimento Sustentável, mais conhecida como Objetivos de Desenvolvimento Sustentável (ODS). Esta agenda compreende 17 objetivos, dentre os quais o 16º objetivo, sobre “Paz, Justiça e Instituições Eficazes”, nos chama atenção. O objetivo é de “Promover sociedades pacíficas e inclusivas para o desenvolvimento sustentável, proporcionar o acesso à justiça para todos e construir instituições eficazes, responsáveis e inclusivas a todos os níveis” (Nações Unidas, 2015). Este objetivo apresenta uma série de objetivos específicos, dos quais destacamos:

[...] 16.3 Promover o Estado de Direito, em nível nacional e internacional, e garantir a igualdade de acesso à justiça para todos;

[...]

16.6 Desenvolver instituições eficazes, responsáveis e transparentes em todos os níveis;

[...]

16.8 Ampliar e fortalecer a participação dos países em desenvolvimento nas instituições de governança global;

[...]

16.10 Assegurar o acesso público à informação e proteger as liberdades fundamentais, em conformidade com a legislação nacional e os acordos internacionais; [...] (Nações Unidas, 2015).

Estes objetivos têm, em seu espírito, uma forte carga de proteção de dados pessoais, pois para que a proteção seja efetiva, ela demanda instituições transparentes e responsáveis, acompanhadas do exercício do direito à informação (se informar e ser informado sobre o tratamento dos seus dados pessoais, por exemplo),

bem como e consequentemente a salvaguarda das liberdades fundamentais dos cidadãos das diferentes nações.

Em 2016 foi aprovada na Europa, aquela que é atualmente uma das maiores referências internacionais em matéria de proteção de dados pessoais e que inspirou (também) a elaboração da normativa brasileira de proteção de dados pessoais, o Regulamento Geral de Proteção de Dados (RGPD). Passamos a apreciar algumas das cláusulas do RGPD, regulamento este que foi aprovado pelo Parlamento Europeu e do Conselho, aos 27 de abril de 2016, revogando ao mesmo tempo a Diretiva 95/46/CE.

O seu objeto e objetivos estão definidos no Artigo 1º, indicado no n.º 1 do mesmo que o “regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados” (Parlamento Europeu, 2016). No n.º 2 indica que “o regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais” (Parlamento Europeu, 2016). Ademais, o regulamento “aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados” (Artigo 2º).

Através do Artigo 4º, várias definições são apresentadas neste instrumento. Mobilizamos algumas destas definições:

Dados pessoais- informação relativa a uma pessoa singular identificada ou identificável (“titular dos dados”); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular (Parlamento Europeu, 2016).

Esta definição de dados pessoais que se aplica no âmbito do RGPD, é a que ilumina diversas normativas mundo afora, incluindo no Brasil. Ela carrega em si, a noção de dados pessoais de forma mais generalizada, mas também aponta para dados pessoais sensíveis através dos chamados “identificadores”, que são na essência os dados em si.

Tratamento - uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição (Parlamento Europeu, 2016).

O tratamento, como podemos ver, remete à gestão desses dados pessoais. Quer dizer, quando falamos da gestão de documentos, entendemos que o tratamento dos dados pessoais é parte integrante, desde a produção documental até a eliminação ou conservação a longo prazo e, por essa razão, o tratamento de dados pessoais tem imbricada a noção de ciclo vital dos dados *voire* dos documentos. Para um melhor entendimento, o quadro que segue, ilustra esta relação.

Quadro 6 – Gestão de documentos e Tratamento de dados pessoais

Gestão de documentos		Tratamento de Dados Pessoais
conjunto de procedimentos e operações técnicas ligadas à produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, com vista à sua eliminação ou recolhimento.		
Fase corrente	Fase Intermediária	
Elaboração, Protocolo (recebimento e classificação, registro e movimentação); expedição; arquivamento; empréstimo e consulta; e, destinação (Avaliação, seleção, eliminação, transferência e eventual recolhimento direto, avaliado o valor dos documentos)	Avaliação, seleção, eliminação e recolhimento.	Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

Fonte: Elaborado pela autora.

Para além da definição de dados pessoais e de tratamento, o Artigo 4º apresenta outras importantes definições na esteira da proteção de dados pessoais. Essas definições são apresentadas no quadro 7.

Quadro 7 – Definições no âmbito da proteção de dados pessoais no RGPD

Termo	Definição
Consentimento do titular dos dados	Manifestação de vontade, livre, específica, informada e inequívoca, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento

Dados biométricos	Dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos
Dados genéticos	Dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa
Pseudonimização	Tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável
Responsável pelo tratamento	Pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais
Violação de dados pessoais	Violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento

Fonte: Adaptado de RGPD (2016).

Destas definições, podemos perceber que, em relação ao consentimento, ele é espelho de uma instituição, ou melhor, de um tratamento transparente de dados pessoais, o que significa igualmente ter o acesso à informação sendo exercido, na medida em que o titular dos dados é informado da intenção de tratamento de seus dados e por via disto consente (ou não).

O consentimento pode ser dado para o tratamento de dados pessoais que podem ser de diferentes categorias de dados, incluindo dados pessoais sensíveis, como os dados genéticos ou dados biométricos.

No tratamento dos dados pessoais, previamente consentido, pode ser usada a pseudonimização como medida e/ou técnica, de modo que o nome de uma pessoa seja substituído por pseudônimos afim de evitar a sua identificação.

Para o tratamento de dados pessoais deve haver sempre, pelo menos um, responsável por essa operação, seja a nível institucional ou nacional ou ainda internacional (caso da União Europeia, por exemplo).

No que toca a violação de dados pessoais, parece-nos que esta pode facilmente ocorrer se a gestão de documentos, sejam eles eletrônicos ou tradicionais, não estiver a ser implementada, já que a gestão de documentos oferece operações

técnicas que imprimem, por exemplo, maior segurança face à possibilidade de acesso não autorizado acidental ou ilícito.

Seja para tratamento de dados pessoais considerados sensíveis ou não, o RGPD orienta-se por um leque de princípios nesse tratamento, apresentados no n.º 1 do Artigo 5º. No quadro a seguir, são apontados esses princípios e respectiva descrição.

Quadro 8 – Princípios de tratamento de dados pessoais

Princípio	Descrição
Licitude, lealdade e transparência	[os dados pessoais são] objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados
Limitação das finalidades	[os dados pessoais são] recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais [...]
Minimização dos dados	[os dados pessoais são] adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados
Exatidão	[os dados pessoais são] exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora
Limitação da conservação	[os dados pessoais são] conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos [...]
Integridade e confidencialidade	[os dados pessoais são] tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas

Fonte: Adaptado de RGPD (2016).

Estes seis princípios, apresentados no quadro 8, que são basilares no tratamento de dados pessoais, comportam no seu âmago aspectos arquivísticos, (como é mostrado na página 135, quadro 9), desde logo na recolha ou registro, ou seja, na produção documental como temos estado a fazer referência, onde são e/ou devem ser coletados/registrados os dados pessoais mínimos pertinentes para a finalidade pretendida. Esses dados pessoais registrados devem ser mantidos com as características iniciais até sua eliminação, ou seja, a integridade e acurácia devem

acompanhá-los ao longo de todo o tratamento que recair sobre eles. Ademais, porque algum nível de sigilo lhes é aplicado, medidas de confidencialidade lhes são aplicadas, devendo o titular dos dados poder aceder a estes sempre que se justificar.

Quadro 9 – Princípios de tratamento de dados pessoais face aos princípios arquivísticos e ao papel do arquivista na proteção de dados pessoais

Princípio de tratamento de dados	Princípios arquivísticos	Funções arquivísticas	Papel do arquivista
Licitude, lealdade e transparência	Organicidade Proveniência Territorialidade Teoria das Três Idades	Produção, classificação, aquisição	Papel jurídico, ético e de comunicação
Limitação das finalidades	Organicidade Proveniência Territorialidade Teoria das Três Idades	Produção; descrição; aquisição; difusão	Papel jurídico, ético e de comunicação
Minimização dos dados	Organicidade Proveniência Territorialidade Teoria das Três Idades	Produção, aquisição	Papel jurídico, ético e de comunicação
Exatidão	Organicidade Proveniência Teoria das Três Idades	Conservação, avaliação	Papel jurídico, ético e de comunicação; papel técnico e tecnológico
Limitação da conservação	Organicidade Proveniência Teoria das Três Idades	Conservação; avaliação; difusão; descrição; produção	Papel jurídico, ético e de comunicação; papel técnico e tecnológico
Integridade e confidencialidade	Organicidade Proveniência Territorialidade Teoria das Três Idades	Conservação; avaliação	Papel técnico e tecnológico

Fonte: Elaborado pela autora.

Depois de termos discutido na seção 4, A PROTEÇÃO DE DADOS PESSOAIS DESDE UMA PERSPECTIVA ARQUIVÍSTICA, sobre os princípios arquivísticos, as funções arquivísticas, assim como o papel do arquivista na proteção de dados pessoais, o quadro acima busca conjugar estes aspectos com os princípios de tratamento de dados pessoais. Nele podem ser vistos o alinhamento mais específico de cada princípio de tratamento de dados pessoais com a aplicabilidade dos princípios arquivísticos na sua globalidade, do mesmo modo para as funções arquivísticas e o papel do arquivista.

Um outro aspecto colocado no RGPD que merece atenção, está plasmado no capítulo V sobre “Transferências de dados pessoais para países terceiros ou

organizações internacionais”, em que em seu Artigo 44º é apresentado o princípio geral das transferências, segundo o qual

Qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento (Parlamento Europeu, 2016).

Foi considerando o RGPD que foi atualizada, em 2018, a Convenção 108 para 108+, a Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal, adotada em Elsinore pelo Conselho da Europa. Ela fundamenta-se na necessidade de

garantir a dignidade humana e a proteção dos direitos humanos e das liberdades fundamentais de todas as pessoas e, dada a diversificação, intensificação e globalização do tratamento de dados e dos fluxos de dados pessoais, a autonomia pessoal com base no direito de uma pessoa ao controlo dos seus dados pessoais e do tratamento desses dados (Conselho da Europa, 2018, p. 2).

Nos seus fundamentos, o Conselho da Europa faz recordar que “o direito à proteção dos dados pessoais deve ser considerado tendo em conta o seu papel na sociedade e que tem de ser conciliado com outros direitos humanos e liberdades fundamentais, incluindo a liberdade de expressão” (Conselho da Europa, 2018, p. 2).

Os dados pessoais são definidos no Artigo 2º desta convenção como qualquer informação relativa a uma pessoa singular identificada ou identificável, sendo que essa pessoa singular é o titular dos dados.

No Artigo 6º são apresentadas as categorias especiais de dados, sendo eles: dados genéticos; dados pessoais relativos a infrações, processos penais e condenações, bem como medidas de segurança conexas; dados biométricos que identifiquem uma pessoa de forma inequívoca; e, dados que revelem a origem racial ou étnica, as opiniões políticas, a filiação sindical, as crenças religiosas ou outras, a saúde ou a vida sexual. Ora, o tratamento destes dados “só será permitido se estiverem previstas na lei garantias apropriadas que complementem as previstas na presente Convenção” (Conselho da Europa, 2018).

Conforme o Artigo 9º que dispõe sobre os direitos do titular dos dados, todas as pessoas terão direito de:

- a) não ser objeto de uma decisão que as afete significativamente, com base exclusivamente num tratamento automatizado de dados, sem que os seus pontos de vista sejam tomados em consideração;
- b) obter, mediante pedido, a intervalos razoáveis e sem demora ou despesas excessivas, a confirmação do tratamento dos dados pessoais que lhe digam respeito, a comunicação, sob forma inteligível, dos dados tratados, toda a informação disponível sobre a sua origem e o período de conservação, bem como qualquer outra informação que o responsável pelo tratamento seja obrigado a fornecer a fim de assegurar a transparência do tratamento [...];
- c) obter, mediante pedido, informação sobre a fundamentação subjacente ao tratamento de dados, nos casos em que os resultados de tal tratamento lhe sejam aplicados;
- d) se opor, em qualquer momento, por motivos relacionados com a sua situação, ao tratamento dos dados pessoais que lhe digam respeito, salvo se o responsável pelo tratamento demonstrar motivos legítimos para o tratamento que prevaleçam sobre os seus interesses ou direitos e liberdades fundamentais;
- e) obter, mediante pedido, gratuitamente e sem demora excessiva, a retificação ou a supressão, consoante o caso, desses dados, se estes estiverem a ser ou tiverem sido tratados em violação das disposições da presente Convenção;
- f) dispor de uma via de recurso [...], caso os direitos que lhe são conferidos pela presente Convenção tenham sido violados;
- g) beneficiar, independentemente da sua nacionalidade ou da sua residência, da assistência de uma autoridade de controlo, [...], no exercício dos direitos que lhe são conferidos pela presente Convenção (Conselho da Europa, 2018).

Nos meados de 2024, em São Tomé, foi aprovada a Carta de Direitos e Princípios em Ambientes Digitais da Comunidade dos Países de Língua Portuguesa (CPLP), onde os países reconhecem que os direitos existentes no ambiente *offline* também devem ser protegidos no ambiente digital. Nesta senda, dentre os “Direitos e Liberdades em Ambiente Digital”, “a garantia, o respeito, a promoção e proteção dos direitos humanos serão garantidos também nos ambientes digitais, bem como os demais direitos presentes nas nossas constituições e marcos jurídicos” (CPLP, 2024).

No quesito Privacidade e Cibersegurança, a carta determina que “todas as pessoas têm direito à privacidade e proteção dos seus dados pessoais em ambiente digital; e, todas as pessoas têm direito a usufruir de um ambiente digital aberto, seguro, estável, acessível e pacífico” (CPLP, 2024). Sobre a “Proteção da criança e do adolescente” a carta estabelece que

Os Estados-Membros da CPLP desenvolvem os melhores esforços para promover políticas ativas que tenham por objeto assegurar o respeito à integridade, intimidade e privacidade de crianças e adolescentes nos ambientes digitais, bem como impulsionam estratégias e programas de formação orientados ao desenvolvimento de competências para o acesso

seguro aos ambientes digitais por parte de crianças e adolescentes (CPLP, 2024).

Para além destes instrumentos mais amplos em termos de aplicação territorial, há várias normativas de nível nacional que vêm sendo aprovadas desde a segunda metade do séc. XX à atualidade. Estas normativas, aos olhos de diferentes autores, podem ser subdivididas em gerações, conforme as características dominantes que apresenta .

A seguir vamos revisitar o desenvolvimento dessas normativas de proteção de dados pessoais. Um levantamento feito por Doneda (2011), aponta mudanças de enfoque nesse processo de desenvolvimento. Ele visualiza quatro diferentes gerações de leis que partem desde um enfoque mais técnico e restrito até a abertura a técnicas mais amplas e condizentes com a profundidade da tecnologia adotada para o tratamento de dados, em busca de uma tutela mais eficaz e vinculanda a matéria aos direitos fundamentais. Contudo, Mendes (2019) nos chama atenção para uma nova geração de normativas, a quinta. Segundo o autor, a quinta geração nasce devido aos “novos desenvolvimentos nessa seara, tais como a revisão pela OCDE⁸ das Diretrizes relativas à proteção de dados pessoais e ao fluxo de dados transfronteiriços de 2013, a edição do [RGPD] [...], assim como a recém-aprovada Lei de Proteção de Dados da Califórnia” (Mendes, 2019, p. 42).

Sobre a primeira geração das leis, Doneda (2011) aponta que ela é composta por normas que refletiam o estado da tecnologia e a visão do jurista na época, pretendendo regular um cenário no qual centros elaboradores de dados, de grande porte, concentrariam a coleta e gestão dos dados pessoais. Elas giravam em torno da concessão de autorizações para a criação desses bancos de dados e do seu controle a posteriori por órgãos públicos. Essas leis enfatizavam o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas . A estrutura e a gramática de tais leis era algo tecnocrático e condicionado pela informática. Nelas, tratava-se dos “bancos de dados”, e não propriamente da “privacidade”, desde seus princípios genéricos até os regimes de autorização e de modalidades de tratamento de dados. São exemplos de normas da primeira geração as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o

⁸ Organização para a Cooperação e o Desenvolvimento Econômico

Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Todas essas normas podem ser consideradas de primeira geração pela sua estrutura e linguagem (Mendes, 2019, p. 37).

A segunda geração, diz Doneda (2011), surgiu no final da década de 1970, tendo como característica básica e que diferencia tais leis das da primeira geração, a sua estrutura não estar mais fixada em torno do fenômeno computacional em si, mas se baseia na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão. Estas leis apresentavam igualmente seus problemas, acrescenta Doneda, o que motivou uma subsequente mudança. Percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social. O que era exceção veio a se tornar regra. Tanto o Estado quanto o privado utilizavam intensamente o fluxo de informações pessoais para seu funcionamento. Como consequência, “a privacidade informacional é inserida nos textos das Constituições da Áustria, da Espanha e de Portugal e são exemplos de normas da segunda geração, as leis da Áustria, da França, da Dinamarca e da Noruega” (Mendes, 2019, p. 39).

Doneda (2011) aponta que a terceira geração de leis, surgida na década de 1980, procurou sofisticar a tutela dos dados pessoais, que continuou centrada no cidadão, contudo, passou a abranger mais do que a liberdade de fornecer ou não os próprios dados pessoais, preocupando-se também em garantir a efetividade desta liberdade. Aqui a proteção de dados é vista como um processo que envolve a própria participação do indivíduo na sociedade e considera o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é colocada em causa por eventuais condicionantes, proporcionando autodeterminação informativa. Doneda (2022) explica que o tratamento de dados pessoais era tido como um processo que transpassava a simples permissão ou não da pessoa à utilização de seus dados pessoais, e procurava incluí-la em fases sucessivas desse processo e na utilização de sua própria informação por terceiros, como também abarcava algumas garantias, como o dever de informação). São exemplos dessa geração, “a emenda à lei federal de proteção de dados pessoais alemã de 1990, a emenda da lei da Áustria de 1986,

a alteração da lei da Noruega e a previsão constitucional da proteção de dados pessoais da Holanda” (Mendes, 2019, p. 40).

A quarta geração de leis de proteção de dados surgiu e caracterizou-se por procurar suprir as desvantagens do enfoque individual existente. Nesta geração, as leis procuram focar o problema integral da informação, pois elas presumem que não se pode basear a tutela dos dados pessoais simplesmente na escolha individual. Entre as técnicas utilizadas, essas leis procuraram fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados (Doneda, 2011). Outra característica da quarta geração consiste, segundo Mendes (2019) no fato de que, em muitos países, normas gerais sobre a proteção de dados são complementadas com normas setoriais, a fim de ampliar a proteção de dados nos diferentes setores de modo que a legislação possa contemplar as diversas especificidades setoriais existentes. Assim, “na maioria dos países europeus, percebe-se a existência de uma regulamentação geral sobre proteção de dados, mas com códigos de conduta setoriais suplementares” (Mendes, 2019, p. 42).

De acordo com Mendes , atualmente, já se fala em uma quinta geração de normativas de proteção de dados pessoais. A característica dessa geração

é a aposta em um sistema de corregulação, amparado no princípio da *accountability*, isto é, passa-se a entender que a efetividade da proteção de dados não reside mais apenas em ampliar o controle do indivíduo, mas também em atribuir responsabilidade a toda a cadeia de agentes de tratamento de dados pelos riscos do processamento de informações. Isso porque se compreende que tais agentes têm mais condições de implementar medidas técnicas e organizativas capazes de proteger os dados pessoais dos titulares. Nesse contexto, as mais recentes legislações, das quais se destaca o Regulamento Geral de Proteção de Dados europeu, passam a prever novos mecanismos que não estavam presentes nos marcos anteriores, tais como relatórios de impacto, códigos de boas condutas, certificações, programas de governança, bem como normas que incentivam a implementação do conceito de *privacy by design* (Mendes, 2019, p. 42).

De acordo com Banisar (2024), 160 países e jurisdições e territórios autônomos no mundo já contam com normativas abrangentes de proteção de dados e/ou de privacidade. Em particular, pelo menos 137 Estados-membros das Nações Unidas adotaram normativas de proteção de dados. Alguns destes países constam do quadro 10 na página a seguir.

Quadro 10 - Principal legislação internacional de proteção de dados pessoais

Ano	Instrumento normativo	País ou organização
2024	Carta da Comunidade dos Países de Língua Portuguesa de Direitos e Princípios em Ambientes Digitais	CPLP
2023	Lei de Proteção de Dados Pessoais Digitais	Índia
2019	Lei da Proteção de Dados Pessoais	Portugal
2018	Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal (Convenção 108+)	Parlamento Europeu Conselho da Europa
2016	Regulamento Geral de Proteção de Dados (RGPD)	
2015	Objetivos de desenvolvimento Sustentável / Agenda 2030	Nações Unidas
2001	Convenção de Budapeste	Conselho da Europa
1966	Pacto Internacional dos Direitos Civis e Políticos	Nações Unidas
1950	Convenção Europeia dos Direitos do Homem	Conselho da Europa
1948	Declaração Universal dos Direitos Humanos (DUDH)	Nações Unidas
1978	<i>Loi Informatique et Libertés</i>	França
1977	<i>Bundesdatenschutzgesetz</i> (Lei Federal sobre proteção de dados pessoais)	Alemanha

Fonte: Elaborado pela autora

No quadro acima, são apresentadas algumas normativas de proteção de dados pessoais no plano internacional, exceto de Moçambique, pois mais adiante é reservada uma seção para o QUADRO LEGAL MOÇAMBICANO DA PROTEÇÃO DE DADOS PESSOAIS.

6.2 Legislação brasileira

Esta subseção resulta do levantamento da principal legislação federal atinente à proteção de dados pessoais. Este levantamento parte da Constituição da República Federativa do Brasil (1988) e desemboca na Lei Geral de Proteção de Dados (2018).

A Constituição da República Federativa do Brasil de 1988, estabelece no Capítulo I “dos direitos e deveres individuais e coletivos”, inciso XXXIII que

Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (Brasil, 1988).

A constituição prevê a concepção de *habeas data*, no inciso LXXII, alíneas a) e b), “para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de

caráter público” (Brasil, 1988) e “para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo” (Brasil, 1988), respetivamente.

O inciso LXXIX determinando que “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” foi introduzido na Constituição pela Emenda Constitucional nº 115, de 2022. Portanto, no Brasil a proteção de dados pessoais encontra-se fundamentada na Constituição, apresentando seu balanço com acesso à informação como também se aplicando não apenas aos meios digitais.

Olhando para normativas ordinárias, podemos destacar a Lei nº 8.078, de 11 de setembro de 1990, que dispõe sobre a proteção do consumidor e dá outras providências. No *caput* do artigo 43º lê-se que “Art. 43ºo consumidor, [...], terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes” (Brasil, 1990). O parágrafo 1º deste artigo aponta que “[...] §1º os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos” (Brasil, 1990). Podemos perceber que estão nas entrelinhas os princípios de tratamento de dados pessoais. Estes são complementados pelo direito à informação adjacente ao parágrafo 2º deste mesmo artigo onde “a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele” (Brasil, 1990).

O inciso II do Artigo 54-D, prevê que antes da contratação num processo de oferta de crédito, o fornecedor ou o intermediário deverá, entre outras condutas, “[...] II -avaliar, de forma responsável, as condições de crédito do consumidor, mediante análise das informações disponíveis em bancos de dados de proteção ao crédito, observado o disposto neste Código e na legislação sobre proteção de dados; [...]” (Brasil, 1990).

Na segunda metade da década de 1990, foi aprovada a Lei nº 9.507, de 12 de novembro de 1997 (Brasil, 1997), que regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Neste dispositivo “Art. 1º, Parágrafo único. Considera-se de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam

de uso privativo do órgão ou entidade produtora ou depositária das informações.” (Brasil, 1997).

O Código Civil foi instituído pela Lei nº 10.406, de 10 de janeiro de 2002 (Brasil, 2002). Através do artigo 21º o código determina que “Art. 21º, a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (Brasil, 2002).

A chamada Lei do Cadastro Positivo, Lei nº 12.414, de 9 de junho de 2011 (Brasil, 2011a), disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Dentre os direitos do cadastrado arrolados no artigo 5º, destacam-se os direitos de “Art. 5º [...] ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais; [...] e ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados” (Brasil, 2011a).

No âmbito desta lei não podem ser utilizadas informações “Art. 7º, inciso I, que não estiverem vinculadas à análise de risco de crédito e aquelas relacionadas à origem social e étnica, à saúde, à informação genética, ao sexo e às convicções políticas, religiosas e filosóficas” (Brasil, 2011a). O parágrafo 1º do inciso III, determina que “inciso III, §1º, o gestor de banco de dados deve disponibilizar em seu sítio eletrônico, de forma clara, acessível e de fácil compreensão, a sua política de coleta e utilização de dados pessoais para fins de elaboração de análise de risco de crédito” (Brasil, 2011a).

Em 2011 também foi aprovada a Lei de Acesso à Informação, ou seja, a Lei nº 12.527, de 18 de novembro de 2011 (Brasil, 2011b). A lei apresenta algumas definições e considera, ao abrigo do Artigo 4º:

- I - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- II - Documento: unidade de registro de informações, qualquer que seja o suporte ou formato;
- III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;
- IV - Informação pessoal: aquela relacionada à pessoa natural identificada ou identificável (Brasil, 2011b).

No capítulo II do acesso a informações e da sua divulgação, o artigo 6º arrola os deveres dos órgãos e entidades do poder público, cabendo-lhes entre outros, assegurar a “Art. 6º [...] proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade” (Brasil, 2011b) e a “proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso” (Brasil, 2011b).

Na seção III da Proteção e do Controle de Informações Sigilosas, no *caput* do artigo 25º lê-se que “Art. 25º, é dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção” (Brasil, 2011b). Por sua vez a seção V das Informações Pessoais, determina no artigo 31º que “Art. 31º, o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais” (Brasil, 2011b).

O marco civil da internet é, de fato, incontornável num levantamento de normativas de proteção de dados pessoais no Brasil. Aliás, a normativa teve redações dadas pela Lei nº 13.709, de 2018 (Brasil, 2018). Ora, este marco civil da internet é dado em 2014 com a aprovação da Lei nº 12.965, de 23 de abril de 2014 (Brasil, 2014), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

O capítulo I em que são apresentadas as disposições preliminares, apresenta no artigo 3º, os princípios que orientam a disciplina do uso da internet no Brasil, sendo eles: “Art. 3º, garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; proteção da privacidade; e, proteção dos dados pessoais, na forma da lei” (Brasil, 2014).

No que toca a subseção III da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações, o inciso II do artigo 16º, estabelece que na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda “Art. 16º [...] de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais” (Brasil, 2014).

Como se percebeu quando indicamos na introdução desta subseção, o Brasil conta desde 2018 com a Lei Geral de Proteção de Dados (LGPD), aprovada pela Lei nº 13.709, de 14 de agosto de 2018 (Brasil, 2018), que, conforme o artigo 1º,

Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

O artigo 2º arrola os fundamentos da disciplina da proteção de dados pessoais. São eles: o respeito à privacidade; à autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018).

A LGPD define alguns termos no artigo 5º. Desta feita, considera-se:

Art. 5º, I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável”

II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (Brasil, 2018).

Para além da definição destes termos básicos, são apresentadas mais definições orientadas àqueles que, no nosso entender, são os principais atores no processo de tratamento de dados pessoais.

Art. 5º [...], V - Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento

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);

IX - Agentes de tratamento: o controlador e o operador;

[...]

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (Brasil, 2018).

Para além das definições de termos básicos como dados pessoais e da definição dos principais atores no tratamento de dados, a LGPD apresenta a definição de algumas operações que podem ocorrer com o tratamento, apresentando aliás, a própria definição de tratamento no âmbito desta lei.

Art. 5º [...], X - Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
 XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
 XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
 XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
 XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado (Brasil, 2018).

Nesse tratamento de dados devem ser observados não só a boa-fé como também um conjunto de dez princípios estabelecidos no artigo 6º. São eles os princípios de: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e, responsabilização e prestação de contas (Brasil, 2018).

No quadro que segue, são apresentadas as principais normativas brasileiras atinentes à proteção de dados pessoais, aprovadas desde a Constituição da República, passando pelo último dispositivo que estivemos a apreciar, a LGPD, e considerando a emenda constitucional nº 115.

Quadro 11 - Principal legislação brasileira de proteção de dados pessoais

Ano	Instrumento normativo	Aplicação
2022	Emenda Constitucional nº 115	União Estados Distrito Federal Municípios
2018	Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).	
2014	Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco civil da internet)	
2011	Lei nº 12.527, de 18 de novembro de 2011. 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 (Lei de acesso à informação)	
	Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. (a Lei do Cadastro Positivo)	
2002	Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil.	
1997	Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data.	
1990	Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências.	
1988	Constituição da República Federativa do Brasil	

Fonte: Elaborado pela autora

Através do quadro acima, fica evidente que a regulação da temática de proteção de dados pessoais ganha maior atenção do legislador brasileiro a partir dos finais do séc. XX. Isto pode ser entendido também através das lentes da evolução das tecnologias de informação e comunicação, que despertaram maior atenção para a vulnerabilidade dos dados pessoais, sobretudo no entorno eletrônico e digital.

6.3 A África e a proteção de dados pessoais

Em vários momentos ao longo dos últimos 50 anos de promulgação de normativas de privacidade de dados, diferentes regiões do mundo se tornaram bastante ativas na difusão dessas normativas, incluindo, a África que vem apresentando uma expansão cada vez mais rápida de normativas de proteção de dados, com pelo menos 13 países adotando-as desde 2013 (Greenleaf; Cottier, 2022). Na verdade

o conceito de privacidade só se desenvolveu na África no final do período colonial, especialmente porque os poderes coloniais que saíam frequentemente deixavam constituições que previam proteções à privacidade entre outros valores, mesmo que isso fosse inconsistente com os valores mais coletivistas dessas sociedades naquela época (Greenleaf; Cottier, 2022, p. 3).

A primeira normativa africana que podemos mencionar é a Carta Africana dos Direitos Humanos e dos Povos, aprovada pela Conferência Ministerial da Organização da Unidade Africana (OUA) em Banjul, Gâmbia, em janeiro de 1981, e adotada pela XVIII Assembleia dos Chefes de Estado e Governo da Organização da Unidade

Africana (OUA) em Nairobi, Quênia, em 27 de julho de 1981. No seu Artigo 4º determina que “a pessoa humana é inviolável. Todo ser humano tem direito ao respeito da sua vida e à integridade física e moral da sua pessoa. Ninguém pode ser arbitrariamente privado desse direito” (OUA, 1981).

Esta carta tem feito parte dos fundamentos de variados instrumentos africanos, sejam regionais ou não. A Comunidade de Desenvolvimento da África Austral (SADC) toma-a para fundamentar a sua Lei Modelo sobre proteção de dados, aprovada em 2013. Nessa lei modelo, são apresentadas várias definições.

Os dados são definidos como “todas as representações de informações, independentemente do formato ou da mídia” (SADC, 2013, p. 5) e “Dados pessoais referem-se a quaisquer dados relacionados a um titular de dados.” (SADC, 2013, p. 6). por sua vez, no âmbito da lei modelo, Dados sensíveis

- a) referem-se a determinados dados pessoais, incluindo dados genéticos, dados relacionados a crianças, dados relacionados a infrações, sentenças criminais ou medidas de segurança, dados biométricos, bem como, se forem processados pelo que revelam ou contêm, dados pessoais que revelam origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, afiliações, associações sindicais, gênero e dados relativos à saúde ou à vida sexual.
- b) refere-se também a quaisquer dados pessoais considerados por um Estado-Membro como apresentando um risco importante para os direitos e interesses do titular dos dados, em especial discriminação ilegal ou arbitrária (SADC, 2013, p. 6).

O Controlador de dados ou, simplesmente, controlador é qualquer pessoa física, jurídica ou órgão público que, sozinho ou em conjunto com outros, determina a finalidade e os meios de processamento de dados pessoais (SADC, 2013). O Processador de dados no âmbito dessa lei modelo é a pessoa física, jurídica ou órgão público que processa dados pessoais para o controlador e em seu nome, bem como sob suas instruções, com exceção das pessoas que, sob a autoridade direta do controlador, estão autorizadas a processar os dados (SADC, 2013). O Encarregado de proteção de dados ou DPO (*Data Protection Officer*) é qualquer indivíduo nomeado pelo controlador de dados e encarregado de garantir, o cumprimento das obrigações previstas na lei modelo, com exceção de transferência de dados pessoais para um Estado que não seja membro da SADC (SADC, 2013)

No ano seguinte à publicação da lei modelo da SADC, a União Africana (UA) aprovou a chamada Convenção de Malabo, ou seja, a Convenção da União Africana

Sobre Cibersegurança e proteção de dados pessoais, que foi adotada pela vigésima terceira sessão ordinária da cimeira da UA, realizada em Malabo, na Guiné Equatorial, as 27 de junho de 2014. A convenção começa apresentando em seu Artigo 1º as definições que guiam a compreensão do seu texto normativo. Estas são algumas das definições:

Dados pessoais: qualquer informação relativa a uma pessoa singular identificada ou identificável, através da qual esta pessoa pode ser identificada, direta ou indiretamente, em particular através de referência a um número de identificação ou a um ou vários factores específicos à sua identidade física, fisiológica, mental, económica, cultural ou social;

Dados sensíveis: todos os dados pessoais relativos às opiniões ou actividades religiosas, filosóficas, políticas, sindicais, bem como relacionadas à vida sexual ou raça, saúde, medidas sociais, processos judiciais, sanções penais ou administrativas;

Consentimento dos sujeitos titular dos dados: qualquer manifestação de vontade expressa, inequívoca, livre, específica e informada através da qual a pessoa interessada ou o seu representante legal, judicial ou convencional aceita que os seus dados pessoais sejam processados manual ou eletronicamente;

Danos: qualquer prejuízo à integridade ou à disponibilidade de dados, de um programa, sistema ou uma informação;

Processamento de Dados Pessoal: qualquer operação ou conjunto de operações efectuadas sobre os dados pessoais, que através de meios automáticos ou não, tais como tais como recolha, registo, organização, armazenamento, adaptação, alteração, recuperação, suporte, cópia, consulta, utilização, divulgação, ou qualquer outra forma de distribuição, ou doutro modo, fazendo disponibilização, alinhamento ou combinação e bloqueio, encriptação, supressão ou destruição de dados pessoais (UA, 2014).

A convenção dedica o capítulo II à proteção de dados pessoais. O Artigo 8, da seção I, apresenta os objetivos da convenção em relação aos dados pessoais. Deste modo:

1. Cada Estado Parte compromete-se a criar um quadro jurídico, tendo como objectivo reforçar os direitos fundamentais e as liberdades públicas, nomeadamente a protecção de dados físicos, e reprimir qualquer infracção relativa à vida privada, sem prejuízo do princípio da liberdade de circulação de dados pessoais.

2. Esse mecanismo assim criado deve garantir que qualquer tratamento de dados, respeite as liberdades e os direitos fundamentais das pessoas singulares, ao mesmo tempo reconhecendo-se as prerrogativas do Estado, os direitos das comunidades locais e os objectivos para os quais as empresas foram criadas (UA, 2014).

O n.º1 do artigo 9º (âmbito de aplicação da convenção), aponta que estão sujeitos à convenção

a) qualquer recolha, processamento, armazenamento ou utilização de dados pessoais por uma pessoa singular, pelo Estado, pelas comunidades locais e pelos organismos públicos ou privados;

- b) qualquer processamento informatizado ou não de dados contidos ou que devem figurar num ficheiro [...];
- c) qualquer processamento de dados feito no território de um Estado-membro da União Africana
- d) qualquer processamento de dados relativos à segurança pública, defesa, investigação e processos penais ou à segurança do estado, sujeitos a excepções definidas por disposições específicas fixadas por outras leis em vigor (UA, 2014).

Na seção II sobre o quadro institucional da proteção de dados de caráter pessoal, no Artigo 11º, a convenção estabelece que cada Estado parte deve criar uma autoridade responsável pela proteção de dados pessoais. “A autoridade nacional de proteção é um órgão administrativo independente e autónomo, com a tarefa de garantir que o processamento de dados pessoais seja feito em conformidade com as disposições da presente convenção” (UA, 2014).

O Artigo 13º versa sobre os princípios de base que regem o processamento de dados pessoais. São eles: o princípio de consentimento e de legitimidade do processamento de dados pessoais; princípio da legalidade e da lealdade do processamento dos dados pessoais; princípio de finalidade, pertinência, conservação e do processamento de dados pessoais; princípio de exatidão dos dados pessoais; princípio de transparência do processamento de dados pessoais; e, princípio de confidencialidade e de segurança no processamento de dados pessoais.

A seção IV versa sobre os direitos do sujeito titular dos dados. Estes direitos compreendem o direito à informação (Artigo 16º); direito de acesso (Artigo 17º); direito de oposição (Artigo 18º); e, direito de retificação e supressão (Artigo 19º). Em paralelo, há obrigações a serem cumpridas pelo responsável pelos dados pessoais. A seção V aborda as obrigações desse ator, sendo elas as obrigações de confidencialidade (Artigo 20º); obrigações de segurança (Artigo 21º); obrigações de conservação (Artigo 22º); e, obrigações de manutenção (Artigo 23º).

No mesmo ano foi aprovada a Declaração Africana sobre Direitos e Liberdades na Internet pela Coalizão da Declaração Africana sobre Direitos e Liberdades na Internet (AfDec). Ela procura promover padrões altos de direitos humanos e princípios de abertura na formulação e implementação de políticas da Internet no continente. A Declaração foi motivada pela necessidade de “desenvolver e chegar a acordo sobre um conjunto de princípios que vão informar, e esperamos, também inspirar, processos

legislativos e de política sobre direitos, liberdades e governação da Internet em África” (AfDec, 2014, p. 4).

A declaração se guia pelos seguintes princípios: abertura; acesso à Internet e preço comportável; liberdade de expressão; direito à informação; liberdade de reunião e associação e Internet; diversidade cultural e linguística; direito ao desenvolvimento e acesso ao conhecimento; privacidade e proteção de dados pessoais; segurança, estabilidade e resiliência da Internet; grupos marginalizados e grupos em risco; direito a processo judicial; governação *multi-stakeholder* e democrática da Internet; e, igualdade de género. Vale sublinhar dois princípios:

Pelo princípio do direito à informação “todos têm direito ao acesso à informação na Internet. Toda a informação produzida com apoio de fundos públicos, incluindo pesquisa científica e social, deve ser livremente disponível a todos, também na Internet” (AfDec, 2014, p. 11). Quanto ao princípio de Privacidade e proteção de dados pessoais:

Toda a gente tem o direito à privacidade online, incluindo o direito de protecção de dados pessoais que lhe digam respeito. Toda a gente tem o direito de comunicar anonimamente na Internet e a usar a tecnologia apropriada para garantir uma comunicação segura, privada e anónima. O direito à privacidade na Internet não deve ser sujeito a quaisquer restrições, excepto aquelas previstas na lei, que intendam um objectivo legítimo expressamente enunciado ao abrigo da legislação internacional em matéria de direitos humanos (como especificado no Princípio 3 desta Declaração) e são necessárias e proporcionais à prossecução de um objectivo legítimo (AfDec, 2014, p. 12).

Em 2017, os ministros responsáveis pelas tecnologias de informação e comunicação dos países africanos, reunidos em Argel, aprovaram a Declaração Africana sobre Governança da Internet. Com esta declaração, os países membros da UA se comprometeram, entre outras, a:

Proteger a Internet como um espaço público, dando prioridade ao interesse público em caso de conflito entre o interesse público e os interesses privados; Garantir a todos o direito de usar a Internet de maneira que respeite a privacidade, sem prejuízo das limitações necessárias prescritas pelos requisitos de segurança pública, combate ao crime cibernético, extremismo violento e terrorismo (UA, 2017).

No ano seguinte, a Internet Society (ISOC) e a UA traçaram diretrizes relativas à proteção de dados pessoais para a África. Essas diretrizes visam facilitar a implementação da Convenção de Malabo e realçam a importância de assegurar a confiança nos serviços *online*, com vista a manter uma economia digital produtiva e

benéfica. As diretrizes também orientam os indivíduos a terem um papel mais ativo na proteção dos seus dados pessoais. Ademais, elas levam em conta as seguintes características do contexto africano:

A significativa diversidade cultural e jurídica através do continente, com expectativas de privacidade diferentes; variações no acesso à tecnologia e aos serviços em linha, entre os Estados membros; sensibilidades referentes à etnia e à definição do perfil sem consentimento, no contexto do estado nação; níveis diferentes de capacidade em áreas como a tecnologia e a lei e administração relacionada com a tecnologia; riscos decorrentes da elevada dependência de fabricantes e de fornecedores de serviços não africanos (a capacidade limitada dos Estados-membros da União Africana de influenciarem o comportamento de fornecedores de serviços externos; risco potencialmente acrescido de uso indevido dos dados se o conteúdo e os serviços forem fornecidos unicamente por empresas estrangeiras). Estes factores podem aumentar a dificuldade da formulação e aplicação de uma política consistente entre e por vezes mesmo dentro, dos estados-membros (ISOC; UA, 2018, p. 7).

Os países africanos, quanto à promulgação de normativas de proteção de dados pessoais, se enquadram em três categorias, segundo Greenleaf e Cottier (2022). Os autores identificam uma categoria de países com leis principais promulgadas por uma legislatura e que essas leis atendem aos critérios de uma lei de privacidade de dados; uma categoria de países com projetos de lei oficiais para leis de privacidade de dados propostas; e uma categoria de países em que não há nenhuma lei ou projeto de lei de privacidade de dados que atenda aos critérios básicos (Greenleaf; Cottier, 2022). Para os países que contam com uma normativa de proteção de dados pessoais

Quase todas [...] permitem a nomeação de uma autoridade de proteção de dados (DPA), separada de qualquer Ministério, o que é considerado amplamente como um elemento essencial de uma lei de privacidade de dados eficaz. As exceções são a Nigéria, Uganda e (enquanto se aguarda uma segunda lei) Congo-Brazzaville. Em algumas regiões do mundo, um modelo de aplicação por ministérios com responsabilidades setoriais, em vez de uma DPA separada, ainda tem alguns adeptos, mas eles estão desaparecendo (Greenleaf; Cottier, 2022, p. 4).

Na região da África Austral, diversos países já adotaram alguma normativa específica de proteção de dados pessoais. Podemos destacar os países fronteiriços de Moçambique, com Malawi sendo o país com a mais recente normativa, aprovada em 2024. Em 2022, Tanzânia e Eswatini aprovaram normativas de proteção de dados. A Zâmbia e o Zimbabwe já o tinham feito em 2021. A lei da África do Sul data de 2013, embora tenha entrado, de fato, em vigor, em meados de 2021. O quadro 12 na página seguinte, ilustra estas e outras as principais normativas africanas de proteção de dados pessoais.

Ora, essa lei da África do Sul que mencionamos acima, “pode ser um estímulo significativo para a adoção de leis, pelo menos nos outros países da SADC, devido ao papel da África do Sul como potência econômica regional” (Greenleaf; Cottier, 2022, p. 16). Quer dizer, Moçambique pode se espelhar na África do Sul, colher suas experiências para melhor elaborar e implementar a sua própria normativa de proteção de dados pessoais.

Quadro 12 - Principal legislação africana de proteção de dados pessoais

Ano	Instrumento normativo	País ou organização
2024	Lei nº 3 de 2024, Lei de Proteção de Dados ⁹	Malawi
2023	Lei de Proteção de Dados da Nigéria ¹⁰	Nigéria
2022	Lei nº 11 de 2022, Lei de Proteção de Dados Pessoais ¹¹	Tanzânia
	Lei nº 5 de 2022, Lei de Proteção de Dados ¹²	Eswatini
2021	Lei nº 3 de 2021, Lei de Proteção de Dados ¹³	Zâmbia
	Lei nº 5/2021, Lei de Proteção de Dados ¹⁴	Zimbabwe
2018	Diretrizes relativas à proteção de dados pessoais para África.	Internet Society União Africana
2017	Declaração Africana sobre Governança da Internet	União Africana
2014	Convenção de Malabo	União Africana
	Declaração Africana sobre Direitos e Liberdades na Internet	AfDec
2013	Lei nº 4 de 2013, Lei de Proteção de Informações Pessoais (POPIA) ¹⁵	África do Sul
	Lei Modelo sobre proteção de dados	SADC
2009	Lei nº 09-08, Lei sobre a proteção de indivíduos com relação ao processamento de dados pessoais ¹⁶	Marrocos
1981	Carta Africana dos Direitos Humanos e dos Povos	OUA

Fonte: Elaborado pela autora

No quadro acima, são apresentadas as principais normativas africanas de proteção de dados pessoais, com especial enfoque nas normativas da UA e nas normativas dos países da SADC. No quadro a designação das normativas dos países são apresentadas em língua portuguesa mediante tradução nossa.

⁹ Act No. 3 of 2024, data Protection.

¹⁰ Nigeria Data Protection Act.

¹¹ Act No. 11 of 2022, Personal Data Protection Act.

¹² Act No.5 of 2022, Data Protection.

¹³ Act No. 3 of 2021, Data Protection.

¹⁴ Act No. 5/2021, Data Protection.

¹⁵ Act n.º 4 of 2013, Protection of Personal information Act.

¹⁶ Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data.

Como apontamos na introdução desta seção, o mapeamento da legislação de Moçambique atinente a proteção de dados pessoais é feito em seção a parte, portanto na seção 7 a seguir.

7 O QUADRO LEGAL MOÇAMBICANO DA PROTEÇÃO DE DADOS PESSOAIS

Esta seção é dedicada ao mapeamento legal atinente à proteção de dados pessoais em Moçambique. É apresentada a principal legislação conexa através da qual se desenha uma linha de tempo, bem como são identificados os principais atores, enquanto instituições, na proteção de dados pessoais em Moçambique.

7.1 Legislação moçambicana de proteção de dados pessoais: linha de tempo

Para desenhar o quadro da principal legislação moçambicana de proteção de dados pessoais, será preciso lembrar a delimitação temporal desta pesquisa que vai desde 1992, ano em que foi aprovado o primeiro Sistema Nacional de Arquivos, até 2024 ano em que foi apresentada pelo INTIC, a Proposta de Lei de Proteção de Dados Pessoais¹⁷. Portanto, nota-se que Moçambique ainda não conta com uma lei específica de proteção de dados pessoais, o que significa que nesta seção trabalharemos com legislação conexa à proteção de dados pessoais.

É importante antes de avançar para qualquer outra normativa conexa de proteção de dados pessoais, começar por observar o que a Constituição da República de Moçambique (CRM) aponta sobre esta questão. Assim, no Capítulo III dos Direitos, liberdades e garantias individuais, o artigo 71 sobre Utilização da informática, consagra que

- Art. 71, 1. É proibida a utilização de meios informáticos para registo e tratamento de dados individualmente identificáveis relativos às convicções políticas, filosóficas ou ideológicas, à fé religiosa, à filiação partidária ou sindical e à vida privada.
2. A lei regula a protecção de dados pessoais constantes de registos informáticos, as condições de acesso aos bancos de dados, de constituição e utilização por autoridades públicas e entidades privadas destes bancos de dados ou de suportes informáticos.
3. Não é permitido o acesso a arquivos, ficheiros e registos informáticos ou de bancos de dados para conhecimento de dados pessoais relativos a terceiros, nem a transferência de dados pessoais de um para outro ficheiro informático pertencente a distintos serviços ou instituições, salvo nos casos estabelecidos na lei ou por decisão judicial.
4. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação (Moçambique, 2004).

¹⁷ Esta proposta é objeto de apreciação e análise na próxima seção.

É interessante observar na íntegra o artigo 71 pois para além de plasmar os fundamentos da proteção de dados pessoais em Moçambique, ainda que seja numa dimensão mais informática, este mesmo artigo faz o devido balanço, no seu nº 4, com o acesso à informação por parte dos titulares dos dados pessoais. Este aspecto é colocado na Lei das transações eletrônicas, sobre a qual iremos nos debruçar mais adiante.

O Decreto nº 33/92, de 26 de outubro que institui o Sistema Nacional de Arquivos (Moçambique, 1992), assinala um marco extremamente importante para a área de arquivos em Moçambique, pois se trata da instituição do primeiro sistema de arquivos moçambicano a esse nível. Neste sistema, o AHM desempenhava as funções de órgão central, quer dizer, conforme o artigo 8, cabia ao AHM, por exemplo, “Art. 8 [...] propor a política geral de acesso aos arquivos, respeitadas as normas de confidencialidade a que estão sujeitos determinados documentos” (Moçambique, 1992). Portanto a noção da proteção de dados pessoais já estava presente.

O SNA 1992 foi revogado em 2007, pelo Decreto nº 36 /2007, de 27 de agosto que aprova o Sistema Nacional de Arquivos do Estado (Moçambique, 2007). Nesta versão de sistema, o órgão central do sistema passa a ser outro ator, são aprovados instrumentos de gestão de documentos e é apontado, no n.º1 do artigo 16 que é permitido o acesso aos documentos depositados em arquivos públicos salvaguardando-se os princípios que regulam o segredo estatal e a inviolabilidade da vida privada.

Em 2018, o SNAE foi revisto, tendo sido aprovada a revisão pelo Decreto nº 84/2018, de 26 de dezembro (Moçambique, 2018). Através da alínea c, do artigo 25, ficou decretado que as instituições abrangidas pelo SNAE 2018, devem assegurar a preservação do caráter sigiloso dos [documentos] que dizem respeito à ordem nacional e à segurança pública, ao resguardo da inviolabilidade da intimidade e da vida privada, bem como aos relativos aos segredos protegidos por lei. Assim, é aqui evocada à questão da proteção de dados pessoais, à semelhança das suas versões anteriores.

Há um instrumento legal anterior a este período que não devemos ignorar. A Lei nº 12/79, de 12 de dezembro (Moçambique, 1979), visa proteger o segredo estatal relativamente a todos os documentos contendo dados e informações classificadas.

Esta lei chega a definir o grau de sigilo a considerar em face dos dados ou informações contidas nos documentos classificados, sendo eles, conforme o artigo 5, segredo de estado; secreto; confidencial; e, restrito (Moçambique, 1979).

Em 2006, algumas estratégias que interessam à área dos arquivos e da proteção de dados foram aprovadas. Uma, tratamos na seção em que descortinamos a arena arquivística moçambicana, é a EGDAE. A outra merece apreciação neste espaço, a Estratégia de Governo Electrónico de Moçambique.

Dentre os desafios que serão determinantes no planeamento e definição de projetos e na implementação desta estratégia, destaca-se o desafio ligado à segurança e à privacidade. Conforme se pode ler no texto da estratégia

Com a implementação da Estratégia de Governo Electrónico, serão estabelecidas regras de segurança e protecção de dados. A questão do equilíbrio entre a protecção de dados e a legítima necessidade do acesso à informação pública permanecerá, no entanto, um desafio. O acesso equilibrado a dados e informação é uma das fundações de uma sociedade informada e da economia do conhecimento (Moçambique, 2006, p. 9).

Foram previstos três elementos-chave para a estratégia, uma plataforma comum de comunicação; políticas e regulação; e, capacitação institucional e humana. Sobre políticas e regulação, o governo entendeu que para além de políticas de segurança de dados eletrónicos, seriam necessários normativas sobre assinaturas digitais, sistemas de verificação autenticação de terceiras partes e evidência eletrônica. Mais abaixo tratamos de alguns instrumentos que foram aprovados com este teor. Na estratégia foi considerado necessário

um quadro legal para facilitar o uso amplo e autorizado da informação do Governo, sem deixar de proteger a privacidade e os interesses dos cidadãos e do empresariado. Um exemplo de onde tal quadro é necessário está na classificação da Informação do Sector Público: acesso e direito de acesso a dados 'secrets', 'privados' ou 'confidenciais', estejam eles directamente disponíveis para o público ou sejam disponibilizados por meios de canais apropriados da comunicação social, etc. (Moçambique, 2006, p. 14).

Um instrumento mais recente é a Lei do Direito à Informação, Lei nº 34/2014, 31 de dezembro (Moçambique, 2014). Ela aponta no artigo 4 que o exercício do direito à informação rege-se, entre outros, pelos princípios de respeito à dignidade da pessoa humana; transparência da atividade das entidades públicas e privadas; e; respeito pela informação classificada. Estes princípios encontram no seu espírito uma alusão à proteção de dados pessoais. Este espírito é reforçado pelo artigo 20 em que são apontadas as restrições e limites, onde no nº 1 lê-se que “Art. 20, nº 1, o direito à

informação pode ser restringido, condicionado ou limitado quando a informação solicitada tenha sido classificada como segredo de Estado, secreta, restrita e confidencial” (Moçambique, 2014). Ainda no mesmo artigo está plasmado que

2. Sem prejuízo de outras restrições expressamente estabelecidas em legislação específica, as restrições referidas no número anterior aplicam-se nos seguintes casos: a) segredo de Estado; f) dados pessoais constantes de ficheiros electrónicos em poder de autoridades públicas ou privadas; h) informação referente à vida e intimidade privada dos cidadãos (Moçambique, 2014).

Esta lei é clara ao determinar no artigo 25 que “Art. 25, as informações relativas à reserva da intimidade na vida privada de uma pessoa física identificada ou identificável na posse de autoridades não podem ser divulgadas, senão em virtude de uma decisão judicial” (Moçambique, 2014) e no artigo 27

Art. 27, não é fornecida nem divulgada a informação relativa aos direitos de personalidade, nomeadamente, a que causar danos ou prejuízos ao direito à honra, ao bom-nome e à imagem pública” e “a informação relativa a imagens da vida privada só pode ser divulgada com expresse consentimento do seu titular (Moçambique, 2014).

Em 2016 a Lei das Telecomunicações foi alterada pela Lei nº 4/2016, de 3 de junho (Moçambique, 2016). O nº 3 do artigo 12 sobre Redes e serviços privativos de telecomunicações, aponta que com exceção e mediante autorização da autoridade que regula as telecomunicações,

o proprietário da rede privativa pode revender a capacidade existente disponível das suas instalações, ceder ou transferir ou, por qualquer forma, alienar os direitos de uso das referidas instalações a favor de um operador de telecomunicações, para a prestação de serviços públicos de telecomunicações, desde que não ponha em causa a privacidade e sigilo das informações dos clientes e não perigues a segurança do Estado (Moçambique, 2016).

Entendemos que o Estado tomou de antemão a responsabilidade para preservar a privacidade das informações dos clientes assim como tomou cautela para não prejudicar a própria segurança do Estado, o que em outras palavras, em redes públicas assume-se que a proteção de dados pessoais dos cidadãos está, pelo menos na letra, salvaguardada.

No ano seguinte, 2017, assistiu-se à aprovação, até ao momento a mais robusta (dentro das suas fraquezas) ainda que de forma conexa, de uma normativa de proteção de dados pessoais. Trata-se da Lei nº 3/2017, 9 de janeiro, Lei de Transacções Electrónicas (Moçambique, 2017). Ela é aprovada dada a “Art. 2, necessidade de regular as transacções electrónicas, o comércio electrónico e o

governo electrónico, bem como garantir a segurança dos provedores e utilizadores das tecnologias de informação e comunicação” (Moçambique, 2017) conforme se lê na parte introdutória desta normativa, e é aplicada às pessoas singulares, pessoas jurídicas públicas ou privadas que apliquem TICs nas suas transações eletrônicas e governo eletrônico.

O capítulo IX desta lei versa sobre a Protecção de Dados Electrónicos Pessoais. Composto por três artigos, este capítulo abarca as Obrigações do processador de dados (artigo 63), a Protecção de dados (artigo 64) e a Responsabilidade do processador de dados (artigo 65), embora nos pareça uma duplicação em termos de títulos e conteúdo arrolados nos artigos 63 e 65. Por essa razão eles aparecem sequenciados a seguir.

No que toca ao artigo 63, está disposto no nº 2 que “Art. 63, [...] nº 2, os objectivos para os quais os dados pessoais são recolhidos e a identidade do processador de dados devem ser especificados antes da sua recolha, e o seu uso posterior limitado aos objectivos indicados” (Moçambique, 2017d). Este número é bastante interessante mesmo sob uma perspectiva arquivística na qual a produção documental serve para atender às atividades da pessoa singular ou coletiva e o documento resultante pode ser eliminado se tiver cumprido as razões da sua existência. O nº 5 determina que “Art. 63, [...] nº 5, processador de dados deve proteger os dados pessoais contra riscos, perdas, acesso não autorizado, destruição, utilização, modificação ou divulgação” (Moçambique, 2017d). No nº 6, está plasmado que toda a pessoa tem o direito de:

- a) obter de um controlador de dados, ou confirmação acerca do controlador de dados ter ou não dados a seu respeito ou conhecimento a respeito do controlador de seus dados;
- b) ser comunicado a respeito de seus dados dentro de um período razoável, mediante pagamento de uma taxa;
- c) obter em caso de recusa do pedido efectuado nos termos das alíneas a) e b), a devida fundamentação;
- d) opor-se a dados que lhe dizem respeito e caso de aceitação, poder remover, rectificar, completar ou alterar (Moçambique, 2017d).

Este número e suas respectivas alíneas, embora apresente o “balanço acesso à informação – proteção de dados pessoais”, nos parece ao mesmo tempo apresentar alguma contradição com o direito consagrado na CRM seja pelos artigos 48 e 71, como pela lei específica de direito à informação, acima abordada. O pagamento de

uma taxa nos parece dar azo à violação do direito fundamental de acesso à informação e agrava-se quando esta informação é referente ao próprio titular.

Esta inquietação ganha corpo diante do nº 2 do artigo 65, através do qual “Art. 65 [...], nº 2, o processador de dados deve colocar à disposição de qualquer pessoa, informação específica acerca das suas políticas e práticas relacionadas com a gestão de informação pessoal” (Moçambique, 2017d). Esta informação inclui

- a) o nome ou título e endereço do responsável pelas políticas e práticas relativas à gestão de informação pessoal e a quem devem ser dirigidas queixas ou questões;
- b) a forma de obtenção de acesso à informação pessoal retida pelo processador de dados;
- c) a descrição do tipo de informação pessoal retida pela organização, incluindo um relatório geral da sua utilização (Moçambique, 2017d);

Quanto ao artigo 64, a lei determina, em parágrafo único que

Art. 64, parágrafo único, não é permitido o acesso a arquivos, ficheiros e registos informáticos ou de bancos de dados para conhecimento de dados pessoais relativos à terceiros, nem a transferência de dados pessoais de um para outro ficheiro informático pertencente a distintos serviços ou instituições, salvo nos casos estabelecidos por diploma legal ou por decisão judicial (Moçambique, 2017d).

A lei apresenta um glossário em que são definidos diferentes termos aplicados no âmbito desta e parece-nos oportuno apresentar, no quadro a seguir, alguns desses termos definidos.

Quadro 13 – Definições no âmbito da Lei de Transacções Electrónicas

Termo	Definição
Dados pessoais	Qualquer informação relativa a uma pessoa singular que possa ser identificada direta ou indiretamente através da referência a um número de identificação ou a um ou mais fatores específicos à mesma
Documento electrónico	Conjunto de dados lógicos armazenados em suporte susceptível de poder ser lido por equipamentos electrónicos de processamento
Titular	Pessoa singular ou coletiva identificada num certificado como a detentora de um dispositivo de criação de assinatura
Processador de dados	Qualquer pessoa pública ou privada, singular ou coletiva, que requeira, recolha, processe ou armazene eletronicamente informação pessoal de ou a respeito de um sujeito de dados

Fonte: Adaptado de Moçambique (2017d).

Ao observarmos os termos definidos no glossário da lei bem como nos termos apresentados no quadro 12, constatamos a ausência da definição de um dos termos bastante usado ao longo do texto da lei, controlador de dados. Mas também ao olharmos para estas definições apresentadas no quadro 9, percebemos o distanciamento com delas com as noções do entorno arquivístico, como se nota pela

utilização do termo armazenamento e não arquivamento, mesmo em situação de definição do termo documento de arquivo. Ademais, o ser definido o termo processador de dados, parece surgir uma outra figura que carece de definição, o sujeito de dados.

Em 2017 também foi aprovado o Regulamento do Quadro de Interoperabilidade, pelo Decreto nº 67/2017: 1 de dezembro (Moçambique, 2017e). O quadro de interoperabilidade é, segundo o Artigo 1

Art. 1, Quadro de Interoperabilidade de Governo Electrónico é um conjunto de princípios, padrões, directrizes e arquitecturas técnico-organizacionais estabelecidas pelo Governo, para assegurar a partilha e reuso de dados entre infra-estruturas e de tecnologias de informação e sistemas de informação das instituições públicas (Moçambique, 2017e).

São vários os princípios pelos quais se orienta o quadro de interoperabilidade. O artigo 4 arrola:

Art. 4, a) Princípio da Legalidade; b) Princípio da Transparência; c) Princípio da Prossecução do Interesse Público e Protecção dos Direitos e Interesses do Cidadão; d) Princípio da Integridade de Dados e Informação; e) Princípio da Confidencialidade; f) Princípio da Autenticidade; g) Princípio de Partilha de Dados entre as entidades da Administração Pública para a prossecução de uma actividade do Estado; h) Princípio de Recolha de Dados do Cidadão Única Vez pela Administração Pública; i) Princípio de Dados Autoritários; j) Princípio da Celeridade dos Processos Administrativos (Moçambique, 2017e).

Destes, é oportuno apreciarmos com maior detalhe 4 princípios. Conforme o artigo 8, com o princípio da Integridade de Dados e Informação, “art. 8, aplicando o Quadro de Interoperabilidade de Governo Electrónico deve-se assegurar a integridade dos dados e da informação partilhada, mantendo a sua origem e não podendo ser alterados, se não por pessoas autorizadas nos termos da lei.” (Moçambique, 2017e). Com o Princípio da Confidencialidade, “Art. 9, o Quadro de Interoperabilidade de Governo Electrónico, para a salvaguarda dos direitos das pessoas singulares e colectivas, respeita as matérias confidenciais e deve garantir que a informação é somente acedida por pessoas autorizadas nos termos da lei.” (Moçambique, 2017e).

O artigo 12 dispõe sobre o princípio de recolha de dados do cidadão uma única vez pela administração pública, um princípio que julgamos crucial quando tratamos de dados pessoais e todos os direitos e deveres associados. Portanto, neste artigo está disposto que

Art. 12, 1. A Administração Pública deve recolher os dados do cidadão uma única vez, sem prejuízo do estabelecido na legislação específica, passando

os mesmos a estar disponíveis para a utilização das demais entidades públicas, na prossecução dos serviços de Governo Electrónico;
 2. As entidades da Administração Pública são obrigadas, usando o Quadro e a Plataforma de Interoperabilidade, a localizarem e a reutilizarem os dados já disponibilizados pelo cidadão;
 3. O disposto no nº 1, do presente artigo, não se aplica quando a legislação específica exija actualização relativa à recolha de dados do cidadão (Moçambique, 2017e).

Aqui, mais uma vez o balanço “acesso à informação – proteção de dados pessoais”, vem ao de cima. Não só o acesso aos dados deve ser efetivo por parte do titular, para fins de correção e outros, como também este cidadão titular dos dados deve ser informado de toda a movimentação sobre os seus dados. Entendemos que no momento da coleta, o titular deve ser informado que outras instituições poderão ter acesso aos dados e/ou utilizá-los. Contudo, este princípio parece entrar em choque com o princípio de finalidade que caracteriza as normativas de proteção de dados pessoais. Aliás, o nº 2 do artigo 63 da Lei das Transações Electrónicas que vimos anteriormente, é deste princípio um exemplo.

O último dos 4 princípios que estamos a apreciar é o Princípio de Dados Autoritativos. No Artigo 13 lê-se

Art. 13, um dado autoritativo é aquele que é recolhido e gerido em processos que asseguram que é único e autêntico em relação à pessoa física, pessoa jurídica, ou ao evento administrativo, de modo que as outras entidades da Administração Pública não precisem de voltar a recolher esse dado, mas sim de utilizá-lo (Moçambique, 2017e).

Segundo o plasmado no nº 1 do artigo 18º, “Art. 18, nº 1, compete ao Conselho de Ministros, definir as instituições com mandato de recolher e disponibilizar dados autoritativos no âmbito da Administração Pública e de sistemas de governo electrónico em Moçambique [...]” (Moçambique, 2017e). No glossário deste decreto são definidos os dados autoritativos como “os dados sobre pessoas singulares, colectivas, jurídicas e actos administrativos oficialmente reconhecidos, que podem ser certificados e fornecidos por uma fonte autorizada” (Moçambique, 2017e). No mesmo glossário é definida a

Reutilização da Informação e dos Dados [como a] capacidade que os sistemas de informação possuem para a prestação de serviços públicos na partilha e utilização de dados, que são colectados por um determinado sistema ou serviço, fonte autorizada para a recolha e partilha de dados, garantido que o cidadão e o sector privado forneçam os seus dados básicos apenas uma vez e estes sejam reutilizados ou partilhados várias vezes, segundo as regras que forem definidas (Moçambique, 2017e).

A Resolução nº 17/2018, de 12 de dezembro, aprova a Política para a Sociedade de Informação de Moçambique, além de revogar a Resolução nº 28/2000, de 12 de dezembro (Moçambique, 2018b), a antiga Política de Informática.

Contextualizando esta política, o Conselho de Ministros aponta que

A revolução trazida pelas Tecnologias de Informação e Comunicação (TICs) é uma realidade em Moçambique e em todo mundo e tem um significativo impacto na história, forma de viver, trabalhar e interagir da humanidade. Em Moçambique, nos finais da década noventa iniciou-se o processo de consciencialização da sociedade sobre o papel e o potencial das TICs como alavanca do desenvolvimento socioeconómico (Moçambique, 2018b).

Não sabemos se esse processo de consciencialização da sociedade sobre o papel e o potencial das TICs para o desenvolvimento socioeconómico incluiu também os aspectos negativos e ou de risco à integridade de cada um dos cidadãos moçambicanos, ou mesmo da sociedade como um todo ou ainda do Estado que o uso das TICs (e não só) pode acarretar.

Na introdução, o Conselho de Ministros indica que essa política

vem fornecer a visão, missão, objectivos e um quadro de princípios que permitirão que as TICs se assumam como uma alavanca para o desenvolvimento económico e social de Moçambique promovendo a redução da pobreza e a melhoria das condições de vida dos moçambicanos, a melhoria da competitividade do sector empresarial e o consequente crescimento económico, a modernização do aparelho do Estado e da prestação de serviços ao cidadão e uma maior justiça social através do aprofundamento da democracia e a promoção da transparência (Moçambique, 2018b).

E que

A implementação da Política para a Sociedade da Informação e seus instrumentos não será possível sem a criação de um ecossistema inclusivo composto pelo Estado, o sector público, o sector privado, as instituições de ensino, pesquisa e desenvolvimento, as organizações não-governamentais e socioprofissionais, os parceiros de cooperação, as comunidades e o cidadão (Moçambique, 2018b).

Isto significa que com a política para a Sociedade da Informação sendo implementada, se espera que o cidadão moçambicano encontre maior abertura das/nas instituições públicas e serviços modernos que lhe permitam ter, com celeridade, acesso à informação de interesse público e que lhe digam respeito, bem como ver a sua integridade, a sua honra, seu bom-nome, entre outros direitos e liberdades, salvaguardados, incluindo a proteção dos seus dados pessoais.

A Política para a Sociedade da Informação rege-se por um conjunto de seis princípios que guiam as estratégias, os planos de ação e as iniciativas a implementar no âmbito da Sociedade da Informação. Aliás, um dos princípios orientadores desta política é o Princípio da Segurança da Informação. Sobre ele o governo aponta que

O desenvolvimento de uma sociedade, alavancada pela utilização de tecnologias de informação e comunicação tem inúmeras vantagens, mas tem simultaneamente riscos que devem ser acautelados. Enquanto, por um lado, permite estimular uma cultura de partilha, de socialização, de transparência e de criação do conhecimento, por outro, faz emergir questões relacionadas com a protecção, segurança, confidencialidade e privacidade da informação. É assim que, através da Política para a Sociedade da Informação, se prevê a garantia da disponibilidade, da integridade, da confidencialidade e da autenticidade da informação, limitando a ocorrência de crimes relacionados com a violação dos princípios da segurança da informação (Moçambique, 2018b).

Entendemos assim que esta política, associada à Lei das Transações Electrónicas, robustece ou pelo menos pode robustecer o cenário de protecção de dados pessoais em Moçambique, com cada vez mais aspectos concretos, ações concretas a serem desenvolvidas para a protecção dos dados pessoais e sobretudo um amparo que parece cada vez maior da parte do executivo. Contudo, ainda nos inquieta uma aparente ignorância ou desconhecimento dos aspectos arquivísticos na elaboração e implementação dessas normativas, pois como se pode notar, há sempre maior atenção à parte informática.

Ora, a Política para a Sociedade da Informação está estruturada em 7 eixos de intervenção que é a tradução das áreas com prioridade. São eles: educação e desenvolvimento humano; saúde; governança eletrônica ; agricultura, pescas, ambiente e desenvolvimento rural; indústria, comércio e serviços; acesso e conectividade; e, políticas e regulação. Olhando na especialidade o eixo “políticas e regulação”, sobressaem mais os aspectos concretos que aventamos acima, conforme se lê no seu texto:

O desenvolvimento das tecnologias implica a existência de um ambiente regulatório favorável, nomeadamente no que tange às questões da privacidade e segurança da informação, resposta a crimes de natureza cibernética e protecção de dados e privacidade, uma vez que são pilares essenciais na promoção da confiança por parte dos utilizadores (cidadãos e empresas). [...] Esta é uma nova realidade que obrigará os governos, os agentes de regulação e os operadores de mercado a um esforço de aprendizagem e de adaptação. [...] Em Moçambique, o desenvolvimento deste tipo de instrumentos é ainda incipiente, existindo áreas para as quais ainda não está prevista regulação e/ou regulamentação, nomeadamente ao nível da segurança da informação e protecção de dados do cidadão (Moçambique, 2018b).

Este reconhecimento é bastante importante para que se dê o devido passo para a elaboração e implementação de normativas específicas atinentes à estas matérias, em particular, atinentes à proteção de dados pessoais. E neste contexto, de acordo com a Resolução nº 17/2018, de 12 de dezembro, esta política assume como prioridades:

Assegurar a existência de um quadro legal e regulamentar actualizado e que responda aos desafios da massificação das TICs; Definir e divulgar políticas de privacidade que protejam a informação obtida pelos organismos públicos relativamente ao cidadão; Criar políticas e legislação no âmbito da protecção de dados; Criar políticas e legislação para a protecção do consumidor; Criar políticas e legislação de segurança cibernética; Promover a adesão de Moçambique à políticas, instrumentos legais e convenções regionais e internacionais sobre a Sociedade da Informação (Moçambique, 2018b).

Entendemos com isto que, ainda que neste momento Moçambique não conte com uma normativa específica de proteção de dados pessoais, esta está em rota de elaboração. Aliás, tivemos acesso através do *site* do Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC), à uma proposta de Lei de Proteção de Dados que analisaremos mais adiante.

Um dos aspectos que nos interessa ao refletirmos sobre a proteção de dados pessoais, é a questão ética e de conduta, e por isso recorremos à Resolução nº 15/2018, de 24 de maio de 2018 que aprova o Código de Conduta do Funcionário e Agente do Estado (Moçambique, 2018c). Conforme o Artigo 2, a aplicação deste Código é reforçada pelos códigos de conduta específicos de determinadas profissões ou setores.

São definidos neste Código de Conduta do Funcionário e Agente do Estado, os princípios e valores essenciais básicos que devem ser observados em harmonia com os deveres plasmados na Constituição da República de Moçambique e outras normativas aplicáveis. Assim, o Funcionário e Agente do Estado deve observar: a legalidade; o interesse público; a lealdade; o bem servir; o princípio da colaboração e boa-fé; a neutralidade político-partidária; o profissionalismo; a excelência no serviço; a probidade; a transparência; a prestação de contas; a meritocracia; a reserva e discrição; o uso adequado dos fundos e bens do Estado; o trabalho em equipa; a conduta privada exemplar fora do local do trabalho.

Todos estes princípios e valores essenciais básicos, cumulativamente, são importantes para um profissional no exercício das suas funções, em particular para o

arquivista na proteção de dados pessoais. Sem ignorarmos os demais, “reserva e discrição” chamam a nossa atenção. Sobre este, o Código de Conduta do Funcionário e Agente do Estado estabelece que:

1. Respeitando a legislação sobre o direito de acesso à informação, o funcionário e agente do Estado devem usar da maior reserva e discrição de modo a evitar a divulgação de factos e informações de que tenham tido conhecimento no exercício dos seus cargos, devendo:
 - a) Abster-se de divulgar, sem a devida autorização, informação secreta, confidencial ou oficial de que tenha tido conhecimento;
 - b) Abster-se de dirigir-se aos órgãos de comunicação social em matérias relacionadas com o serviço ou políticas oficiais sem a devida autorização;
 - c) Guardar sigilo sobre informação obtida em razão das suas funções em quaisquer documentos, artigos, livros, filmes ou quaisquer outros meios e não [os disseminar] sem permissão expressa do superior hierárquico competente (Moçambique, 2018c).

Como é notável, todo e qualquer funcionário ou agente do Estado em Moçambique deve agir de modo que não coloque em causa a proteção de dados pessoais, este dever ao mesmo tempo princípio e valor é mais ainda cobrado ao arquivista pois afeta diretamente o seu objeto de trabalho.

Moçambique ratificou, em 2019, através da Resolução nº 5/2019, de 20 de junho de 2019 (Moçambique, 2019a), a Convenção da União Africana Sobre Cibersegurança e proteção de dados pessoais, que, como vimos na seção anterior, é conhecida também por Convenção de Malabo. Com esta resolução considera-se, a Convenção, propícia para a criação de um Quadro Jurídico sobre a Cibersegurança e Protecção de Dados Pessoais, e consubstancia-se no compromisso existente dos Estados-Membros da União Africana no plano sub-regional, regional e internacional, com vista a construção da Sociedade de Informação.

No mesmo ano de 2019, foi criado o Sistema de Certificação Digital de Moçambique e aprovado o Regulamento do mesmo, pelo Decreto nº 59/2019, de 3 de julho (Moçambique, 2019b). Conforme o nº 1 do artigo 1, o “Art. 1, nº 1, Sistema de Certificação Digital de Moçambique abreviadamente designado por SCDM é um sistema que engloba as actividades de certificação digital de entidades públicas e privadas” (Moçambique, 2019b). O seu objeto, conforme o Artigo 2, é garantir um ambiente seguro de transações eletrónicas em Moçambique.

Para que de fato este ambiente eletrônico seja seguro, no artigo 27 estão estabelecidos ao que obrigatoriamente deve conter no plano de segurança, sendo dentre diferentes aspectos: a descrição da estrutura organizacional e funcional e da

atividade de certificação; a especificação dos requisitos de segurança física, lógica e operacional; requisitos de proteção da informação, incluindo distinção dos vários níveis de segurança e perfis de acesso implementados; a definição das funções que conferem acesso aos atos e instrumentos de certificação, respetivos requisitos de segurança e perfis de acesso; etc. O artigo ainda avança que no caso de estarem intrincadas matérias classificadas, o plano de segurança deve ser aprovado pela entidade competente para a respectiva fiscalização (Moçambique, 2019b).

E porque os aspectos arquivísticos permeiam estas normativas, ainda que os termos usados muitas vezes não sejam os adequados, conseguimos perceber no artigo 36 (Preservação de Longo Prazo), o espírito da preservação digital, consequentemente há uma ideia de gestão de documentos que adjacente. Este artigo estabelece

Art. 36, 1. Entidades Certificadoras devem informar os requerentes de certificados que para assegurar a preservação de longo prazo dos documentos electrónicos aos quais tenham sido apostas assinaturas electrónicas, será necessária a periódica aplicação de mecanismos que assegurem a sua integridade.

2. A preservação de longo prazo é feita mediante aplicação de validação cronológica e da utilização de algoritmos cuja segurança perdure para além do prazo pelo qual seriam considerados seguros os algoritmos utilizados inicialmente (Moçambique, 2019b).

Quanto à emissão dos certificados, o artigo 41 avança aspectos que, de alguma forma, apontam para um exercício de proteção de dados pessoais. Determina-se pelo nº 1 deste artigo que “a Entidade Certificadora garante que, durante o processo de emissão, os dados de registo do titular são tratados de forma segura e que a chave pública constante do certificado está relacionada com a correspondente chave privada do titular.” (Moçambique, 2019b). O nº 3 dispõe que “Art. 41, nº 3, a Entidade Certificadora assegura a protecção da confidencialidade e integridade dos dados de registo em todos os procedimentos de emissão.” (Moçambique, 2019b). Percebe-se nestes números, aspectos de proteção de dados pessoais.

O ano de 2019 foi marcado pela aprovação da revisão do código penal pela Lei nº 24/2019, que igualmente revogou o Artigo 2 do Decreto-Lei nº 182/74, de 2 de maio e o Código Penal aprovado pela Lei nº 35/2014 de 31 de dezembro (Moçambique, 2019c). No Artigo 252 que versa sobre devassa da vida privada, da seção I dos crimes contra a reserva da vida privada, no capítulo X com o mesmo título (Crimes Contra a Reserva da Vida Privada), está determinado no nº 1 que

Art. 252, 1. É punido com pena de prisão até 1 ano e multa correspondente, quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual:

- a) interceptar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica, imagem, fotografia, vídeo, áudio, facturação detalhada, mensagens de correio electrónico, de rede social ou de outra plataforma de transmissão de dados;
- b) captar, fotografar, filmar, manipular, registar ou divulgar imagem das pessoas ou de objectos ou espaços íntimos;
- c) observar ou escutar às ocultas pessoas que se encontrem em lugar privado; ou
- d) divulgar factos relativos à vida privada ou a doença grave de outra pessoa (Moçambique, 2019c).

O artigo seguinte, 253, versa sobre violação de correspondência ou de comunicações” e estabelece que

- 1. Quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até 1 ano e multa correspondente.
- 2. Na mesma pena incorre quem, sem consentimento, se intrometer no conteúdo de telecomunicação ou dele tomar conhecimento.
- 3. Quem, sem consentimento, divulgar o conteúdo de cartas, encomendas, escritos fechados, ou conteúdos de telecomunicações a que se refere o número anterior, é punido com a pena de 6 meses a 1 ano de prisão e multa correspondente (Moçambique, 2019c).

Com estes artigos do novo Código Penal, conseguimos notar que em Moçambique a violação de dados pessoais recebe tratamento criminal e é punido. Não temos competência para questionar o tamanho da pena prevista para este tipo legal de crime, mas nos parece que os danos que violação de dados pessoais podem causar, podem ser incomensuráveis e requerer, talvez penas mais proibitivas.

O Regulamento do Uso do Domínio .mz Moçambique, também apresenta disposições sobre proteção de dados pessoais. Este regulamento foi aprovado pelo Decreto nº 82/2020, de 10 de setembro (Moçambique, 2020). Conforme o glossário deste decreto, “Dominio. mz é o espaço na *Internet* cuja gestão é da responsabilidade de Moçambique” (Moçambique, 2020). E “Dados Pessoais [é] Informação relativa a uma pessoa singular identificada ou identificável (titular dos dados)” (Moçambique, 2020).

No capítulo VIII sobre Protecção de Dados Pessoais e responsabilidade e regime aplicável, seção I Protecção de dados, o artigo 39 que dispõe sobre o tratamento de dados pessoais, aponta no nº 1 que

Art. 39, 1. As acções de recolha, processamento e divulgação electrónica, nomeadamente via sistema WHOIS, de dados pessoais de responsáveis por nomes de domínio e subdomínios registados sob “.mz”, devem ser efectuadas de forma precisa, completa e actualizada, sem prejuízo do cumprimento das obrigações de confidencialidade que decorrem da lei aplicável (Moçambique, 2020).

O nº 2 do mesmo artigo aponta que “Art. 39, nº 2, os dados pessoais dos responsáveis pelo domínio são recolhidos e tratados para a finalidade de gestão, registo e manutenção dos domínios e subdomínios registados sob “.mz”.” (Moçambique, 2020). O nº 3 por sua vez dispõe que “Art. 39, nº3, os dados pessoais dos responsáveis pelo domínio são recolhidos directamente pela Entidade Reguladora, ou pelos Agentes de Registo para os fins descritos no número anterior.” (Moçambique, 2020). o nº 4 deste artigo avança que

Art. 39, nº 4, Os responsáveis pelo nome de domínio devem, a todo o tempo, solicitar o exercício dos direitos que a Lei aplicável neste âmbito lhes confere, nomeadamente o direito de acesso, actualização, rectificação e confirmação de dados pessoais de que sejam titulares (Moçambique, 2020).

Este número é interessante quando associamos aos princípios de proteção de dados pessoais, em que o titular dos dados deve ter direito de acesso aos seus dados coligidos, para fins de correção e/ou atualização, ou mesmo oposição. Parece que no âmbito deste decreto não há previsão de pagamento de taxas para a fruição deste direito, o que não acontece na lei das Transações Electrónicas. Imprimindo um espírito de acesso à informação e transparência, o decreto estabelece ainda, através do seu artigo 40 que

Art. 40, cabe à Entidade Reguladora a definição e publicação, em local de acesso público, nomeadamente no sítio de Internet por si gerido, da sua política de gestão de dados pessoais, a qual deve incluir, além dos requisitos previstos na lei aplicável, informação específica sobre as práticas relativas a recolha, tratamento e publicação de informação pessoal (Moçambique, 2020).

A Política de Segurança Cibernética e Estratégia da sua Implementação foram aprovadas pela Resolução nº 69/2021, de 31 de dezembro de 2021 (Moçambique, 2021). Esta política “aborda aspectos legais e tecnológicos que visam proteger pessoas (colectivas ou singulares) e bens, com destaque às infraestruturas críticas de informação no espaço cibernético sob a responsabilidade de Moçambique” (Moçambique, 2021). Portanto, seu maior objectivo é “assegurar a protecção de Activos de Informação públicos e privados e suas Infra-estruturas Críticas no espaço cibernético” (Moçambique, 2021).

A política é sustentada por 6 pilares. Chama-nos a atenção o terceiro pilar, Protecção de Activos de Informação. De acordo com o texto da resolução, o objetivo deste pilar é proteger informações e aplicações, por meio de

programas de certificação de qualidade e segurança das aplicações e infraestruturas, mecanismos de controlo de acessos, estratégias de protecção da confidencialidade, integridade e disponibilidade da informação, regulamentos de protecção de informação, adopção de soluções tecnológicas de protecção e de resiliência de sistemas e Activos de Informação, assim como de realização de auditorias e avaliação dos níveis de maturidade no âmbito de segurança cibernética (Moçambique, 2021).

Através deste mesmo pilar, o Conselho de Ministros, sublinha a importância da informação e da sua protecção, colocando nos seguintes termos:

A informação constitui um importante recurso para o desenvolvimento, segurança e defesa das nações, e qualquer impedimento ao acesso ou destruição podem pôr em causa a confiança de cidadãos ou interesses particulares, inclusive a soberania de um país. Por isso, devem ser implementadas medidas contra situações de ameaças às liberdades individuais, aos dados pessoais e, em suma, à privacidade, confidencialidade e integridade de dados (Moçambique, 2021).

Um campo em que é inquestionável a necessidade de medidas de protecção de dados pessoais e que o dado pessoal é seu objeto, é o campo da identificação civil. Em 2022 foi aprovada a Lei nº 6/2022, 20 de junho, que estabelece o Regime Jurídico de Identificação Civil e do Bilhete de Identidade do Cidadão Nacional (Moçambique, 2022). O objeto desta lei é, conforme o Artigo 1 “Art. 1, o regime jurídico relativo à recolha, processamento e conservação de dados pessoais individualizadores do cidadão nacional, com o fim de estabelecer a sua Identidade Civil e a emissão do Bilhete de Identidade” (Moçambique, 2022).

Sobre o acesso aos dados pessoais, o Artigo 36 dispõe que

Art. 36, 1. O cidadão nacional tem acesso aos seus elementos identificadores, constantes da base de dados da identificação civil, mediante pedido à entidade competente dos serviços de identificação civil.
2. Podem ainda aceder aos elementos referidos no número 1 do presente artigo, nos termos da lei, os descendentes, o cônjuge, os ascendentes, o tutor ou o curador do titular da informação ou, em caso de falecimento deste, os herdeiros, desde que mostrem interesse legítimo e não haja risco de intromissão na vida privada do titular da informação.
3. A informação referida no presente artigo é fornecida, mediante o pagamento de uma taxa, a fixar pelo Conselho de Ministros (Moçambique, 2022).

Inquieta-nos a pré-condição de pagamento de uma taxa para que se tenha acesso aos dados pessoais pois, à semelhança de outras normativas já mencionadas, parece-nos contrário à regra de acesso à informação gratuito. Portanto, não

entendemos esta medida. Isto pode levar a inibição da fruição do direito de acesso aos dados pessoais pelos titulares, mesmo até para casos de necessidade de retificação. Aliás, o Artigo 37 versa sobre correção de dados e estabelece:

Art. 37, 1. O cidadão nacional tem o direito de reclamar a correcção dos seus dados indevidamente registados ou omissos, mediante a apresentação da respectiva prova.
 2. O deferimento da reclamação do interessado com fundamento em erro ou omissão implica a rectificação do Bilhete de Identidade.
 3. A emissão do Bilhete de Identidade como resultado da correcção de dados com fundamento em erro ou omissão é feita mediante pagamento da respectiva taxa, salvo se o erro ou omissão for imputado aos serviços de identificação civil (Moçambique, 2022).

Ora, como o cidadão tomará conhecimento sobre incorreções e/ou omissões dos seus dados? Observa-se que o cidadão toma esse conhecimento apenas quando está em posse do seu Bilhete de Identidade (BI).

Os Artigo 38 (Conservação de dados após óbito) e 39 (Arquivo físico e digital), determinam que “Art. 38, Os dados pessoais do titular do Bilhete de Identidade falecido são conservados na base de dados até cinco anos após a data do óbito, ao fim dos quais são conservados em ficheiro histórico, a contar a partir daquela data” (Moçambique, 2022) e que “Art. 39, Os dados do cidadão nacional, constantes dos arquivos físico e digital, são organizados e conservados por ordem numérica” (Moçambique, 2022), respectivamente. Conseguimos notar aqui implícitas as noções de gestão de documentos.

A seção III, do capítulo IV que versa sobre Base de Dados de Identificação Civil e Protecção de Dados do Cidadão Nacional é dedicada à protecção de dados. O Artigo 40 dispõe que os Serviços de Identificação Civil são responsáveis pela protecção de dados pessoais contra riscos, perdas, acesso não autorizado, destruição, utilização, modificação ou divulgação (Moçambique, 2022).

Sobre o dever de sigilo, estabelecido no artigo 42, a lei em apreciação determina que “Art. 42os funcionários dos Serviços de Identificação Civil, bem como aqueles que no exercício das suas funções, tenham conhecimento dos dados pessoais registados na base de dados de identificação civil, estão vinculados ao dever de sigilo profissional” (Moçambique, 2022). Portanto o código de conduta e o código penal tem o seu devido lugar aqui, bem como, no caso dos arquivistas, a ética que rege a sua profissão.

No ano de 2023, dentre vários, foram aprovados dois dispositivos legais que merecem a nossa apreciação. A Lei nº 13/2023 (Moçambique, 2023a) e o Decreto nº 59/2023 (Moçambique, 2023b). O primeiro dispositivo aprova a Lei do Trabalho e revoga a Lei nº 23/2007, de 1 de agosto. Esta lei tem o artigo 8 dedicado à proteção de dados pessoais, onde segundo os nºs 1 e 3:

Art. 8, 1. O empregador não pode exigir ao trabalhador, no acto de contratação ou durante a execução do contrato de trabalho, a prestação de informação relativa à sua vida privada, excepto quando particulares exigências inerentes à natureza da actividade profissional o exijam por força da lei ou dos usos de cada profissão, e seja previamente fornecida, por escrito, a respectiva fundamentação.

[...]

3. Os dados pessoais do trabalhador, obtidos pelo empregador sob reserva de confidencialidade, bem como qualquer informação cuja divulgação viola a privacidade daquele, não podem ser fornecidos a terceiros sem o seu consentimento expresse, salvo se razões legais assim o determinarem (Moçambique, 2023a).

O segundo dispositivo, o Decreto nº 59/2023, 27 de outubro, aprova o Regulamento de Registo e Licenciamento de Provedores Intermediários de Serviços Electrónicos e de Operadores de Plataformas Digitais. No capítulo III sobre “Requisitos de Segurança das Plataformas Digitais”, determina no nº 3 do Artigo 32º que

3. Os Provedores Intermediários de Serviços Electrónicos e Operadores de Plataformas Digitais devem seleccionar os controlos de segurança adequados com base na análise de riscos [...] e na norma de segurança a ser definida pela Autoridade Reguladora de TIC, nas seguintes áreas de segurança:

[...]

b) segurança física e ambiental;

[...]

h) medidas para corrigir e mitigar violações dos sistemas de informação susceptíveis de causar a destruição, a perda acidental, a alteração, ou a divulgação ou acesso não autorizados de dados pessoais a tratar;

[...] (Moçambique, 2023b).

Como apontamos mais acima, a Lei das Transacções Electrónicas é em Moçambique até este momento instrumento de referência quando se trata de proteção de dados pessoais. O Artigo 37 (Tratamento dos dados pessoais), reforça este entendimento ao indicar que “O tratamento da informação, pelas plataformas digitais, que contenham dados pessoais, implica a notificação prévia à Entidade Competente, nos termos previstos na Lei das Transacções Electrónicas” (Moçambique, 2023b).

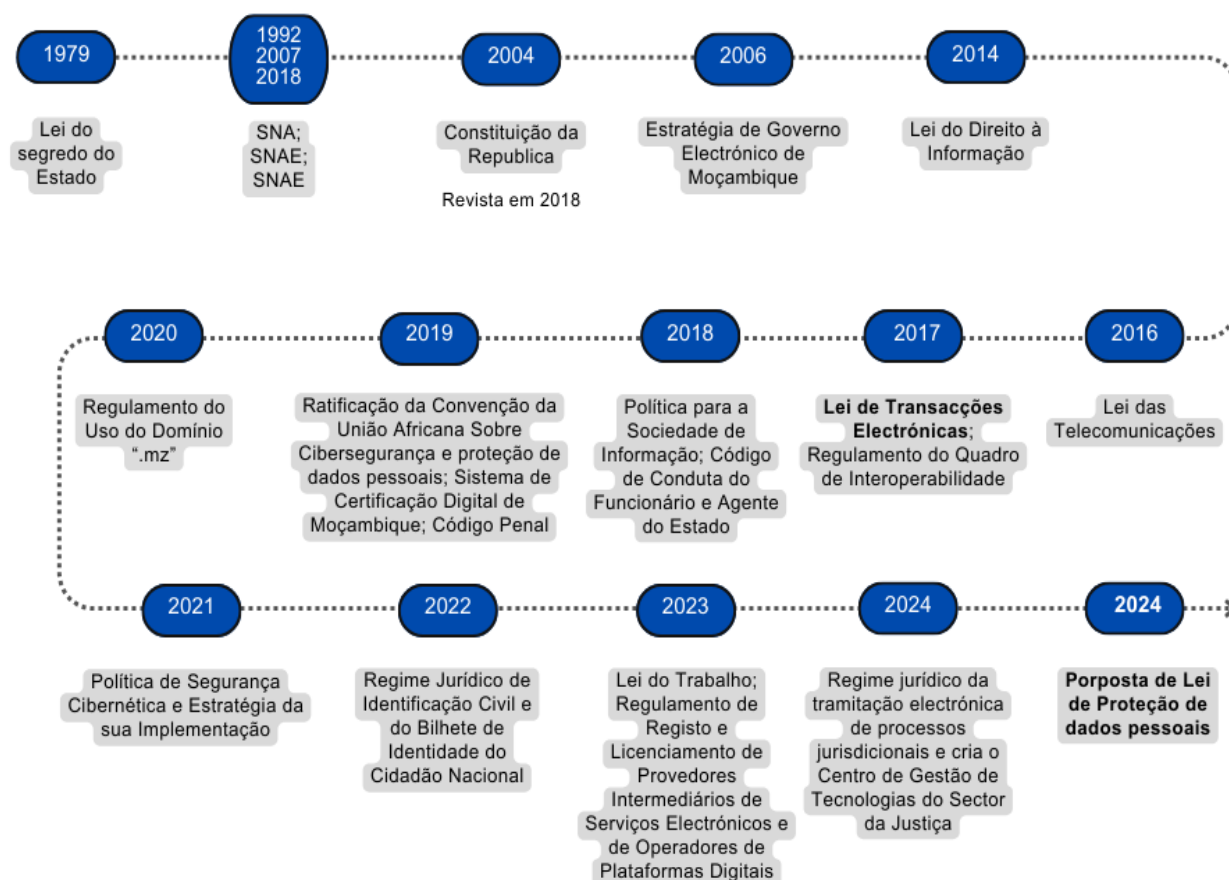
Mais recentemente em 2024, foi aprovada a Lei nº 8/2024, de 7 de junho de 2024, que estabelece o regime jurídico da tramitação electrónica de processos judiciais e cria o Centro de Gestão de Tecnologias do Sector da Justiça, abreviadamente designado CGTSJ (Moçambique, 2024). Este dispositivo é criado, pela

[...] necessidade de estabelecer os princípios e as normas de tramitação electrónica de processos judiciais, com vista a garantir maior celeridade processual, facilidade de acesso à justiça, segurança e protecção dos direitos fundamentais dos cidadãos, imprimir dinâmica ao processo de modernização e simplificação de procedimentos no Sector da Justiça, tendo em conta os desafios impostos pelas tecnologias de informação e comunicação (Moçambique, 2024).

No Artigo 31, em que são apresentadas as garantias, o nº 1 avança que para que seja garantida a protecção dos dados pessoais, da privacidade e de outros direitos fundamentais dos cidadãos e existindo algum receio da sua revelação na audição dos intervenientes processuais, realizada por videoconferência, a imagem deve ser desfocada, desviada ou inabilitada e o som distorcido (Moçambique, 2024). O nº 2 determina que quem preside a sessão deve garantir que o arguido preso possa conferenciar reservadamente com o seu advogado ou defensor, por videoconferência, nos termos estabelecidos nas leis processuais (Moçambique, 2024). Ainda que sejam aqui avançados aspectos para preservar os dados pessoais, a seção II (protecção de dados e segurança), Artigo 35 (Protecção de dados), determina que “Art. 35, os sistemas de tramitação electrónica de processos judiciais garantem o respeito pelo segredo de justiça e pelos regimes de protecção e tratamento de dados pessoais” (Moçambique, 2024).

No ano de 2024 tomamos conhecimento da existência de uma proposta de lei, preparada pelo Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC). Esta proposta é objeto de análise na oitava seção deste trabalho. Na página a seguir, representamos na figura 7, a principal legislação moçambicana atinente à protecção de dados pessoais que estivemos a abordar acima.

Figura 7 – Legislação moçambicana de Proteção de dados pessoais



Fonte: Elaborado pela autora.

Como fizemos referência, a figura acima ilustra a principal legislação moçambicana sobre a proteção de dados pessoais e, decorrente desta legislação, foi possível identificarmos aqueles que constituem os principais atores do ecossistema de dados pessoais e vamos apresentar aqueles que consideramos serem as principais instituições envolvidas na proteção de dados pessoais no cenário atual.

7.2 Principais atores do cenário de proteção de dados pessoais em Moçambique

Com base na legislação apreciada acima, pudemos identificar alguns atores que consideramos chave para a proteção de dados pessoais em Moçambique.

7.2.1 Instituto Nacional das Comunicações de Moçambique (INCM)

O Instituto Nacional das Comunicações de Moçambique (INCM) foi criado pelo Decreto nº 22/92 de 11 de novembro (Moçambique, 1992b). Em 2001, a sua forma de organização e o seu modo de funcionamento foram definidos pelo Decreto nº 32/2001, de 6 de novembro, que também revogou o Decreto nº 22/92 (Moçambique, 2001). Vinte anos depois, através do Decreto nº 39/2021, de 17 de junho (Moçambique, 2021), é aprovado o Estatuto Orgânico do Instituto Nacional das Comunicações de Moçambique, abreviadamente designado por INCM e revogado o Decreto nº 32/2001, de 6 de novembro.

Conforme este estatuto, no seu Artigo 2, o INCM é uma instituição pública, que desempenha as funções de regulação, supervisão, fiscalização, sancionamento e representação do sector das telecomunicações e postal. Ele é tutelado pelo Ministro que superintende a área das Comunicações, e, financeiramente é tutelado pelo Ministro que superintende a área das finanças, de acordo com o Artigo 5 (Moçambique, 2021).

São órgãos do INCM, o Conselho de Administração; o Conselho Fiscal; e, o Conselho Consultivo (Artigo 7). O Conselho de Administração é o órgão colegial responsável pela definição, implementação e gestão da atividade da INCM e pela direção dos serviços que a integram (Moçambique, 2021).

Quanto à estrutura, conforme o Artigo 28º, o INCM estrutura-se em: Divisão de Engenharia e Fiscalização; Divisão de Regulamentação; Divisão de Regulação de Mercado e Estatísticas; Divisão de Assuntos Corporativos; Fundo do Serviço de Acesso Universal; Gabinete Jurídico; e, Departamento de Aquisições.

Dentre os órgãos subordinados, encontra-se a Unidade de Controlo de Tráfego de Telecomunicações, abreviadamente designado por UCTT, subordinado ao Conselho de Administração, de acordo com o Artigo 36º. Esta unidade tem, entre outras, as seguintes funções:

- a) assegurar a implementação do controlo do tráfego de telecomunicações;
- b) gerir e manter actualizado o registo de subscritores de serviços telecomunicações;
- [...]
- e) garantir a protecção de dados dos utilizadores de telecomunicações;

- f) participar e colaborar em processos que requeiram investigação, por parte das entidades competentes, no acesso aos dados de qualquer natureza, decorrente da utilização das redes de telecomunicações;
 - g) coordenar a implementação de soluções para investigação e garantia de protecção dos cidadãos, quando esteja em causa a protecção contra qualquer forma de crime, usando as redes de telecomunicações;
 - h) actuar, sempre que necessário, na protecção das redes de telecomunicações contra eventuais ataques cibernéticos a interesses e infraestruturas críticas nacionais;
 - i) implementar e gerir os mecanismos de partilha de dados e colaboração para a melhoria da qualidade dos serviços prestados ao cidadão pelas entidades públicas e privadas usando redes de telecomunicações;
 - j) desenhar e propor planos de contingência nacional para a garantia de segurança e resiliência das comunicações em moçambique;
 - k) auditar os sistemas e infraestruturas das comunicações dos provedores das comunicações ao abrigo da legislação em vigor;
- [...] (Moçambique, 2021b).

É notória a função de protecção de dados desta instituição através da unidade que acabamos de indicar as suas funções mais específicas. Como se nota, esta função aparece de forma direta, mas também indiretamente quando há indicação de protecção da infraestrutura tecnológica, por exemplo.

7.2.2 Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC)

O Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC) foi criado pelo Decreto nº 9/2011, 4 de maio, dada a “necessidade, no domínio das tecnologias de informação e comunicação (TICs), de melhorar a prestação de serviços públicos e da governação” (Moçambique, 2011). Seu estatuto foi aprovado em 2012 pela Resolução nº 4/2012, de 19 de abril e o seu regulamento interno em 2017, pelo Diploma Ministerial nº 9/2017, 19 de janeiro. O estatuto sofreu alterações em 2020, assim como o regulamento interno foi atualizado em 2022 pelo Diploma Ministerial nº 34/2022, de 28 de março (Moçambique, 2022). De acordo com as disposições gerais deste regulamento, em seu Artigo 1º, o INTIC é uma instituição pública, dotada de personalidade jurídica e autonomia administrativa, e tem como objeto regular, supervisionar e fiscalizar o sector das TICs (Artigo 2).

São várias as competências do INTIC que podem ser vistas através do Artigo 6º. Portanto, entre outras competências, compete ao INTIC:

- a) garantir o respeito e cumprimento da Lei e os respectivos regulamentos;
- b) apresentar a proposta de regulamentos e outros diplomas de implementação da Lei de Transacções Electrónicas, dentro dos limites;

- c) desempenhar as funções de regulação, supervisão e fiscalização de TIC;
- d) assegurar a implementação do quadro de interoperabilidade do governo electrónico;
- e) aplicar sanções decorrentes da Lei de Transacções Electrónicas e demais legislação aplicável;
- f) divulgar e promover a aplicação das transacções electrónicas, do comércio electrónico e do governo electrónico;
- g) emitir, modificar, renovar, suspender ou cancelar as licenças e registos estabelecidos na Lei de Transacções Electrónicas;
- h) assegurar a gestão do domínio “.mz”;
- i) assegurar a implementação e funcionamento do Sistema de Certificação Electrónica do Estado (SCEE);
- j) propor um quadro legal de protecção do consumidor no âmbito das transacções electrónicas, do comércio electrónico e do governo electrónico;
- k) criar mecanismos de protecção da indústria e serviços nacionais de Tecnologias de Informação e Comunicação (TIC);
- [...]
- p) propor um quadro legal de protecção de dados pessoais e de combate a crimes cibernéticos;
- [...]
- t) realizar estudos das TIC e propor acções estratégicas para o desenvolvimento da Sociedade de Informação em Moçambique;
- [...] (Moçambique, 2022b).

São órgãos do INTIC, conforme o Artigo 7º, o Conselho de Administração; o Conselho Consultivo; o Conselho Fiscal; e o Conselho Técnico. A sua estrutura compreende: Divisão de Regulação e Fiscalização; Divisão de Licenciamento e Certificação; Divisão de Segurança Cibernética e Protecção de Dados; Divisão de Governança Digital; Gabinete Jurídico; Gabinete de Comunicação e Imagem; Departamento de Informática e Gestão Documental; Departamento de Administração e Finanças; Departamento de Recursos Humanos; Departamento de Estudos, Planificação e Cooperação; e, Departamento de Aquisições, como se lê no Artigo 19º. O nº 1 do Artigo 26º aponta as funções da Divisão de Segurança Cibernética e Protecção de Dados, que são:

- a) assegurar a criação de capacidade nacional de prevenção, monitorização, e combater incidentes de segurança cibernética;
- b) assegurar a produção e implementação de instrumentos normativos em matéria de cibersegurança;
- c) coordenar a Equipa Nacional de Resposta a Emergências Informáticas (CERT);
- d) estabelecer e coordenar o funcionamento da Rede Nacional de CSIRTs;
- e) estabelecer e coordenar o funcionamento do Centro Nacional de Operações de Segurança Cibernética (SOC Nacional);
- f) estabelecer o Observatório Nacional de Segurança Cibernética;
- g) estabelecer e gerir o Portal de Registo de Incidente Cibernéticos;
- h) contribuir para melhoria contínua da segurança dos sistemas de informação e de comunicação das infraestruturas críticas do Estado;
- i) promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis em matérias de cibersegurança a nível nacional, regional e internacional;

- j) dinamizar acções de formação e a qualificação de recursos humanos na área da segurança cibernética, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de segurança cibernética;
- k) apoiar o desenvolvimento das capacidades técnicas, científicas, promovendo projectos de inovação e desenvolvimento tecnológico na área da segurança cibernética;
- l) assegurar a implementação de medidas de segurança nos sistemas de informação e comunicação dos prestadores dos serviços digitais;
- m) propor directrizes para a Protecção de Dados Pessoais e da Privacidade;
- n) promover o conhecimento pelo cidadão de normas e das políticas públicas sobre protecção de dados pessoais e das medidas de segurança;
- o) empreender outras acções e iniciativas que concorram para a Segurança Cibernética e Protecção de Dados; e
- p) realizar as demais actividades que superiormente sejam determinadas nos termos do presente Estatuto Orgânico e demais legislação (Moçambique, 2022b).

O nº 2 do mesmo artigo aponta que a Divisão de Segurança Cibernética e Protecção de Dados é dirigido por um director de divisão e integra o Departamento de Segurança Cibernética e um Departamento de Protecção de Dados. São funções do Departamento de Protecção de Dados, conforme o Artigo 28º

- a) propor directrizes para a protecção de dados pessoais e da privacidade;
- b) promover o conhecimento pelo cidadão de normas e das políticas públicas sobre protecção de dados pessoais e das medidas de segurança;
- c) promover as abordagens de privacidade por desenho e por padrão;
- d) promover a realização de acções de formação sobre as boas práticas para a protecção de dados;
- e) assegurar o estabelecimento e o cumprimento das políticas estratégias nacionais de privacidade e proteção de dados;
- f) controlar e acompanhar a produção do Avaliação de Impacto sobre Protecção de Dados (AIPD);
- g) realizar estudos sobre o tratamento de dados pessoais;
- h) realizar a avaliação da exposição aos riscos de privacidade e mitigação com acções de melhoramento;
- i) controlar o funcionamento dos controladores e processadores de dados;
- j) estabelecer e manter actualizada a base de dados dos registos de tratamento de dados;
- k) empreender outras acções e iniciativas que concorram para a protecção de dados;
- l) realizar as demais actividades que superiormente sejam determinadas nos termos do presente Estatuto Orgânico e demais legislação (Moçambique, 2022b).

Por sua vez, o Departamento de Informática e Gestão Documental, que é dirigido por um Chefe de Departamento Autónomo, nomeado pelo Presidente de Conselho de Administração, compreende duas repartições, uma Repartição de Informática e uma Repartição de Gestão Documental. O Artigo 36º estabelece as funções da Repartição de Gestão Documental. São elas:

- a) implementar o Sistema Nacional de Arquivo do Estado ao nível do INTIC, IP;

- b) elaborar e actualizar o Plano de Classificação e Tabela de Temporalidade de Documentos das Actividades – fim e do Classificador de Informação Classificada do INTIC, IP;
- c) coordenar as actividades da Comissão de Avaliação de Documentos (CAD) do INTIC, IP;
- d) assegurar a capacitação técnica dos membros da CAD e demais funcionários e agentes do Estado do INTIC, IP em matérias de gestão de documentos e arquivos;
- e) coordenar a organização, avaliação regular dos arquivos correntes das unidades orgânicas da instituição;
- f) organizar e gerir o Arquivo Intermediário do INTIC, IP ;
- g) implementar as normas que regulam o acesso e manuseamento de informação classificada;
- h) elaborar o plano de gestão de desastres de arquivos; e
- i) promover a gestão electrónica de documentos e arquivos na instituição (Moçambique, 2022b).

Observando as funções dos dois departamentos acima, fica implícito que, aparentemente, as valências do departamento responsável pela gestão de documentos não são capitalizadas para a proteção de dados pessoais.

7.2.3 Instituto Nacional de Governo Electrónico (INAGE)

O Instituto Nacional de Governo Electrónico (INAGE) foi criado pelo Decreto nº 61/2017, 6 de novembro, dada a “necessidade de criar uma entidade de prestação de serviços de Governo Electrónico” (Moçambique, 2017d). Conforme o Artigo 1º deste dispositivo, o INAGE é uma instituição pública dotada de personalidade jurídica e autonomia administrativa. O Diploma Ministerial nº 93/2018, 2 de novembro, aprova o Regulamento Interno do Instituto Nacional de Governo Electrónico. Contudo suas atribuições, competências e demais aspectos são ajustados pelo Decreto nº 35/2022, de 22 de julho., que igualmente revoga o Decreto nº 61/2017, de 6 de novembro, com excepção do Artigo 1º que cria o INAGE.

Assim, o INAGE à luz do Artigo 1º deste novo dispositivo, é “[instituto público] uma pessoa colectiva de direito público, de categoria A, responsável pela coordenação e prestação de serviços de Governo Electrónico, dotada de personalidade jurídica, autonomia administrativa, financeira e patrimonial” (Moçambique, 2022c).

O mais recente instrumento legal concernente ao INAGE é a Resolução nº 6/2024, de 6 de maio que aprova o seu estatuto orgânico. O Artigo 3º deste instrumento aponta que o INAGE, IP, é tutelado pelo dirigente que superintende a área

de Tecnologias de Informação e Comunicação (TIC) e, financeiramente, pelo Ministro que superintende a área das Finanças.

O Artigo 4º define as atribuições do INAGE, que são, dentre outras:

- a) prestação de serviços de assistência técnica, consultoria, formação, aconselhamento e outros serviços conexos no domínio das TIC, inovação tecnológica e transformação digital;
- d) elaboração e implementação de soluções tecnológicas transversais para a Administração Pública e para a prestação de serviços de Governo Electrónico;
- f) gestão da plataforma comum de comunicação de dados e de interoperabilidade, de alto débito, fiável, segura e eficiente;
- g) implementação e gestão de soluções de Computação em Nuvem do Governo de Moçambique;
- h) elaboração de propostas de políticas, estratégias e normas que garantam o funcionamento e a segurança das infra-estruturas, aplicações e serviços de Governo Electrónico;
- i) condução de processos de inovação e modernização do Estado, com recurso às TIC, no âmbito da Reforma da Administração Pública;
- j) implementação e gestão dos Centros de Dados do Governo e os respectivos serviços;
- k) criação de capacidade no domínio das TIC a nível nacional e a transferência de conhecimento necessário para a implementação de soluções e serviços de TIC na Função Pública;
- m) mobilização de recursos financeiros, materiais e humanos necessários à materialização da Política para a Sociedade de Informação e dos respectivos Planos Estratégico e Operacional (Moçambique, 2024b).

Os órgãos do INAGE são: o Conselho de Direcção; o Conselho Consultivo; o Conselho Técnico para a Transformação Digital (GovDigital); e, o Conselho Fiscal., de acordo com o Artigo 6º. E a sua estrutura compreende, de acordo com o Artigo 14º: a Divisão de Transformação Digital; a Divisão de Segurança Cibernética; a Divisão de Recursos Partilhados; a Divisão da Rede de Ensino e Investigação; o Gabinete Jurídico; o Gabinete de Gestão de Negócio; o Gabinete de Comunicação e Imagem; o Departamento de Planificação e Cooperação; o Departamento de Administração e Finanças; o Departamento de Recursos Humanos; e, o Departamento de Aquisições.

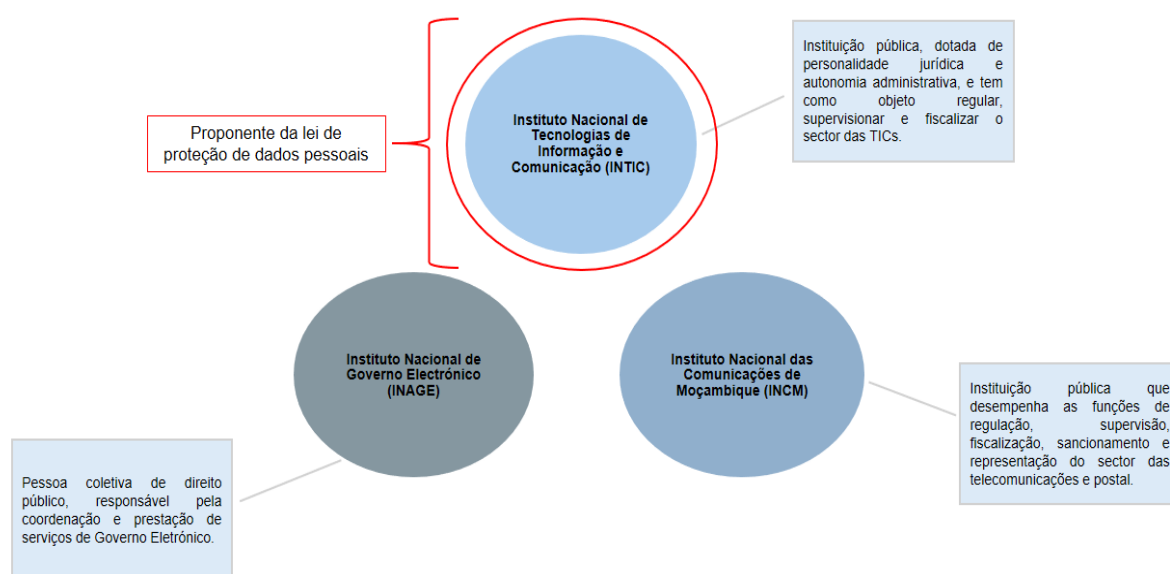
A Divisão de Segurança Cibernética tem suas funções estabelecidas no Artigo 16º. Dentre estas funções destacamos:

Implementar normas e criar capacidade de prevenção e resposta a incidentes de segurança cibernética na Administração Pública; estabelecer um Comité de Segurança Cibernética na Administração Pública; desenvolver acções de formação e sensibilização, com vista a criar uma cultura de segurança cibernética na Administração Pública; propor o quadro legal de segurança de informação; estabelecer mecanismos e sistemas de protecção e segurança de dados nos Centros de Dados do Governo e na Rede Electrónica do Governo; gerir e configurar os equipamentos de Segurança dos Centros de

Dados do Governo e da Rede Electrónica do Governo; propor o Plano de Continuidade de Negócios, Plano de Recuperação em caso de Desastre e Plano de Gestão de Crises nos Centros de Dados do Governo e na Rede Electrónica do Governo; desenvolver e implementar programas que permitam o uso das redes sociais na Internet pela Administração Pública, maximizando os benefícios e minimizando os riscos; implementar e assegurar o cumprimento da legislação estabelecida no âmbito da segurança cibernética; implementar e gerir a infra-estrutura e serviços de certificação digital do Governo, no âmbito do Sistema de Certificação Digital de Moçambique; emitir certificados e assinaturas digitais, identificadores da qualidade de titular de alto cargo do Estado; cooperar com outros organismos nacionais e internacionais especializados em segurança cibernética, para a colaboração e melhoria na eficácia da prevenção, detecção e mitigação de incidentes de segurança (Moçambique, 2024).

Diante do exposto, parece-nos oportunos representar, na figura 8, estas principais instituições e sua relação no campo da proteção de dados pessoais.

Figura 8 - Principais entidades na proteção de dados pessoais em Moçambique



Fonte: Elaborado pela autora.

Tomando a apresentação e análise da legislação moçambicana de proteção de dados pessoais feita nesta seção, e junto das anteriores seções, passamos a seguinte seção, na qual é analisada a versão de 2024 da Proposta de Lei de Proteção de Dados Pessoais, do INTIC, consultada aos 20 de abril de 2025. Esta análise é feita atentos aos preceitos arquivísticos. Para além da referida análise, são propostas diretrizes para elaboração de uma normativa de proteção de dados pessoais que coadune com a gestão arquivística.

8 PELA PROTEÇÃO DE DADOS PESSOAIS CONSENTÂNEA COM POLÍTICA ARQUIVÍSTICA EM MOÇAMBIQUE

Nesta seção é analisada, numa perspectiva arquivística, a Proposta de Lei de Proteção de Dados Pessoais (Instituto Nacional de Tecnologias de Informação e Comunicação - INTIC, 2024). A Proposta aqui analisada é a datada de 26 de abril de 2024 e foi consultada aos 20 de abril de 2025. Na sequência, são apresentadas diretrizes para a elaboração de normativas de proteção de dados pessoais consentâneas com a gestão de documentos. Essas diretrizes são colocadas em três dimensões que se entrelaçam, a saber: elaboração e formalização de política arquivística nacional, revisão do sistema nacional de arquivos e institucionalização da gestão de documentos.

8.1 A Proposta de Lei de Proteção de Dados Pessoais sob a lupa arquivística

Os países têm adotado diferentes modelos jurídicos para a proteção de dados pessoais. Um dos modelos consiste numa proteção constitucional, por meio da garantia de um direito fundamental e por meio de um regime legal de proteção de dados, na forma de uma lei geral. Moçambique parece estar a dar passos para a adoção desse modelo, na medida em que a Constituição da República já avança os fundamentos da proteção de dados pessoais e desde 2024, com mais vigor, o INTIC está prepara uma proposta de lei de proteção de dados pessoais.

Aqui fazemos uma análise à essa proposta (ver Anexo A) apresentada pelo INTIC buscando olhar para os aspectos arquivísticos presentes e/ou ausentes nela. De modo geral, ao todo a proposta apresenta 12 capítulos e 64 artigos que se distribuem em 37 páginas da Proposta de Lei de Protecção de Dados Pessoais. Antes de prosseguirmos, é oportuno fazer um apontamento sobre a variação da forma de apresentação ou grafia dos artigos na legislação moçambicana.

Constatamos, ao analisar as normativas arquivísticas bem como aquelas inerentes especificamente a proteção de dados pessoais, que há uma regular variação. Nem sempre os primeiros nove artigos são apresentados de forma ordinal e

por vezes mesmo os artigos acima desde número são apresentados de forma ordinal. São exemplos os artigos 48º e 249º da CRM e o artigo 5 da Lei do Direito à Informação citados mais acima. Esta situação em muito contrasta com o que pode ser observado no Brasil. Portanto este cenário pode ser visto na proposta que passamos a analisar.

O texto da proposta apresenta repetições e, em alguns casos, omissões incluindo artigos sem conteúdo (texto) entre outros erros de digitação e/ou revisão. Neste sentido, ao analisarmos algumas disposições colocadas na proposta, fizemos referência *ipsis litteris* conforme encontrada e extraída. Ademais, o texto encontra-se em português de Moçambique, mais semelhante ao português de Portugal, pelo que, a sua redação não corresponde, em várias ocorrências, ao português escrito e falado no Brasil.

Na proposta de Capítulo I (Disposições Gerais), o artigo 1 apresenta o objeto da lei segundo o qual é estabelecer o “Art. 1, regime jurídico aplicável ao tratamento e à livre circulação de dados pessoais nos meios físicos e digitais, que visa garantir o respeito pelas liberdades públicas e os direitos fundamentais das pessoas singulares” (INTIC, 2024). Portanto, prevê-se, embora não esteja colocado de forma explícita, que serão objeto desta lei não apenas documentos em ambientes eletrônicos como também, e antes de mais, os documentos de arquivo ditos tradicionais, ou impressos, ou ainda analógicos.

A sua aplicação é apontada no artigo 2, prevendo-se aplicar

- Art. 2, 1.a) a qualquer recolha, processamento, armazenamento ou utilização de dados pessoais realizados no território nacional, por uma pessoa singular, independentemente da natureza pública ou privada do responsável pelo tratamento;
- b) qualquer processamento automatizado ou não de dados contidos ou que devem figurar num ficheiro;
- c) aos dados processados nas embaixadas e consulados de que sejam titulares Moçambicanos residentes no estrangeiro (INTIC, 2024)

Esta aplicação alinha-se ao princípio de territorialidade, conforme vimos, os documentos de um território, seguem o destino desse território, e pode ser aplicado em nível nacional, regional e/ou institucional. Portanto, a Proposta de Lei de Protecção de Dados Pessoais, coloca no centro do tratamento dos dados pessoais, o nível nacional, mesmo que geograficamente distinto da latitude e longitude que encerra o país Moçambique.

A proposta de aplicação colocada na linha a) do nº 1, causa-nos estranheza por não estarem contempladas a recolha, processamento, armazenamento ou utilização de dados pessoais realizados por pessoas jurídicas de direito público ou privado. Em geral, as alíneas do nº 1 deste artigo parecem apresentar uma linguagem não muito clara, todavia, percebe-se através da proposta que se prevê que a lei abranja, uma vez aprovada, todo o ciclo de vida de dados e de documentos, que incluem o processamento automatizado ou não por uma entidade pública ou privada, como também a abrangência de ciclo não só dentro das fronteiras de Moçambique, como também nas representações diplomáticas.

Achamos oportuno relembrar as palavras de Cuesta (2012) ao considerar os arquivos como grandes depósitos ou arquivos de dados pessoais e, portanto, sujeitos à legislação de proteção de dados. E por essa razão vê um peso importante dos arquivos como agentes na proteção de dados pessoais.

Ora, a lei não se aplicará

- 2.a) ao processamento de dados feitos por uma pessoa singular no quadro exclusivo das suas actividades pessoais ou domésticas, desde que esses dados não sejam destinados a uma comunicação sistemática a terceiros ou a difusão;
- b) as cópias temporárias feitas no quadro das actividades técnicas de transmissão e acesso a uma rede digital, com o objectivo de armazenamento automático, intermédio e temporário de dados, tendo como finalidade exclusiva permitir aos destinatários do serviço o melhor acesso possível as informações enviadas;
- c) processamento, recolha ou divulgação electrónica de dados pessoais para efeitos de jornalismo, expressão artística, literária ou quando decidido pelas autoridades competentes para a salvaguarda da segurança pública e defesa nacional;
- d) processamento de dados em que o fornecimento da informação ao titular seja impossível, envolva um esforço desproporcional, o seu registo ou divulgação seja permitido por lei e, ainda, nos casos de registo de dados para efeitos estatísticos históricos ou científicos.
- e) redes e sistemas de informação directamente relacionados com o comando e controlo das entidades que superintendem as áreas de Defesa e Segurança;
- f) redes e sistemas de informação que processem informação classificada conforme a legislação específica (INTIC, 2024)

As alíneas do nº 2, à semelhança do número anterior, têm uma linguagem não clara que dificultará, supomos, o entendimento de quem deverá implementar a lei bem como do cidadão comum que se apoiará na lei para ver salvaguardados os seus direitos.

Atinente ao Artigo 3 sobre as definições, através do texto da proposta não pudemos apreciar o glossário pois este não era parte integrante.

A proposta de capítulo II (Princípios de Base que regem o Processamento de Dados Pessoais) é apresentar, através do Artigo 4, aqueles que constituirão os princípios da lei a ser aprovada. São eles, conforme a proposta: a) Princípio do Consentimento é considerado legítimo quando o titular dos dados der o seu consentimento. Ora, para que haja a possibilidade de se dar o consentimento, o titular deve ser informado sobre a coleta e tratamento de dados; b) Princípio de Legalidade é a recolha, o registo, o processamento, o armazenamento e a transmissão de dados pessoais devem ser feitos de uma forma lícita, justa e não fraudulenta (INTIC, 2024); c) Princípio da finalidade é a realização de tratamento para propósitos legítimos específicos, explícitos e informados ao titular sem possibilidade de tratamento posterior de forma incompatível com esses fins; d) Princípio de exactidão. Os dados pessoais, devem ser exactos actualizados, tendo em conta os fins para os quais foram recolhidos e posteriormente processados (INTIC, 2024);

e) Princípio de transparência o tratamento de dados pessoais deve ser processado de forma transparente, em estrito respeito pelo princípio de reserva da vida privada, bem como pelos direitos, liberdades e garantias públicas fundamentais previstos na constituição da República de Moçambique e na presente lei (INTIC, 2024)

É preciso lembrar que o princípio de transparência é intimamente ligado ao direito à informação e ao exercício de acesso. Esse direito ele é usufruído quando a pessoa coletiva, tem a gestão de documentos institucionalizada, o que facilita a resposta pontual às demandas. Assim, ao se orientar por este princípio depreende-se que, através da lei que for aprovada, os cidadãos titulares de dados deverão saber que tratamento é feito de seus dados, por exemplo. E os cidadãos não necessariamente titulares de dados objeto de tratamento, deverão saber, por exemplo, que incidentes de proteção de dados pessoais ocorreram com as pessoas coletivas.

O princípio a seguir é a outra face da mesma moeda do princípio anterior. Com o processo de gestão de documentos estabelecido em uma instituição, quer sejam estes documentos digitais ou em moldes ditos tradicionais, os aspectos de confidencialidade e segurança estarão serão observados desde a primeira etapa da primeira fase da gestão de documentos, ou seja, desde a elaboração ou

recebimento dos documentos contendo dados pessoais em ambiente eletrônico ou analógico.

f) Princípio de Confidencialidade e de Segurança os dados pessoais devem ser processados num ambiente confidencial e serem protegidos, principalmente quando o processamento envolve transmissão de dados através de uma rede (INTIC, 2024)

Um dos aspectos interessantes na produção documental é a avaliação da necessidade da própria produção. Mesmo que os documentos de arquivo sejam produzidos para o cumprimento das atividades das pessoas, esse fim para os quais são produzidos devem estar alinhados com a produção. Na Proposta de Lei a alínea g) carrega este espírito da gestão de documentos. Lê-se nela “g) Princípio da proporcionalidade os dados Pessoais sujeitos a tratamentos devem ser pertinentes, adequados e não excessivos relativamente à finalidade que legitimaram a sua recolha e tratamento.” (INTIC, 2024).

h) Princípio da duração do período de conservação os dados pessoais devem ser conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário a prossecução das finalidades que originaram a sua recolha ou tratamento, devendo ser posteriormente eliminados ou tornados anónimos. A conservação de dados pessoais para fins históricos, estatísticos, de investigação criminal e segurança nacional pode ser autorizada pela Agência Nacional de Protecção de Dados por período superior mediante requerimento do responsável pelo tratamento (INTIC, 2024)

Sobre o princípio disposto na alínea h), importa recuperar o pensamento de Beckles (2014), segundo o qual os documentos que contêm dados pessoais não devem ser mantidos por mais tempo do que o necessário. Isso significa que, desde o início, a gestão de documentos, em conjunto com os setores ou serviços em que são produzidos estes documentos, deve determinar por quanto tempo um documento com dados pessoais deve ser mantido no sistema com base no objetivo e na intenção declarados do documento. “Se os documentos forem de arquivo para a organização e forem retidos para fins de pesquisa, outras medidas deverão ser tomadas para proteger os dados pessoais contidos neles” (Beckles, 2014, p. 243). Na proposta de lei podem ser notadas, mais abaixo, medidas de anonimização e de pseudominização para proteger os dados pessoais.

Na gestão de documentos, os procedimentos e operações técnicas são realizados sempre com o alicerce legal e ético. O Arquivista deve ser conhecedor exímio das normativas específicas e conexas que orientam o seu trabalho, como as que aprovam o sistema de arquivos, as que regulam o acesso à informação, as que

regulam a proteção de dados pessoais etc. A alínea i) aponta “i) Princípio da legalidade a recolha, o registo, o processamento, o armazenamento e a transmissão de dados pessoais devem ser feitos de uma forma lícita, justa e não fraudulenta.” (INTIC, 2024), sublinhando a postura que o arquivista tem no exercício das suas competências.

No que toca ao “j) Princípio de exactidão os dados recolhidos devem ser exactos e actualizados, tendo em conta os fins para os quais foram recolhidos e posteriormente processados e possam ser apagados ou rectificados.” (INTIC, 2024). Vale reforçar pensar na gestão de documentos como o conjunto de procedimentos e operação que vai proporcionar a fiabilidade, a exatidão e a fidedignidade dos documentos de arquivo, o que por sua vez, propicia a exatidão e a fidedignidade dos dados pessoais contidos nesses documentos.

k) Princípio da transparência o tratamento de dados pessoais deve processar-se de forma transparente, em estrito respeito pelo princípio de reserva da vida privada, bem como pelos direitos, liberdades e garantias públicas fundamentais previstos na constituição da República de Moçambique e na presente lei. Para efeito de disposto no número anterior, os dados pessoais devem ser conservados de forma a permitir o exercício aos seus titulares de acesso, informação, rectificação, cancelamento e oposição, conforme na presente lei (INTIC, 2024)

l) Princípio da licitude o tratamento de dados pessoais deve ser efectuado de forma lícita e leal, com respeito pelo princípio da boa-fé. O tratamento de dados pessoais que conduza a uma discriminação arbitrária e ilícita em relação ao seu titular é considerado ao princípio da boa-fé (INTIC, 2024).

Sobre o princípio estabelecido na alínea m), fizemos o comentário mais acima. Na verdade, esta alínea é uma das repetições de que falamos. “m) Princípio da proporcionalidade os dados Pessoais sujeitos a tratamentos devem ser pertinentes, adequados e não excessivos relativamente à finalidade que legitimaram a sua recolha e tratamento.” (INTIC, 2024).

Na alínea n) “Princípio de livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre integralidade de seus dados pessoais” (INTIC, 2024), compreendemos que não se estabelece, aos titulares de dados, o direito de saber da razão da coleta, o direito de ser informado sobre quais dados estão sendo coletados.

o) Princípio de qualidade de Dados: garantia, aos titulares, de exactidão, clareza, relevância e actualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (INTIC, 2024).

p) Princípio Responsabilidade e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a

observância e o cumprimento das normas de protecção de Dados pessoais e, inclusive, da eficácia dessas medidas (INTIC, 2024)

Antes de avançarmos para outros detalhes, queremos notar que embora seja uma proposta de lei, aqui nos princípios há repetições de que fizemos referência mais acima. É o caso do princípio da legalidade, que ocorre nas alíneas b) e i); o princípio da transparência que ocorre nas alíneas e) e k); nas alíneas g) e m) para o princípio de proporcionalidade; e, o princípio de exactidão está repetido nas alíneas d) e j).

Sobre o princípio da transparência achamos curioso a adoção do termo transparência para os princípios mas para a materialização deste princípio na proposta é utilizado o termo publicidade, como se verá na proposta de Artigo 32. A alínea k) que se apresenta com mais conteúdo, remete aos direitos que em geral são atribuídos aos titulares de dados, conhecidos como ARCO (Acesso, Retificação, Cancelamento e Oposição) apontando a liberdade de acesso aos seus dados que o titular deverá ter, a possibilidade de corrigir dados desatualizados ou equivocados e a possibilidade de cancelar o tratamento de dados que teve o consentimento cancelado ou revogado ou que os dados foram indevidamente armazenados.

A alínea h, que aponta o princípio da duração do período de conservação, merece nossa especial atenção. Pois ao estabelecer que

[...] os dados pessoais devem ser conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário a prossecução das finalidades que originaram a sua recolha ou tratamento, devendo ser posteriormente eliminados ou tornados anónimos. A conservação de dados pessoais para fins históricos, estatísticos, de investigação criminal e segurança nacional pode ser autorizada pela Agência Nacional de Protecção de Dados por período superior mediante requerimento do responsável pelo tratamento (INTIC, 2024).

Este princípio faz alusão ao processo de gestão de documentos, incluindo seus instrumentos, com particular referência à tabela de temporalidade de documentos, bem como o processo de avaliação e seleção. Conseguimos inferir deste princípio, as fases da gestão documental, o ciclo de vida dos documentos e a teoria das três idades.

Achamos que pode ser interessante, observarmos aqui, o possível alinhamento entre os princípios que estão sendo propostos no documento que estamos a apreciar, diante dos princípios avançados pelo RGPD bem como pela LGPD, atendendo que estes são instrumentos que, mesmo sem declaração oficial, tem inspirado a elaboração de normativas de proteção de dados pessoais em diversos países e Moçambique não constitui exceção.

Quadro 14 – Princípios de tratamento de dados pessoais no RGPD, na LGPD e na Proposta de Lei de Protecção de Dados Pessoais de Moçambique

Princípios de tratamento de dados pessoais no RGPD (Parlamento Europeu, 2016)	Princípios de tratamento de dados pessoais na LGPD (Brasil, 2018)	Princípios de Base que regem o Processamento de Dados Pessoais na Proposta de Lei de Protecção de Dados Pessoais (INTIC, 2024)
Licitude, lealdade e transparência	Transparência; prevenção; não discriminação	Princípio do Consentimento; Princípio de transparência; Princípio da licitude; Princípio de Legalidade
Limitação das finalidades	Finalidade	Princípio da finalidade
Minimização dos dados	Adequação	Princípio da proporcionalidade
Exactidão	Necessidade	Princípio de exactidão
Limitação da conservação	Segurança	Princípio da duração do período de conservação
Integridade e confidencialidade	Qualidade dos dados	Princípio de Confidencialidade e de Segurança; Princípio de qualidade de Dados
Nada consta	Livre acesso	Princípio de livre acesso
Nada consta	Responsabilização e prestação de contas	Princípio Responsabilidade e prestação de contas

Fonte: Elaborado pela autora.

O quadro revela que a proposta moçambicana tem um número de princípios muito maior que as normativas europeia e da brasileira. Parece-nos que ocorre bastante sinónimos e que são tomados, pelo menos na versão da proposta que estamos a analisar, como princípio distintos.

Ora, observando os princípios que a proposta de lei avança (ignorando suas repetições), infere-se que os documentos contendo dados pessoais deverão ser processados de forma justa, garantindo de que todos os direitos e deveres que envolvem os diferentes atores na coleta e tratamento de dados estarão salvaguardados. Ademais, parece pontual citar Beckles (2014) que estando atenda aos princípios gerais que regem a protecção de dados pessoais no mundo, entende que eles visam garantir medidas de segurança na manutenção de dados pessoais e por esta razão, devem ser considerados os dados pessoais acessados remotamente por meio de aparelhos como smartphones, tablets, laptops etc. A autora ainda acrescenta que a criptografia desses dados seria uma medida útil para protegê-los em caso de furto ou roubo. Com estas palavras de Beckles, chamamos a atenção a ausência, na proposta de lei que estamos a analisar, de mecanismos de criptografia com vista a reforçar a segurança.

Na proposta de capítulo III sobre Autoridade Nacional de Protecção de Dados, são propostos os artigos sobre a sua natureza, composição e competências. Assim o Artigo 5 (Natureza);

1. A Autoridade Nacional de Protecção de Dados é um órgão de Aparente do Estado, independente dotada de autonomia administrativa, financeira e patrimonial e com poderes de autoridade.
2. A Autoridade Nacional de Protecção de Dados controla e fiscaliza o cumprimento da presente Lei, bem como das demais disposições legais e regulamentares em matéria de protecção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais.
3. A Autoridade Nacional de Protecção de Dados age com independência na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos pela presente lei.
4. Os membros de uma Autoridade Nacional de Protecção de Dados não devem ser membros do Governo, nem pessoas que exercem funções executivas e possuem acções em empresas no sector de Tecnologias de Informação; não podendo, durante o seu mandato, desempenhar outra actividade, remunerada ou não, com excepção da actividade de docência no ensino superior e de investigação (INTIC, 2024).

Conforme a proposta no seu Artigo 6, a composição dessa autoridade será:

- a) três cidadãos designados pelo Presidente da República, dos quais nomeia o Presidente da Autoridade;
 - b) três cidadãos eleitos pela Assembleia da República;
 - c) dois magistrados, sendo um magistrado judicial, designado pelo Conselho Superior da Magistratura, e um magistrado do Ministério Público, designado pelo Conselho Superior do Ministério Público.
1. O mandato dos membros da ANPD é de cinco anos, renovável duas vezes, e cessa com posse dos novos membros.
 2. A designação dos membros da ANPD consta de lista publicada no Boletim da República.
 3. Os membros da ANPD tomam posse perante o Presidente da República nos 10 dias seguintes à publicação da lista referida no número anterior. (INTIC, 2024)

Porque através desta proposta não é possível visualizar quais seriam os critérios para a designação dos cidadãos pelo Presidente da República e nem mesmo para a eleição destes pela Assembleia da República, resta-nos indagar sobre os termos de referência para tais atos. Questionamos qual é o perfil de cidadão que se antevê. Não nos parece que se inclui aqui alguém que tenha competências em determinada área e, se se pensa em algum profissional, nos parece razoável que houvesse menção explícita. Estamos ao mesmo tempo apontando a nossa preocupação pela inexistência de um profissional de informação, concretamente arquivista, na composição dessa entidade.

São apontadas como competências desta Autoridade, “Art. 7, a) zelar pela protecção de dados pessoais nos termos da legislação aplicável” (INTIC, 2024), isto

implica zelar, não apenas a proposta que estamos apreciar, eventualmente quando já aprovada, mas também uma série de normativas arquivísticas e conexas de que Moçambique dispõe.

A alínea “Art. 7, b) elaborar diretrizes para Política Nacional de Protecção de Dados Pessoais e da Privacidade” (INTIC, 2024), parece nos revelar uma vez mais que em Moçambique, a regra é a criação de leis para posterior elaboração de políticas, significando que neste país as políticas não precedem as leis. Aliás, o cenário arquivístico moçambicano é o grande exemplo que temos estado a apontar com a realização desta tese.

- c) fiscalizar, auditar e aplicar sanções em caso de tratamento de dados realizados em incumprimento da legislação aplicável;
- d) receber reclamações, petições e as queixas relativas ao processamento de dados pessoais e informar os seus actores sobre os resultados inerentes a esta matéria;
- e) Comunicar às autoridades competentes as infracções penais das quais tiver conhecimento (INTIC, 2024);

A alínea “f) autorizar o processamento de ficheiros, em determinados casos, especialmente os ficheiros sensíveis” (INTIC, 2024), remete-nos à atividade classificatória de documentos. Isto significa que para a autorização do processamento desses ficheiros, que são, nada mais e nada menos que documentos de arquivo, deverá haver, para além do consentimento do titular dos dados, a análise da sensibilidade desses dados e sua classificação para maior reforço de segurança e atenção à temporalidade.

- g) promover o conhecimento dos instrumentos normativos e da cultura da protecção de dados pessoais e das medidas de segurança;
- h) promover e elaborar os estudos sobre as práticas Nacionais e Internacionais de protecção de dados pessoais e privacidade (INTIC, 2024)

Sobre a alínea “i) dispor sobre as formas de publicidade das operações de tratamento de dados pessoais respeitados os segredos comerciais industriais” (INTIC, 2024) importa lembrar que, ao se evocar a publicidade das operações de tratamento de dados pessoais, a proposta está fazendo alusão ao direito à informação, mais concretamente ao direito de ser informado, sobretudo o titular dos dados objeto de tratamento. Mas também chamamos a atenção para que tal Autoridade adote formas de publicidade mais abrangentes, visto que a ideia de publicidade, atrelada à transparência, obriga esta entidade a tornar de conhecimento público desde a existência de um banco de dados com dados pessoais e as operações realizadas.

- j) realizar auditorias ou determinar a sua realização no âmbito da actividade de fiscalização de que trata o artigo
- k) receber as formalidades prévias para o processamento de dados pessoais (INTIC, 2024);

Competirá igualmente à essa Autoridade, “l) autorizar a transferência transfronteiriça de dados pessoais” (INTIC, 2024). Esta operação de transferência é detalhada mais abaixo.

- m) Arrecadar e aplicar suas receitas e publicar no relatório de actividades
- n) Estabelecer mecanismos de cooperação com as autoridades de protecção de dados pessoais;
- o) Participar em negociações internacionais em matéria de protecção de dados pessoais;
- p) Informar de imediato, a autoridade judiciária sobre determinados tipos de infrações de que tiver conhecimento (INTIC, 2024)

a semelhança da alínea i), esperamos que a competência plasmada na alínea “q) elaborar relatórios anuais de actividades” (INTIC, 2024), seja cumprida dentro do espírito de informação de interesse público.

O Capítulo IV é proposto para avançar aspectos à volta dos Encarregados de Protecção de Dados. Na proposta de Artigo 8 (Encarregados de Protecção de Dados), está definido que:

- Art. 8, 1. O encarregado de protecção de dados é a pessoa indicada pelo controlador e operador para actuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Protecção de Dados (ANPD).
2. O encarregado de protecção de dados é designado com base nos requisitos previstos na presente Lei, não carecendo de certificação profissional para efeito.
- Independentemente da natureza da sua relação jurídica, o encarregado de protecção de dados exerce a sua função com autonomia técnica perante a entidade responsável pelo tratamento ou subcontratante.
- a) O controlador deve indicar encarregado pelo tratamento de dados pessoais;
 - b) A identidade e as informações de contacto de encarregado devem ser divulgadas publicamente, de forma clara e objectiva, preferencialmente no sítio electrónico do controlador;
3. Aceitar as actividades de controlador do encarregado consiste em:
- a) aceitar reclamação e comunicações dos titulares, prestar esclarecimento e adoptar providencias;
 - b) orientar os funcionários e os controladores da entidade a respeito das práticas a serem tomadas em relação a protecção de dados pessoais; e
 - c) Executar as demais atribuições determinadas pelo controlador (INTIC, 2024)

Atentos ao nº 2 do Artigo 8, entendemos ser preciso recordar que Beckles (2014) chamou atenção para que os documentos com dados pessoais nunca sejam deixados sem supervisão em qualquer formato (papel/impreso ou digital) e que o

peçoal que trabalha com esses documentos deve ser cuidadosamente selecionado, com seus contratos de confidencialidade assinados como uma medida adicional.

Na proposta de Artigo 9 é avançado o Dever de sigilo e confidencialidade do encarregado de protecção de dados pessoais. Assim,

Art. 9, O encarregado de protecção de dados está obrigado a um dever de sigilo profissional em tudo o que diga respeito ao exercício dessas funções, que se mantém após o termo das funções que lhes deram origem (INTIC, 2024).

O encarregado de protecção de dados, bem como os responsáveis pelo tratamento de dados, incluindo os subcontratantes, e todas as pessoas que intervenham em qualquer operação, de tratamento de dados, estão obrigados a um dever de confidencialidade que acresce aos deveres de sigilo profissional previsto na lei (INTIC, 2024).

Para além do dever de sigilo e confidencialidade do encarregado de protecção de dados pessoais, este terá, conforme o Artigo 10 (Funções do encarregado de protecção de dados), as seguintes funções:

Art. 10, 1. São funções do encarregado de protecção de dados:

- a) Assegurar a realização de auditorias, quer periódicas, quer não programadas;
- b) Sensibilizar os utilizadores para a importância da detecção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança;
- c) Assegurar as relações com os titulares dos dados nas matérias abrangidas pela legislação nacional em matéria de protecção de dados.

A proposta de lei em apreciação prevê a existência de encarregados de protecção de dados pessoais em entidades públicas assim como em entidades privadas. Na proposta de Artigo 11 (Encarregados de protecção de dados em entidades públicas), aponta que

1. É obrigatória a designação de encarregados de protecção de dados nas entidades públicas, de acordo com o disposto nos números seguintes.

2. Para efeitos do número anterior, entende-se por entidades públicas:

- a) O Estado;
- b) As regiões autónomas;
- c) As autarquias locais e as entidades supranacionais previstas na lei;
- d) As entidades administrativas independentes e o Banco de Moçambique;
- e) Os institutos públicos;
- f) As instituições de ensino superior públicas, independentemente da sua natureza;
- g) As empresas do sector empresarial do Estado e dos sectores empresariais regionais e locais;
- h) As associações públicas.

3. Independentemente de quem seja responsável pelo tratamento, existe pelo menos um encarregado de protecção de dados:

- a) Por cada ministério ou área governativa, no caso do Estado, sendo designado pelo respectivo ministro, com faculdade de delegação em qualquer secretário de Estado que o coadjuvar;

- b) Por cada secretaria regional, no caso das regiões autónomas, sendo designado pelo respectivo secretário regional, com faculdade de delegação em dirigente superior de 1.º grau;
- c) Por cada município, sendo designado pela câmara municipal, com faculdade de delegação no presidente e subdelegação em qualquer vereador;
- 4. Por cada entidade, no caso das demais entidades referidas no número anterior, sendo designada pelo respectivo órgão executivo, de administração ou gestão, com faculdade de delegação no respectivo presidente. (INTIC, 2024)

A alínea b) do n° 3 nos chama atenção por parecer se desviar da Constituição da República de Moçambique (CRM) que, até ao momento que estivemos a apreciar a legislação moçambicana, incluindo a CRM e a presente proposta de lei de proteção de dados, nada estava fundamentado na CRM sobre regiões autónomas, mesmo depois da revisão pontual da CRM de 2018.

No que toca ao encarregado de proteção de dados em entidades privadas, a proposta de Artigo 12 (Encarregado de Protecção de Dados Entidades Privadas) dispõe,

- 1. O responsável pelo tratamento e o subcontratante designam um encarregado de protecção de dados sempre que a actividade privada desenvolvida, a título principal, implique:
 - a) operações de tratamento que, devido à sua natureza, âmbito e ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou
 Operações de tratamento em grande escala das categorias especiais de dados nos termos do Artigo 9.º do RGPD, ou de dados pessoais relacionados com condenações penais e contra ordem nacionais nos termos do Artigo 10.º do RGPD (INTIC, 2024).

Ora, um pouco à semelhança do que acabamos de constatar no artigo anterior, através da alínea b) do n° 3, ocorre no n° 1 do Artigo 12, na sua, presumível, alínea b). A proposta de lei de proteção de dados pessoais de Moçambique faz referência à uma normativa na União Europeia (apreciada no capítulo 6 desta tese, PANORAMA INTERNACIONAL E BRASILEIRO DA PROTEÇÃO DE DADOS PESSOAIS), portanto o RGPD. Como já apontamos noutras ocasiões, mostra-se gritante a maneira como Moçambique tem “importado” normativas para o seu ordenamento.

A proposta de Capítulo IV versa sobre Requisitos para o tratamento de dados pessoais. No Artigo 13 (Requisitos Gerais) deste capítulo, o proponente estabelece,

- 1. Salvo disposição legal em contrário, o tratamento de dados pessoais só pode ser efectuada verificadas as seguintes circunstâncias:
 - a) Consentimento inequívoco e expresso do seu titular;
 - b) Pela notificação da Autoridade Nacional de Protecção de Dados
- 2. Sem prejuízo do direito à informação, o consentimento do titular dos dados é dispensável quando o tratamento for necessário para:

- a) cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito;
- b) protecção de interesses vitais do titular dos dados, pelo seu representante legal se aquele estiver física ou legalmente incapaz de dar o seu consentimento;
- c) execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;
- d) prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados.
- e) execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração negocial efectuadas a seu pedido;
- f) Para a realização de estudos por órgãos competentes garantida, sempre que possível, a anonimização dos dados pessoais (INTIC, 2024);

Na proposta de Artigo 14, são apontados os “Requisitos de tratamento de dados sensíveis saúde e da vida sexual”. Neste contexto, estabelece-se que

1. É proibido o tratamento de dados pessoais que revelam origem racial, étnica, filiação, ideológica, políticas, crenças religiosas ou convicções filosóficas, filiação em associação política ou sindical, vida sexual, informação genética ou, de uma forma geral, as informações relativas ao estado de saúde do titular dos dados.
2. A proibição estabelecida no número 1 do presente artigo, não se aplica para as categorias de processamento que se seguem, quando:
 - a) o tratamento dos dados a serem efectuados com o consentimento inequívoco, expresso e escrito do seu titular ou do seu representante legal;
 - b) o processamento for necessário para o cumprimento de uma obrigação legal ou regulamentar ao qual o sujeito titular dos dados está vinculado;
 - c) Autorização da Agência Nacional de Protecção de Dados Pessoas quando for por motivo de interesse público.
 - d) O processamento de dados pessoais for necessário para proteger os interesses vitais do titular dos dados ou de uma outra pessoa, se o sujeito titular dos dados estiver física ou juridicamente incapacitado para dar o seu consentimento.
 - e) um processo judicial ou uma investigação penal tiver sido iniciado;
 - f) o processamento for necessário no interesse público, especialmente para fins históricos, artísticos, estatísticos, científicos, jornalísticos e de investigação;
 - g) o processamento de dados for necessário para execução de uma missão no interesse público;
 - h) O tratamento dos dados referente a saúde e a vida sexual incluindo os dados genéticos pode ser efectuados quando for necessário para fins de medicina preventiva, de diagnósticos médicos de tratamentos médicos que seja efectuado por um profissional de saúde sujeito a segredo profissional (INTIC, 2024);

Aspectos sobre Dados de Crianças e Adolescentes são propostos no Artigo 15.

No nº 1 deste artigo, é apontado

1. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

2. O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
3. No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados colectados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o artigo 18 desta Lei.
4. Poderão ser colectados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a colecta for necessária para contactar os pais ou o responsável legal, utilizada uma única vez e sem armazenamento, ou para sua protecção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
5. Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras actividades ao fornecimento de informações pessoais além das estritamente necessárias à actividade.
6. O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
7. As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (INTIC, 2024).

Atendendo que apreciamos, antes desta análise à proposta de lei de protecção de dados pessoais de Moçambique, a legislação internacional e do Brasil atinente a protecção de dados pessoais, conseguimos dizer aqui que o Artigo 15 proposto tem o texto extraído de uma normativa estrangeira à Moçambique e, infelizmente, sem nenhuma adequação e/ou enquadramento. Este ato é notório desde logo pela referenciação que se faz aos parágrafos utilizando o símbolo “§” e a enumeração ordinal e não cardinal que é usuária em Moçambique.

O artigo que vemos a seguir, tem o texto bastante confuso. Nele, Artigo 16, está disposto sobre o “Tratamento para fins de interesse público” onde se pode ler “O tratamento para fins de tratamento interesse pública deve respeitar o princípio da minimização dos dados e incluir a anonimização ou a pseudonomização dos mesmos sempre que os visados possam ser atingidos por uma destas vias”. Considerando a sua redação precária, inferimos que a proposta de lei avança prevendo a aplicação de técnicas para ocultar os dados pessoais dos titulares quando os documentos ou informações, de modo geral, forem tratados para atender o interesse público.

Os Requisitos específicos para o tratamento de dados relativos a actividades ilícitas, crimes e contravenções são apontados na proposta de Artigo 17. Segundo esta proposta,

1. O tratamento de dados pessoais relativos a pessoas suspeitas de actividades ilícitas, infracções penais, contravenções e de aplicação de penas, medidas de segurança, multas e sanções acessórias, os quais são considerados dados sensíveis, só pode ser efectuado por autoridade pública, verificadas as seguintes circunstâncias:

a) disposição legal que permita tal tratamento por autoridades com competência específica, em respeito das normas procedimentais e de protecção de dados previstas por lei e mediante prévio parecer da Autoridade de Protecção de Dados; ou

b) Autorização da Autoridade de Protecção de Dados, a qual só pode ser concedida quando tal tratamento for necessário à execução de finalidades legítimas do seu responsável e sejam observadas as normas de protecção de dados e de segurança da informação.

2. Sem prejuízo do disposto em legislação específica, o tratamento de dados pessoais para fins de investigação policial deve limitar-se ao necessário para o cumprimento de finalidades de prevenção geral e especial ou repressão de uma infracção determinada, nos termos da presente lei e de legislação específica (rever) (INTIC, 2024).

Em matéria de requisitos para tratamento de dados pessoais, o Artigo 18, aponta aqueles que serão os Requisitos específicos para o tratamento de dados em sistemas de videovigilância e outros meios de controlo electrónica, estabelecendo que

1. O tratamento de dados pessoais no âmbito da instalação de sistemas de videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas, incluindo os sistemas de vigilância electrónica, está sujeita ao disposto ao Artigo 4.º da presente Lei.

2. O responsável pelo tratamento de dados pessoais deve disponibilizar, nos locais com sistemas de videovigilância, informação relativa à existência dos mesmos, à captação de som e de imagem e o nome do responsável pelo tratamento dos dados, seu endereço, número de telefone e e-mail.

3. As regras aplicáveis à instalação de sistemas de videovigilância e ao tratamento de dados recolhidos neste âmbito são objecto de regulamentação específica.

O capítulo V da proposta em análise, versa sobre os Direitos de Titular dos dados. No Artigo 19 (Direito de informação), são arrolados os direitos do titular, à medida que, concomitantemente, são apontados os deveres do responsável pelo tratamento dos dados pessoais. Na sequência, a proposta de Artigo 20 (Direito de acesso), aponta:

Quadro 15 – Direito de informação e Direito de acesso na Proposta de Lei de Protecção de Dados Pessoais

Artigo 19 (Direito de informação)	Artigo 20 (Direito de acesso)
1. o responsável pelo tratamento deve disponibilizar aos titulares dos dados pelo menos a seguinte informação: a) a identidade e endereço do responsável pelo tratamento; b) as finalidades do tratamento e a criação de um ficheiro com a referida finalidade;	1. O titular dos dados tem o direito de obter do responsável pelo tratamento, livremente, sem restrições, demoras ou custos excessivos, informação sobre se são ou não tratados dados que lhe digam respeito, as finalidades desse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de

c) os destinatários ou categorias de destinatários dos dados; d) o carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências de não responder; e) existência e condições do direito de acesso e de rectificação, actualização, eliminação e oposição; f) as consequências da recolha dos dados sem o consentimento do titular ou, em caso de incapacidade deste, pelo seu representante legal; g) outras informações necessárias para garantir o tratamento lícito de tais dados pessoais.	destinatários a quem são comunicados os dados.
2. Quando os dados pessoais sejam recolhidos directamente do titular dos dados, a informação deve ser prestada no momento da recolha, excepto se já tiver sido prestada em momento prévio.	2. O responsável pelo tratamento deve ainda comunicar ao titular os dados específicos objecto de tratamento, bem como quaisquer informações disponíveis sobre a origem desses dados.
3. Caso os dados pessoais não sejam recolhidos directamente do titular dos dados, o responsável pelo tratamento deve prestar-lhe a informação referida no momento do registo dos dados ou o mais tardar no prazo de trinta dias após a sua recolha, salvo se dele já for conhecida.	3. Sem prejuízo do disposto em legislação específica, no tratamento de dados pessoais relativos à segurança do Estado, à prevenção ou investigação criminal e ao segredo de justiça, o direito de acesso é exercido através da Agência de Protecção de Dados.
4. A informação deve ser prestada de maneira clara, precisa e objectiva em particular quando tenha como destinatários menores e pessoas com necessidades especiais.	4. No tratamento de dados pessoais efectuado para fins exclusivamente jornalísticos, o direito de acesso é exercido pela Agência de Protecção de Dados com salvaguarda das normas constitucionais aplicáveis, designadamente as que garantem a liberdade de expressão e a liberdade de imprensa.
5. A obrigação de informação pode ser dispensada mediante disposição legal ou deliberação da Agência de Protecção de Dados, nos seguintes casos: a) por motivos de segurança do Estado e prevenção ou investigação criminal; b) quando a prestação de informação ao titular dos dados se revelar impossível ou implicar esforços desproporcionados, nomeadamente nos casos de tratamento de dados com finalidades estatísticas, históricas ou de investigação científica; ou c) quando a lei determinar expressamente o registo dos dados ou a sua divulgação.	5. Nos casos previstos nos n 3 e 4, se o acesso aos dados pelo seu titular puder prejudicar a segurança do Estado, a prevenção ou a investigação criminal, o segredo de justiça ou ainda a liberdade de expressão e a liberdade de imprensa, a Agência de Protecção de Dados limita-se a informar o titular dos dados das diligências efectuadas.
6. A obrigação de informação, nos termos do número anterior, não se aplica ao tratamento de dados efectuado para fins exclusivamente jornalísticos ou de expressão artística ou literária.	6. lei pode restringir o direito de acesso verificadas as seguintes circunstâncias: a) os dados não serem utilizados para tomar medidas ou decisões relativamente a pessoas determinadas, mas exclusivamente para fins de investigação científica ou conservados sob forma de dados pessoais durante um período que não exceda o necessário à finalidade exclusiva de elaborar estatísticas; b) não existir qualquer perigo de violação dos direitos, liberdades e garantias fundamentais do titular dos dados pessoais, designadamente do direito à reserva de intimidade da vida privada.
7. No caso de recolha de dados em redes abertas, considera-se prestado o direito de informação através da publicação e disponibilização de políticas de privacidade que sejam de fácil acesso e incluam: a) as informações descritas no nº 1 do	7. O direito de acesso do titular dos dados à informação sobre os dados de saúde e vida sexual, incluindo os dados genéticos, é exercido por intermédio de médico escolhido

presente Artigo; b) a informação de que os seus dados pessoais podem circular na rede sem condições de segurança, correndo o risco de serem vistos e utilizados por terceiros não autorizados.	pelo titular dos dados ou de seu representante legítimo.

Fonte: Adaptado de INTIC (2024).

Sobre os dois artigos apresentados acima, 19 e 20, parece-nos interessante analisá-los sob égide do direito à informação. Depreende-se, ao analisar os dois artigos em alusão, que o direito à informação, como um dos direitos do agrupamento de direitos de proteção de dados pessoais, está presente na proposta de lei de proteção de dados pessoais nas dimensões do direito de ser informado e direito de se informar, embora estas duas dimensões apareçam mescladas nos dois artigos, podemos encontrar uma forte carga do direito de ser informado no Artigo 19 e do direito de se informar no Artigo 20. É igualmente interessante notar que a liberdade de informação não é colocada de forma explícita nestes artigos, embora esteja no seu âmago.

O direito à informação de que falamos, seja na forma de direito de ser informado ou direito de se informar, quer dizer, quando as pessoas coletivas são proativas em prover informação para o cidadão, ou quando as pessoas singulares (os cidadãos) são proativas na busca pela informação, cada um destes cenários dá espaço para o exercício de outros direitos como os de oposição, retificação, atualização, ou mesmo de apagamento ou eliminação. Desta feita, o Artigo 21 versa sobre o “Direito de oposição”, dispondo que

1. O titular dos dados tem o direito de:
 - a) salvo disposição legal em contrário, e pelo menos nas situações referidas acima se opor em qualquer altura a que os dados que lhe digam respeitam sejam objecto de tratamento quando existam razões ponderosas e legítimas relacionadas com a sua situação particular, devendo neste caso o responsável excluir do tratamento tais dados;
 - b) se opor ao tratamento dos seus dados em outras circunstâncias previstas na presente lei e em outra legislação específica (INTIC, 2024)

O Artigo 21 apresenta um dos direitos do conjunto de Direitos à abstenção. Na presente proposta de lei, o direito à oposição é vigente, contudo, o direito de impedir o tratamento de dados sensíveis, não está previsto na proposta em análise.

Alguns Direitos de controle estão previstos na proposta, como o Direito de rectificação, atualização, eliminação (apagamento ou esquecimento) e Direito de bloqueio, como podemos ver a seguir. Ao titular dos dados, é reservado, no Artigo 22, o Direito de rectificação, actualização e eliminação. Assim,

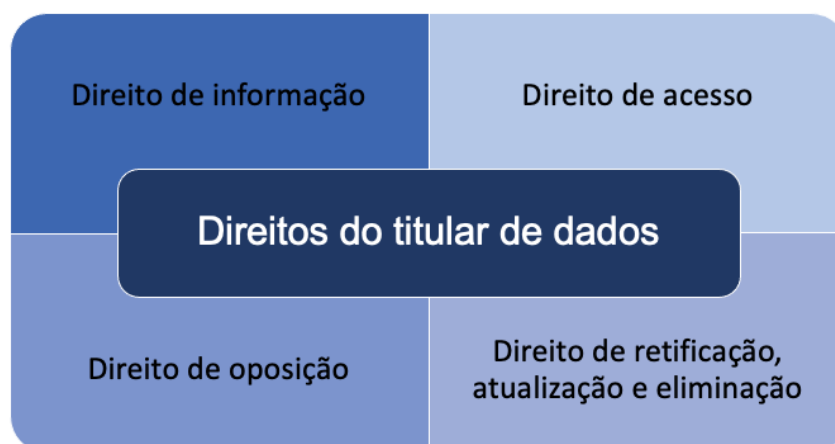
1. É assegurado ao titular dos dados pessoais os direitos de rectificação, actualização ou eliminação dos seus dados pessoais cujo tratamento não cumpra o disposto na presente lei, nomeadamente devido ao carácter incompleto ou inexacto desses dados.
2. O responsável pelo tratamento é obrigado, nos termos da presente lei e legislação especial, a assegurar o direito de rectificação, actualização e eliminação de dados num período de sessenta dias úteis.
3. Se os dados objecto de rectificação, actualização ou eliminação tiverem sido previamente comunicados a destinatário, o responsável pelo tratamento fica obrigado a notificar a este tal rectificação, actualização ou eliminação, salvo se isso for comprovadamente impossível, devendo o destinatário agir em conformidade.
4. No caso previsto no número anterior, o destinatário que tratar os dados para os seus próprios fins ou para fins de um terceiro pode não proceder à eliminação dos dados, devendo neste caso tal destinatário informar o titular dos dados desta situação e confirmar se este pretende também rectificar, actualizar ou eliminar os seus dados dos ficheiros respectivos.
5. O responsável pelo tratamento deve, contudo, bloquear e/ou conservar os dados pessoais nos seguintes casos:
 - a) disposição legal ou ordem de autoridade competente que obrigue o responsável pelo tratamento a bloquear e/ou conservar os dados por um determinado período de tempo;
 - b) se o bloqueamento e/ou conservação dos dados for necessário à prossecução de um interesse legítimo do responsável pelo tratamento, designadamente para o exercício de um direito ou para o cumprimento de obrigações legais;
 - c) se os dados estiverem a ser utilizados para efeitos de investigação criminal;
 - d) se os dados se tratarem de dados relativos ao crédito e à solvabilidade, enquanto a situação creditícia do titular não estiver regularizada (INTIC, 2024).

No que toca aos incapazes, o Artigo 23 (Direito dos incapazes), propõe que “Art. 23, quando os titulares dos dados sejam incapazes, os direitos previstos nos artigos anteriores são exercidos por intermédio dos respectivos representantes legais” (INTIC, 2024). Em outros casos, conforme o Artigo 24 (Direitos do titular dos dados em casos especiais),

Art. 24, Os direitos de informação, de acesso, de rectificação, de apagamento e de limitação do tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, detenção, investigação ou repressão de infracções penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças a segurança pública são exercidos nos termos da lei processual pela, demais legislações aplicáveis e da presente Lei (INTIC, 2024).

De modo geral, os Direitos de Titular dos dados que esta proposta apresenta em seu capítulo V, estão subdivididos em 4 tipos de direitos, que passamos a representar na figura abaixo.

Figura 9 – Direitos do titular dos dados na Proposta de Lei de Protecção de Dados Pessoais



Fonte: Elaborado pela autora

Os artigos que se seguem na proposta de lei, tem enfoque na transferência de dados pessoais. Parece oportuno lembrar aqui do princípio geral das transferências avançado no RGPD, segundo o qual

Qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de protecção das pessoas singulares garantido pelo presente regulamento (Parlamento Europeu, 2016).

A proposta de Artigo 25 sobre Transferência de Dados para Países que assegurem um nível de Protecção adequado, está previsto que

- Art. 25, 1. A transferência internacional de dados para países que assegurem nível de Protecção adequado esta sujeita a notificação à Autoridade Nacional de Protecção de Dados.
2. Entende-se que um país assegura um nível de protecção adequado quando o mesmo garante, no mínimo, um nível de protecção igual ao estabelecimento presente na lei.
3. Cabe à Autoridade Nacional de Protecção de Dados decidir se um estado assegura um nível de protecção adequado, mediante a emissão de parecer a este respeito.
4. A adequação do nível de protecção de dados num Estado é apreciada pela Autoridade Nacional de Protecção de Dados em função de todas as circunstâncias que rodeiam a transferência ou o conjunto de transferência de dados, atendendo em especial à natureza dos dados, à finalidade e à duração do tratamento ou tratamentos projectados, aos países de destino final e às regras de direito, gerais ou sectoriais em vigor no Estado em causa, incluindo

as regras profissionais e as medidas de segurança que são respeitadas nesse Estado. (INTIC, 2024).

Por alguma razão, os Artigo 26 sobre Avaliações prévias de impacto e Artigo 27 sobre Dever de Colaboração não apresentam conteúdo algum. A proposta de Artigo 28 dispõe sobre Transferência de Dados para Países que não asseguram um nível de Protecção Adequado.

Art. 28, 1. A transferência internacional de dados para um país que não assegure um nível de protecção adequado está sujeita a autorização da Autoridade Nacional de Protecção de Dados, a qual só pode ser concedida verificada uma das seguintes circunstâncias constantes de legislação específica:

- a) se o titular de dados tiver dado o seu consentimento inequívoco, expresso e escrito;
 - b) se a transferência internacional de dados decorrer da aplicação de tratados ou acordos internacionais em que a República de Moçambique seja parte;
 - c) se a transferência de dados tiver como finalidade exclusiva a resposta ou pedido de ajuda humanitária;
 - d) se a transferência de dados for necessária para a execução de um contrato entre titulares de dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido titular dos dados;
 - e) se a transferência dos dados for necessária para a execução ou celebração de um contrato do titular dos dados, entre o responsável pelo tratamento e um terceiro;
 - f) se a transferência de dados for necessária ou legalmente exigida para a protecção de um interesse público importante ou para a declaração, o exercício ou a defesa de um direito num processo judicial;
 - g) se a transferência de dados for necessária para proteger os interesses vitais do titular dos dados, ou para a prevenção, ou diagnóstico ou tratamento médico e o titular estiver física ou legalmente incapaz de dar o seu consentimento;
 - h) se a transferência de dados for realizada a partir de uma fonte acessível publicamente;
 - i) se o destinatário dos dados assegurar contratualmente, perante o responsável pelo tratamento, o nível de protecção adequado aos dados transferidos.
2. Incumbe à Autoridade Nacional de Protecção de Dados determinar as condições específicas que devem constar no contrato referido na alínea i) do nº anterior.
3. No caso de transferência internacional de dados entre empresas do mesmo grupo empresarial, a garantia de cumprimento de um nível de protecção adequado pode ser alcançada através da adopção de regras internas relativas à privacidade e protecção de dados cujo cumprimento seja obrigatório (INTIC, 2024).

O capítulo VII dispõe sobre Notificação e autorização. Nesta senda, a Obrigação de Notificação ou de Obtenção de Autorização, está disposto no Artigo 29, nos seguintes termos:

Art. 29, 1. Sem prejuízo do disposto na presente Lei, o tratamento de dados está sujeito a notificação prévia à Autoridade Nacional de Protecção de Dados ou autorização desta.

2. Se for necessária mera notificação, a Autoridade Nacional de Protecção de Dados deve pronunciar-se sobre o pedido do responsável pelo tratamento no prazo de 30 dias após a sua recepção, findo o qual se entende que o tratamento foi devidamente notificado.
3. A Autoridade Nacional de Protecção de Dados pode autorizar a simplificação ou isenção da notificação para determinadas categorias de tratamento que, atendendo a especialidade dos dados, não sejam susceptíveis de por em causa os direitos garantias e liberdades fundamentais dos titulares dos dados e tendo em conta pós créditos de celeridade, economia e eficiência.
4. A autorização de isenção deve, entre outros aspectos, especificar as finalidades do tratamento, os dados ou categorias de dados a tratar a categoria ou categorias de titulares dos dados, os destinatários ou categorias de destinatários a quem podem ser comunicados os dados e o período de conservação dos dados.
5. Estão isentos de notificação os tratamentos cuja única finalidade seja a manutenção de registos que se destinem a informação do público que possam ser consultadas pelo público em geral ou por qualquer pessoa que provar um interesse legítimo.
6. É dispensada a obtenção de autorização da Autoridade Nacional de Protecção de Dados se o tratamento decorrer de diploma legal, bastando neste caso, proceder a mera notificação, salvo se indicado em contrário em legislação específica (INTIC, 2024).

A proposta não apresenta o Artigo 30, contudo supomos que Conteúdo das Notificações e dos Pedido de Autorização refere-se ao artigo em alusão ora, omissos do texto da proposta. Sobre o esse Conteúdo das Notificações e dos Pedido de Autorização, a proposta estabelece que

As notificações e pedidos de autorização remetidos à Autoridade Nacional de Protecção de Dados devem conter as seguintes informações:

- a) o nome e endereço do responsável pelo tratamento e, se for o caso, do seu representante;
- b) finalidade do tratamento;
- c) a descrição da ou das categorias de titulares dos dados ou categorias de dados pessoais que lhes respeitem;
- d) destinatários ou categorias de destinatários a quem os dados podem ser comunicados e em que condições;
- e) entidade encarregada do processamento da informação, se não for o próprio responsável do tratamento;
- f) eventuais interconexões de tratamento de dados pessoais;
- g) tempo de conservação dos dados pessoais;
- h) forma e condições como os titulares dos dados podem exercer seus direitos;
- i) transferências de dados previstas para países terceiros;
- j) descrição geral que permita avaliar de forma preliminar a adequação das medidas tomadas para garantir a segurança do tratamento (INTIC, 2024)

Conforme a proposta de Artigo 31,

Art. 31, 1. Os registos de tratamento de dados pessoais e as autorizações da Autoridade Nacional de Protecção de Dados devem pelo menos indicar:

- a) o responsável e, se for caso disso, o seu representante;
- b) as categorias de dados pessoais tratados;
- c) as finalidades a que se destinam os dados e as categorias de entidades a quem podem ser transmitidos;
- d) a forma de exercício de direito de acesso, de rectificação, autorização e cancelamento;

- e) eventuais interconexões de tratamento de dados pessoais;
 - f) transferência de dados previstas para países terceiros.
2. Qualquer alteração das indicações constantes do número anterior está sujeita aos procedimentos previstos no Artigo 65º (INTIC, 2024).

As disposições propostas no artigo acima, remetem a alguns questionamentos. O primeiro questionamento deriva do fato de estar ausente na alínea d) as formas de exercício do direito à oposição, tal direito já apresentado mais acima, na proposta de Artigo 21. O segundo questionamento reside na nº 2, em que é feita alusão à um Artigo 65. Ora, a proposta que estamos a apreciar tem até 64 artigos, como apresentamos no início desta subseção. Ademais, mais uma vez achamos estranho quando verificamos uma numeração ordinal em meio à numeração cardinal em uso na proposta. O mesmo se sucede no Artigo 32, sobre Publicidade dos Tratamentos em que o proponente indica que

- Art. 32, 1. O tratamento de dados pessoais, quando deva ser autorizado ou notificado, consta de registo da Autoridade Nacional de Protecção de Dados, aberto à consulta pública.
2. O registo contém as informações enumeradas nas alíneas a) a d) e i) do Artigo 66º.
3. O responsável pelo tratamento não sujeito a notificação está obrigado a apresentar, de forma adequada, a qualquer pessoa que o solicite, pelo menos as informações indicadas no nº 1 do Artigo 67º. O disposto no presente Artigo não se aplica ao tratamento de dados em fontes acessíveis publicamente (INTIC, 2024).

Contudo, não existem os artigos 66 e 67 na proposta em análise. E atendendo que este artigo remete a estes outros inexistentes, significa que, o que se pretende regular aqui, encontra um vazio. Este vazio, se proposta for à aprovação nestas condições, vai ferir gravemente o direito à informação, dado que o artigo trata sobre a publicidade do tratamento.

O capítulo VIII versa sobre Acreditação, certificação e código de conduta. A proposta de Artigo 33 (Acreditação e Certificação) indica que

- Art. 33, 1. A autoridade competente para a acreditação dos organismos de certificação em matéria de protecção de dados é Autoridade Certificadora...
2. O ato de acreditação emitido pela Autoridade Certificadora, deve tomar em consideração os requisitos previstos na presente Lei, bem como os requisitos estabelecidos pela Autoridade Nacional de Protecção de Dados.
3. A certificação, bem como a emissão de selos e marcas de protecção de dados, é efectuada por organismos de certificação acreditados nos termos do nº 1, destinando-se a atestar que os procedimentos implementados cumprem o disposto na presente Lei.

Quanto ao código de conduta, este está previsto no Artigo 34 (Códigos de Conduta), onde lê-se que

Art. 34, 1. Compete à ANPD promover a elaboração de códigos de conduta destinados a contribuir em função das características dos diferentes sectores, para boa execução das disposições da presente Lei.

2. O tratamento de dados pessoais no âmbito da presente Lei é objecto de código de conduta.

3. Os códigos de conduta devem ser registados na ANPD.

4. ANPD pode rejeitar o registo de Código de conduta quando considere os mesmos contrários às disposições da presente Lei e demais legislação aplicável.

5. Compete à ANPD emitir pareceres e recomendações para que os responsáveis pela criação dos códigos de conduta efectuem as correcções necessárias. (INTIC, 2024)

O capítulo IX regula sobre a “Tutela administrativa e jurisdicional”. No Artigo 35 aponta

Art. 35, sem prejuízo do direito de apresentação de queixa à ANPD, qualquer pessoa pode, nos termos da lei, recorrer a meios administrativos ou jurisdicionais para garantir o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais (INTIC, 2024).

A proposta de Artigo 36, sobre Tutela jurisdicional, não deixa claro à que tribunais devem ser colocadas as ações intentadas contra o responsável pelo tratamento de dados ou o subcontratante quanto este tiver o estabelecimento em território estrangeiro, mas aponta que

Art. 36, 1. Qualquer pessoa, pode nos termos da Lei, recorrer judicialmente da violação dos direitos previstos na presente Lei.

2. As acções propostas contra ANPD são da competência dos Tribunais Administrativos.

3. O titular dos dados pode propor acções contra o responsável pelo tratamento ou o subcontratante, incluindo acções de responsabilidade civil.

4. As acções intentadas contra o responsável pelo tratamento ou um subcontratante são propostas nos tribunais nacionais se o responsável ou subcontratante tiver o estabelecimento em território nacional ou se o titular dos dados residir habitualmente (INTIC, 2024).

Sobre a Legitimidade da Autoridade nacional de Protecção de dados, o proponente indica, no Artigo 37, que

A ANPD tem legitimidade para intervir em processos judiciais no caso de violação das disposições da presente lei, e deve denunciar ao Ministério Público as infracções penais de que tiver conhecimento, no exercício das suas funções e por causa delas, bem como praticar os atos cautelares necessários e urgentes para assegurar os meios de prova (INTIC, 2024).

Na proposta que estamos a apreciar, aparentemente os artigos 38 e 39 foram reservados para a indicação das contraordenações muito graves e contraordenações graves, respetivamente. Contudo, nada consta do Artigo 39. No Artigo 38 (Contraordenações muito graves) lê-se que

1. Constituem contraordenações muito graves:

- a) Os tratamentos de dados pessoais com inobservância dolosa dos princípios previstos no Artigo 4 da presente Lei.
- b) Os tratamentos de dados pessoais que não tenham por base o consentimento ou outra condição de legitimidade, nos termos do Artigo 13 da presente Lei;
- c) O incumprimento das regras relativas à prestação do consentimento previstas no Artigo 19 da presente Lei.
- d) Os tratamentos de dados pessoais previstos no nº 1 do Artigo 14 da presente Lei, sem que se verifique uma das circunstâncias previstas no nº 2 do mesmo Artigo.
- e) Os tratamentos de dados pessoais previstos no Artigo 17 da presente Lei, que contrariem as regras estabelecidas.
- f) A exigência do pagamento de uma quantia em dinheiro fora dos casos previstos no Artigo 19 da presente Lei (INTIC, 2024).

À semelhança do Artigo 39 em que nada consta, o Artigo 40 reservado para dispor sobre a “Determinação da medida das sanções”, nada consta. Na sequência, o Artigo 41 (Prescrição do procedimento por contraordenação) aponta

O procedimento por contraordenação extingue -se por efeito da prescrição logo que sobre a prática da contraordenação hajam decorrido os seguintes prazos:

- a) Três anos, quando se trate de contraordenação muito grave;
- b) Dois anos, quando se trate de contraordenação grave (INTIC, 2024).

A proposta de Artigo 42 (Prazo de prescrição das sanções), faz o apontamento da prescrição das sanções, apontando a relação das sanções com o montante em causa. Assim, embora sem definição dos montantes,

As sanções previstas na presente lei prescrevem nos seguintes prazos:

- a) Três anos, no caso de sanções com montante superior a
- b) Dois anos, no caso de sanções de montante igual ou inferior a (INTIC, 2024).

O Artigo 43 apresenta o Destino das Multas. Segundo este artigo o “Art. 43, montante das sanções cobradas reverte em 60 % para o Estado e em 40 % para a ANPD.” (INTIC, 2024). Constitui preocupação para nós não termos observado ao longo desta proposta de lei alguma previsão de indenização para com as pessoas vítimas de contraordenações e/ou crimes no âmbito do tratamento dos seus dados pessoais. Este vazio pode não inibir a prática indisciplinada de tratamento de dados pessoais, por um lado. Por outro lado, com esta proposta de artigo parece que, mais uma vez, o cidadão é o maior lesado, tendo não só os seus dados pessoais maltratados, como nem sequer receber alguma indemnização decorrente disto.

Assim, verifica-se que, dos direitos que o direito de proteção de dados pessoais agrupa, como o Direito à informação; Direito de controle; Direito à abstenção, e; Direito à indenização, este último não está previsto na proposta de lei de proteção de dados pessoais de Moçambique, significando que, se a lei for aprovada com esta lacuna, os

danos materiais e morais frutos de coleta, tratamento ou divulgação de dados pessoais não será objeto de alguma indemnização.

O Artigo 44 sobre Cumprimento do dever omitido, aponta que “Sempre que a contraordenação resulte da omissão de um dever, a aplicação da sanção e o pagamento, não dispensam o infrator do seu cumprimento se este ainda for possível”.

O âmbito de aplicação das contraordenações, está disposto no Artigo 45, da seguinte maneira:

Art. 45, 1. As sanções previstas na presente lei aplicam -se de igual modo às entidades públicas e privadas.
 2. Nos termos do disposto no nº 7 do Artigo 83.º do RGPD, as entidades públicas, mediante pedido devidamente fundamentado, podem solicitar à ANPD a dispensa da aplicação de sanção durante o prazo de três anos a contar da entrada em vigor da presente lei.
 3. As entidades públicas estão sujeitas aos poderes de correção da ANPD, tal como previstos no RGPD e na presente lei, com exceção da aplicação de sanção nos termos definidos no número anterior. (INTIC, 2024).

Mais uma vez encontramos na proposta as marcas da “importação” de textos estrangeiros sem a devida adequação.

No que tange ao Regime subsidiário, a proposta de Artigo 46 aponta que “Art. 46, em tudo o que não esteja previsto na presente lei em matéria contraordenacional, aplica –se o disposto no regime geral do ilícito de mera ordenação social.” (INTIC, 2024).

A proposta em análise avança um conjunto de crimes ao longo dos seus artigos 47 a 53. O Artigo 47 versa sobre incumprimento das obrigações relativas a protecção de dados pessoais e dispõe que

Art. 47, 1. Sem prejuízo das demais obrigações reguladas na presente Lei, incorre em crime punível com pena de prisão de até 1 ano ou pena de multa de 120 dias, quem intencionalmente:
 a) Omitir a notificação ou o pedido de autorização a ANPD;
 b) Fornecer falsas informações na notificação ou nos pedidos de autorização para tratamento de dados pessoais, ou neste proceder a modificações consentidas pela presente Lei;
 c) Desviar ou utilizar dados pessoais de forma incompatível com finalidade determinante da recolha ou com base Legal
 d) Promover ou efectuar uma interconexão ilegal de dados pessoais
 e) Findo o prazo que estiver sedo fixado pela ANPD para cumprimento das obrigações previstas na presente Lei ou em outra legislação subsidiárias, as não cumprir
 f) Após a notificação pela ANPD para o não fazer, manter o acesso a redes abertas de transmissão de dados a responsável pelo tratamento de dados pessoais que não cumpram as disposições da presente Lei

2. A pena é agravada para o dobro nos seus limites quando se tratar dos dados pessoais a que se referem os Artigos 9.º e 10.º do RGPD (INTIC, 2024).

Sobre crime ligado ao Acesso indevido, o Artigo 48 avança que

Art. 48, 1. Quem, sem a devida autorização ou justificação, aceder, por qualquer modo, a dados pessoais é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

3. A pena é agravada para o dobro nos seus limites quando se tratar dos dados pessoais a que se referem

4. A pena é também agravada para o dobro nos seus limites quando o acesso:

a) for conseguido através de violação de regras técnicas de segurança; ou

b) tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial (INTIC, 2024).

O crime de Desvio de dados encontra-se descrito no Artigo 49, da seguinte maneira:

Art. 49, 1. Quem copiar, subtrair, ceder ou transferir, a título oneroso ou gratuito, dados pessoais

2. sem previsão legal ou consentimento, independentemente da finalidade prosseguida, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

3. A pena é agravada para o dobro nos seus limites quando se tratar dos dados pessoais a que se referem os

4. A pena é também agravada para o dobro nos seus limites quando o acesso:

a) for conseguido através de violação de regras técnicas de segurança; ou

b) tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial (INTIC, 2024).

A Viciação ou destruição de dados é um crime previsto no Artigo 50, referindo-se à

Art. 50, 1. Quem, sem a devida autorização ou justificação, apagar, destruir, danificar, ocultar, suprimir ou modificar dados pessoais, tornando-os inutilizáveis ou afetando o seu potencial de utilização, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.

2. A pena é agravada para o dobro nos seus limites se o dano produzido for particularmente grave.

3. Nas situações previstas nos números anteriores, se o agente atuar com negligência é punido com pena de prisão:

a) até 1 ano ou multa até 120 dias, no caso previsto no nº 1;

b) até 2 anos ou multa até 240 dias, no caso previsto no nº 2. (INTIC, 2024).

Ainda sobre os crimes tipificados na proposta de lei em apreciação, consta a Inserção de dados falsos no Artigo 51. Neste artigo lê-se que

Art. 51, 1. Quem inserir ou facilitar a inserção de dados pessoais falsos, com a intenção de obter vantagem indevida para si ou para terceiro, ou para causar prejuízo, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.

2. A pena é agravada para o dobro nos seus limites se da inserção referida no número anterior resultar um prejuízo efetivo (INTIC, 2024).

Os crimes dispostos do artigo 48 ao 51 podem ser evitados ao se adotar uma gestão arquivística dos dados, das informações, dos documentos contendo os

dados pessoais. A gestão de documentos oferece subsídios para fazer frente aos aspectos elencados nestes artigos.

O crime de Violação do dever de sigilo, está plasmado no Artigo 52 nos seguintes termos:

Art. 52, 1. Quem, obrigado a sigilo profissional nos termos da lei, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2. A pena é agravada para o dobro nos seus limites se o agente:

- a) for trabalhador em funções públicas ou equiparado, nos termos da lei penal;
- b) for encarregado de proteção de dados;
- c) for determinado pela intenção de obter qualquer vantagem patrimonial ou outro benefício ilegítimo;
- d) puser em perigo a reputação, a honra ou a intimidade da vida privada de terceiros.

3. A negligência é punível com pena de prisão até 6 meses ou com pena de multa até 60 dias (INTIC, 2024).

É igualmente punida, conforme o Artigo 53, a Desobediência. Este artigo aponta que

Art. 53, 1. Quem não cumprir as obrigações previstas e na presente lei, depois de ultrapassado o prazo que tiver sido fixado pela ANPD para o respetivo cumprimento, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2. A pena é agravada para o dobro nos seus limites se, depois de notificado para o efeito, o agente:

- a) não interromper, cessar ou bloquear o tratamento ilícito de dados;
- b) não proceder ao apagamento ou destruição dos dados quando legalmente exigível, ou findo o prazo de conservação fixado nos termos da presente lei; ou
- c) recusar, sem justa causa, a colaboração que lhe for exigida nos termos do Artigo 8.º da presente lei. (INTIC, 2024).

O Artigo 54 sobre punibilidade da tentativa aponta que nos crimes previstos pela proposta, a tentativa é sempre punível, e, a responsabilidade recai sobre as pessoas coletivas, de acordo com o Artigo 55 (Responsabilidade das pessoas coletivas).

Art. 55, As pessoas colectivas e entidades equiparadas, com exceção do Estado, de pessoas colectivas no exercício de prerrogativas de poder público e de organizações de direito internacional público, são responsáveis pelos crimes previstos na presente secção, nos termos do Artigo 11.º do Código Penal (INTIC, 2024).

Sem a indicação do capítulo X, a proposta aponta o Capítulo XI que versa sobre as Medidas de Segurança. O Artigo 56 (Segurança de Tratamento) determina que

Art. 56, 1. O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas, e estabelecer níveis de segurança adequadas, para

proteger os dados pessoais contra destruição total ou parcial, acidental ou ilícita, a perda acidental, a alteração total ou parcial, a difusão ao direit[o] não autorizado, fundamentalmente quando o tratamento implicar a sua transmissão em rede, e contra qualquer outra forma de tratamento ilícito.

2. As medidas de segurança devem assegurar atendimento aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, o nil de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.

3. O responsável pelo tratamento deve elaborar um documento com medidas, normas e procedimento de segurança aplicáveis ao tratamento de dados pessoais, detalhando os níveis de segurança, os recursos a proteger e as funções e obrigações das pessoas com acesso aos dados, de acordo com as regras de segurança (INTIC, 2024).

O termo documento aparece aqui apenas para se referenciar a alguma ação-meio para a proteção de dados pessoais e não como um elemento-fim e fulcral na proteção de dados pessoais. Sem dúvidas que a questão de segurança de(no) tratamento de dados pessoais está intimamente ligada ao processo de gestão de documentos, desde aspectos inerentes às características arquivísticas desses dados que devem ser preservados ao longo de todo o seu ciclo, como os aspectos inerentes à atividade classificatória, incluindo a observância dos graus de sigilo.

No Artigo 57 são apontadas como Medidas Especiais de Segurança:

1. O responsável pelo tratamento dos dados deve, relativamente aos dados indicados acima, tomar as medidas adequadas para:
 - a) impedir o acesso da pessoa não autorizada aos ficheiros e às instalações utilizadas para o tratamento dos dados;
 - b) impedir que suportes de dados passem a ser lidos, copiados, alterados ou retirados por pessoas não autorizadas;
 - c) impedir a introdução não autorizada bem como a tomada de conhecimento, a alteração ou eliminação não autorizada de dados pessoais inseridos;
 - d) impedir que os sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas através de instalação de transmissão de dados;
 - e) garantir que só as pessoas autorizadas possam ter acesso aos dados abrangidos pela autorização;
 - f) garantir a verificação das entidades a quem possam ser transmitidos os dados pessoais através das instalações de transmissão de dados;
 - g) garantir que se possa verificar a posterior em prazo adequado à natureza do tratamento conforme fixado em regulamentação aplicável a cada sector, quais os dados pessoais introduzidos, quando e por quem;
 - h) impedir que na transmissão de dados pessoais bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada.
2. Os sistemas devem garantir a separação lógica entre os dados referentes à saúde e à vida sexual, incluindo os genéticos dos restantes dados pessoais.
3. A Autoridade Nacional de Protecção de Dados pode determinar que, nos casos em que a circulação em rede de dados pessoais referidos nos Artigos acima possam por em risco direitos, liberdades e garantias de respectivos titulares, a transmissão seja cifrada.

A proposta dispõe, no Artigo 58, sobre o Sigilo Profissional. Antes de avançarmos apontando os parágrafos deste artigo, importa recordar que o sigilo profissional perpassa todas as áreas de atuação profissional, sobretudo a atuação do profissional de informação, em particular, o arquivista. Na gestão da informação os aspectos inerentes ao sigilo, desde a própria informação até aos ligados à ética e deontologia profissional, estão impostas. No Artigo 58 está definido que

Art. 58, 1. Os responsáveis de tratamento de dados pessoais, bem como as pessoas que no exercício das suas funções, tenham conhecimento dos dados pessoais tratados, ficam obrigados a sigilo profissional, mesmo após o término das suas funções.

2. Aplica-se o disposto no nº anterior aos membros da Autoridade Nacional de Protecção de Dados, bem como aos funcionários, agentes ou técnicos que exerçam funções de assessoria à Autoridade Nacional de Protecção de Dados, mesmo após o término do mandato.

3. O disposto nos números anteriores não exclui o dever de fornecimento das informações obrigatórias, nos termos legais, excepto quando constem de ficheiros organizados para fins estatísticos.

4. A violação do sigilo profissional obriga os seus autores à responsabilidade criminal, nos termos do Artigo 58 da presente Lei diploma, sem prejuízo da responsabilidade disciplinar ou civil, nos termos da presente Lei (INTIC, 2024).

O capítulo XI faz as Disposições finais e transitórias. No Artigo 59 (Disposição transitória) aponta:

Art. 59, 1. Os tratamentos de dados existentes em ficheiros manuais à data da entrada em vigor da presente Lei devem cumprir o disposto nos Artigos 7.º (Artigo 7.º Tratamento de dados sensíveis), 8.º (Artigo 8.º Suspeitas de actividades ilícitas, infracções penais e infracções administrativas), 10.º (Artigo 10.º Direito de informação) e 11.º (Artigo 11.º Direito de acesso) no prazo de 2 anos.

2. Em qualquer caso, o titular dos dados pode obter, a seu pedido e, nomeadamente, aquando do exercício do direito de acesso, a rectificação, a eliminação ou o bloqueio dos dados incompletos, inexactos ou conservados de modo incompatível com os fins legítimos prosseguidos pelo responsável pelo tratamento.

3. A Agência Nacional de Protecção de Dados Pessoais pode autorizar que os dados existentes em ficheiros manuais e conservados unicamente com finalidades de investigação histórica não tenham que cumprir os Artigos 7.º, 8.º e 9.º (Artigo 9.º Interconexão de dados pessoais), desde que não sejam em nenhum caso reutilizados para finalidade diferente (INTIC, 2024).

Os artigos citados nos parágrafos 1 e 3, apontam para matéria diferente do conteúdo apresentado na proposta em análise. Recapitulando os artigos em referência, o Artigo 7 é referente à Competências da Autoridade Nacional de Protecção de Dados; o Artigo 8 versa sobre Encarregados de Protecção de Dados; o Artigo 9 enfoca sobre o Dever de sigilo e confidencialidade; o Artigo 10 aponta as Funções do encarregado de protecção de dados; e o Artigo 11, por sua vez, versa sobre Encarregados de protecção de dados em entidades públicas (INTIC, 2024).

Portanto, a proposta de Artigo 59 fica esvaziada. Aliás, não existe ao longo de toda a Proposta de Lei de Protecção de Dados Pessoais que estamos a analisar, nenhum artigo sobre “Suspeitas de actividades ilícitas, infracções penais e infracções administrativas” (INTIC, 2024) e, também, nenhum artigo que disponha sobre “Interconexão de dados pessoais”, apenas a alínea d) do n° 1 do Artigo 47 que versa sobre “incumprimento das obrigações relativas a protecção de dados pessoais”, apontando que

Sem prejuízo das demais obrigações reguladas na presente Lei, incorre em crime punível com pena de prisão de ate 1 ano ou pena de multa de 120 dias, quem intencionalmente:

[...]

d) Promover ou efectuar uma interconexão ilegal de dados pessoais [...] (INTIC, 2024).

Ademais, é oportuno notar que, não apenas no artigo anterior, mas ao longo de toda a proposta em análise, o proponente faz menção à uma “Agência Nacional de Protecção de Dados” (INTIC, 2024) e, também, a uma “Autoridade Nacional de Protecção de Dados” (INTIC, 2024) sobre a qual dedica a proposta de capítulo III para indicar a sua natureza, composição e competências. Ora, nos parece que se trata da mesma entidade, porém em nenhum momento está estabelecida a sinonimidade no texto, como também não encontramos, para o caso da “Agência Nacional de Protecção de Dados” (INTIC, 2024), a sua natureza, composição e competências. Esta situação é flagrante do que estamos a chamar de “importação” de textos estrangeiros sem a devida adequação. Nesta senda, merece mencionar alguma falta de padronização terminológica nesta proposta de lei.

A proposta apresenta o capítulo XII para dispor sobre “Responsável dos Dados Pessoais?”¹⁸ e define, sem indicar o artigo, o responsável como “Qualquer pessoa singular ou colectiva, pública ou privada, qualquer outra organização ou associação que sozinha ou em conjunto com outras pessoas decida recolher e processar dados pessoais e determinar a sua finalidade” (INTIC, 2024).

São apontadas algumas obrigações desse responsável, do artigo 60 ao 63. No Artigo 60 (Obrigações de confidencialidade) está plasmado que “Art. 60, O processamento de dados pessoais é confidencial. É efectuado exclusivamente por indivíduos que agem sob a autoridade do responsável dos dados e somente sob as

¹⁸ O ponto de interrogação (?) foi encontrado assim na própria proposta de lei apreciada.

suas instruções” (INTIC, 2024). Este responsável tem Obrigações de Segurança, plasmadas no Artigo 61, isto é “Art.61, O responsável pelos dados deve tomar todas as precauções apropriadas, de acordo com a natureza dos dados e, em particular, evitar que esses dados sejam alterados ou destruídos, utilizados por pessoas não autorizadas” (INTIC, 2024).

Ora, “Art. 62, os dados pessoais não devem ser conservados para além do período necessário para fim pelo qual se fez a sua recolha e o seu processamento” conforme o Artigo 62 que aponta as Obrigações de Conservação (INTIC, 2024). Aliada à estas obrigações, através do Artigo 63 (Obrigações de Manutenção),

Art. 63, 1.O responsável pelos dados deve tomar todas as medidas necessárias com vista a assegurar que os dados pessoais processados possam ser explorados independentemente do dispositivo técnico utilizado no processo.
2.O funcionário que faz o processamento deve, em particular, assegurar que as mudanças tecnológicas não constituam um obstáculo para a utilização dos dados (INTIC, 2024).

A proposta de lei em apreciação, tem no seu último artigo, o Artigo 64, disposições sobre dados anonimizados. Nesta senda dispões que,

Art. 64, 1.Os dados anonimizados não serão considerados dados pessoais para os fins salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
2.A determinação do que seja razoável deve levar em consideração factores objectivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.
3.Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.
4.A autoridade nacional poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Protecção de Dados Pessoais (INTIC, 2024)

Com este artigo, notamos que a proposta parece não tomar como central a operação ou técnica de pseudonomização de modo que o nome de uma pessoa seja substituído por pseudônimos para evitar que seja identificada, dando primazia à anonimização, sendo ambas, técnicas relevantes para a protecção de dados pessoais, como se nota, por exemplo, através da proposta de Artigo 16.

O Artigo 64 apesar de ser o último, apresenta-nos uma surpresa, o “Conselho Nacional de Protecção de Dados Pessoais” (INTIC, 2024). Esta entidade em nenhum momento foi introduzida ao longo da proposta. Chegados aqui, inferimos a criação de

pelo menos três entidades no xadrez desta proposta de lei: uma Agência nacional de Proteção de Dados, uma Autoridade Nacional de Proteção de Dados e um Conselho Nacional de Protecção de Dados Pessoais. Não está claro se serão, de fato, três entidades distintas com as suas atribuições bem definidas e a desenvolverem as suas funções concomitantemente, ou se o proponente utiliza estas designações de forma indiscriminada querendo se referir à apenas uma, provavelmente à Autoridade Nacional de Proteção de Dados, sobre a qual dedicou um capítulo na proposta analisada.

Chegados aqui, constatamos que a proposta de lei não dedica alguma parte para dispor sobre o controlador de dados, como faz com o encarregado de proteção de dados. Do mesmo modo, também não apresenta disposições sobre o operador. Importa reforçar aqui que conforme os princípios gerais que orientam as normativas de proteção de dados pessoais, o controlador de dados tem a obrigação de garantir que todas as informações em seus sistemas de gestão de documentos estejam sempre atualizadas, o que demanda avaliação periódica dos documentos nos sistemas, evitando que dados imprecisos levem as instituições a violar direitos dos titulares de dados.

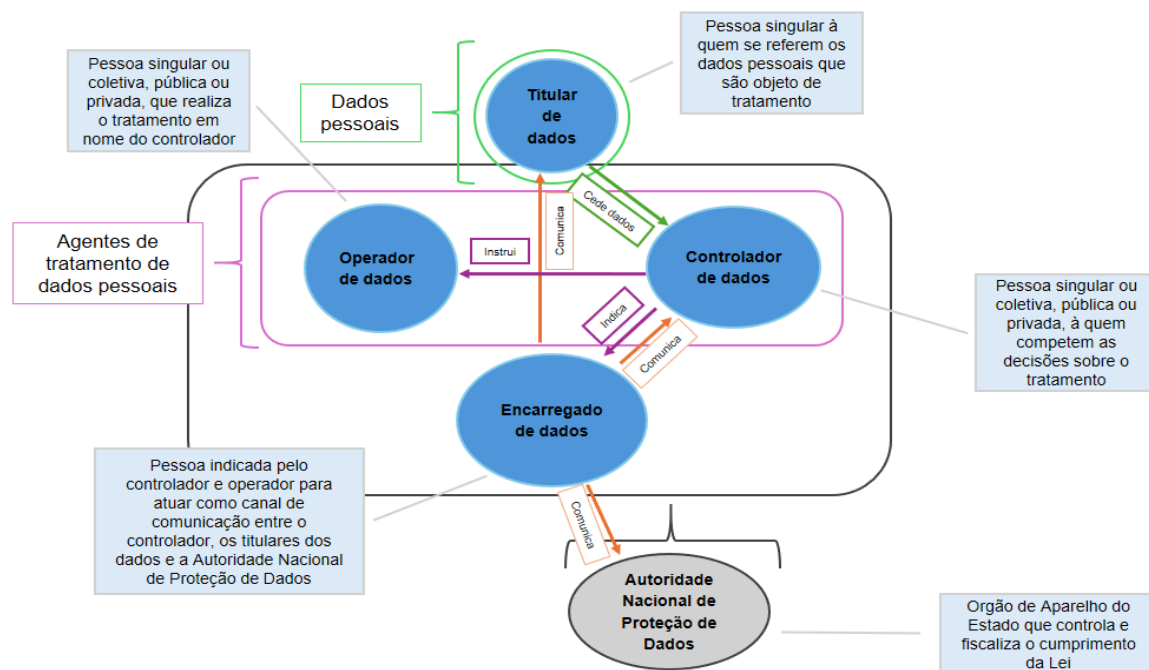
Ao finalizarmos a análise à proposta, chegamos à conclusão de que, a “Proposta de Lei de Protecção de Dados Pessoais” está sendo preparada seguindo a “tradição” de um “copiar-colar” de normativas estrangeiras sem que se observe adequações. Marcas gritantes desta prática pudemos observar, por exemplo, através da proposta do Artigo 15 sobre dados de Crianças e Adolescentes; Artigo 12 sobre encarregado de Protecção de Dados Entidades Privadas; Artigo 45 sobre o âmbito de aplicação das contraordenações; e, Artigo 47 sobre o incumprimento das obrigações relativas a proteção de dados pessoais, para citar alguns exemplos.

Resultando desta prática é notório também pela ocorrência de numeração ordinal de alguns artigos em detrimento de numeração cardinal que é comumente utilizada na legislação moçambicana.

Esta proposta de lei permite-nos visualizar, embora com alguma dificuldade, os principais atores e entidades no ecossistema de proteção de dados pessoais em Moçambique. Assim, a figura 10, na página 214, ilustra os atores que a Proposta de Lei elenca e sua relação. Aliás, em geral as normativas de proteção de dados pessoais

identificam quatro cruciais atores, o titular dos dados, os agentes de tratamento que são o controlador de dados e o operador de dados, e, o encarregado de dados. Estes quatro podem ser visualizados na proposta de lei do INTIC.

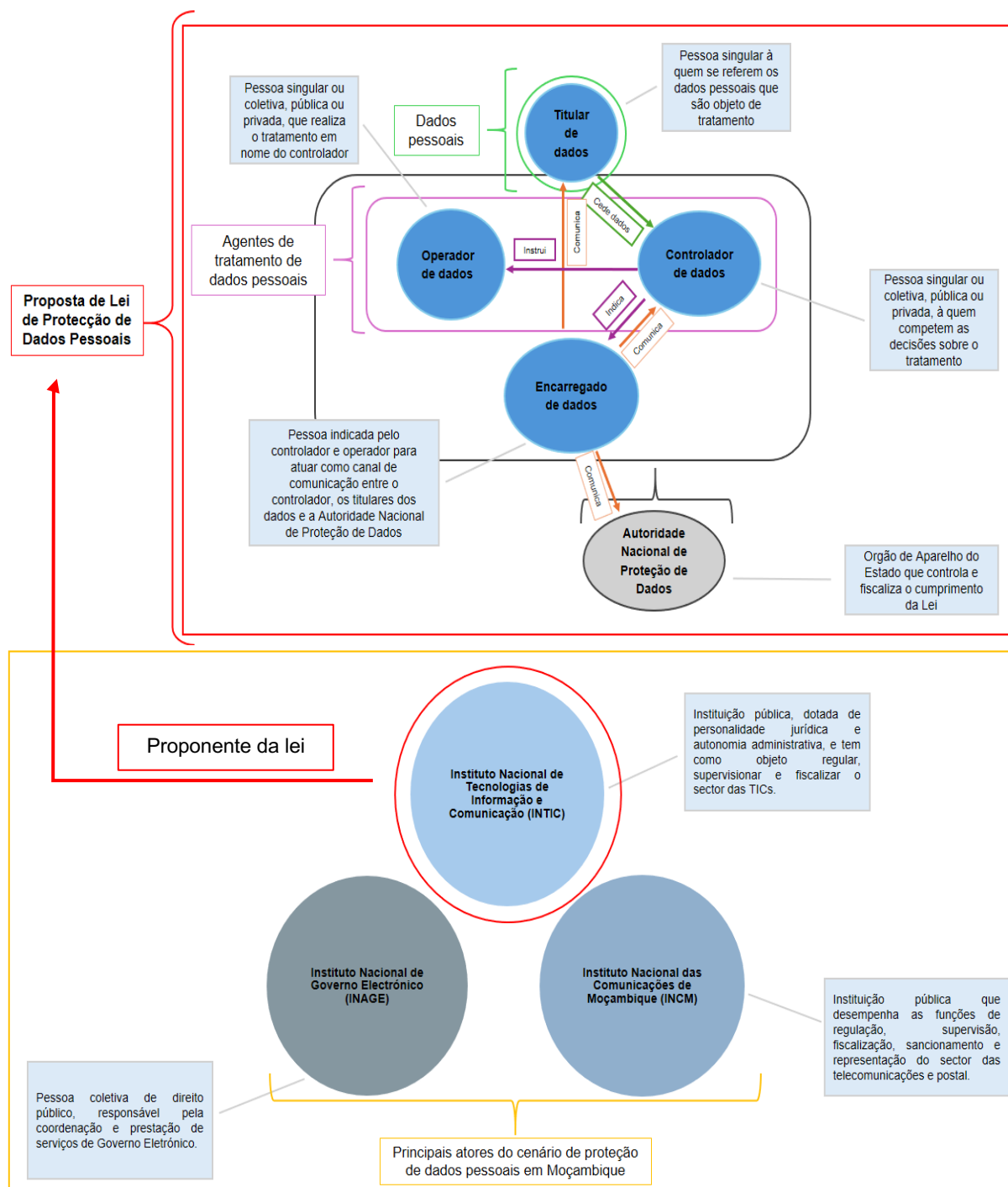
Figura 10 – Atores do processo de Proteção de dados pessoais em Moçambique



Fonte: Elaborado pela autora.

Atendendo os atores elencados na proposta de lei e considerando os atores identificados na seção 7, O QUADRO LEGAL MOÇAMBICANO DA PROTEÇÃO DE DADOS PESSOAIS, concretamente na subseção 7.2 Principais atores do cenário de proteção de dados pessoais em Moçambique, é ilustrado, na página a seguir, o ecossistema de proteção de dados pessoais em Moçambique, com a notável falta de atores arquivísticos, pelo menos explicitamente.

Figura 11 – Ecossistema da Proteção de dados pessoais em Moçambique



Fonte: Elaborado pela autora.

Como dissemos, a proposta de lei analisada foi elaborada pelo INTIC, como um dos principais atores do setor em que se pretende regular/legislar a proteção de dados pessoais, o que indica a inexistência de um órgão que se dedique à elaboração e redação de normativas o que faz com que o texto da proposta tenha fortes traços

das fontes estrangeiras à Moçambique. Nas subseções que se seguem são apontadas as diretrizes arquivísticas para a elaboração de uma normativa de proteção de dados pessoais.

8.2 Diretrizes arquivísticas para a elaboração de normativas de proteção de dados pessoais

Na esteira da proteção de dados pessoais, há diferentes mecanismos e/ou estratégias que podem ser adotadas para minimizar o risco de violação dos dados pessoais. Tais mecanismos e/ou estratégias partem desde estratégias mais técnicas da informática, aliado ao Direito, até a estratégias mais arquivísticas que tocam a gestão de documentos. É neste sentido que as diretrizes identificadas aqui, são sem equívoco, diretrizes arquivísticas.

No traçado das diretrizes, fazemos um caminho que parte da proposição de elaboração e formalização de uma política arquivística em Moçambique, passando pela revisão do sistema nacional de arquivos, adentrando na institucionalização da gestão de documentos e desembocando em aspectos arquivísticos mais específicos que devem ser acomodados nas normativas de proteção de dados pessoais.

8.2.1 Elaboração e formalização de política arquivística em Moçambique

Como fizemos indicação na nossa fundamentação teórica, é oportuno antes de avançarmos, lembrar que a perspectiva de política arquivística impingida aqui, é a de *policy*, ou seja, políticas públicas. À semelhança de outras, essa política arquivística determina os recursos administrativos, humanos, tecnológicos, etc., necessários para o alcance dos seus objetivos. Atendendo a sua forte relação com os sistemas organizacionais, as políticas arquivísticas configuram-se em nacional, estadual, regional, provincial, local, etc., conforme a estruturação dos países. Assim, neste trabalho é na dimensão nacional que se desenham propostas à volta da política arquivística em Moçambique, atentos ao fato de que não se deve confundir a legislação arquivística com a política, mas com o entendimento de que a legislação é

a fornecedora de elementos normalizadores à política, quer dizer, a legislação é um instrumento e objeto da política arquivística, neste caso.

Se olharmos para a política arquivística como uma política pública, o que significa que ela é consubstanciada por ações (e inações), tomada de decisão (e não tomada de decisão), então, a inexistência de uma política arquivística nacional em Moçambique formalizada em algum documento, como uma resolução aprovada pelo Conselho de Ministros, por exemplo, não significa que ela não existe, pois, a sua inexistência formal emite significados e propicia o *status quo* arquivístico em Moçambique.

Portanto, se o Estado moçambicano pretende ter os dados pessoais dos seus cidadãos salvaguardados, um dos principais aspectos que deverá ser considerado, que aliás é urgente, é a adoção formal de uma política arquivística nacional que orientará a identificação e utilização sistemática de recursos necessários para a implementação da própria política. Essa política de dimensão nacional deve compreender, para além de definir a missão, o objeto, os objetivos, os tipos de serviços e demais aspectos pertinentes à produção, uso e preservação da informação arquivística de natureza pública e privada, compreenderá programas, estratégias, incluindo o sistema nacional de arquivos, sobre o qual falamos a seguir. Esse sistema conhecerá melhor implementação e funcionamento se, de fato, for precedido pela elaboração e implementação da política arquivística nacional.

Sublinhamos a pertinência da formalização da política arquivística nacional em Moçambique pois, como apontamos nas sessões anteriores, a ausência de uma política formalizada em um documento pode significar a desvirtualização dos objetivos, da missão, dos serviços e instituições arquivísticas e propiciar violações de direitos aos cidadãos, bem como a falta de responsabilização.

É importante lembrar que uma política arquivística é transversal e esta sua qualidade demanda para a sua elaboração, para além de conhecimento técnico e científico da área arquivística, conhecimento sobre a realidade do Estado que pretende regular a área arquivística, as formas de produção, uso e conservação dos arquivos públicos e privados, os atores abrangidos pela política arquivística, para além de conhecimentos oriundo do Direito, da Informática, entre outras áreas. Este

envolvimento de atores não arquivísticos vai possibilitar acautelar diversos aspectos que a política arquivística deve dar conta, incluindo a proteção de dados pessoais.

Não só é necessário prosseguir com este caráter transdisciplinar na concepção da política arquivística nacional (de Moçambique), como deve-se igualmente pensar nesta política em termos interdisciplinares, pois como dissemos mais acima, a perspectiva de política arquivística que conduz esta tese, é a de *policy*, ou seja, políticas públicas, e como tal, dialoga ou deve dialogar com outras políticas públicas. Moçambique conta hoje como uma panóplia de políticas públicas formalizadas em documento, como são os casos da política para a sociedade de informação, política de segurança cibernética, entre outras, com as quais a política arquivística nacional deverá ser dialogante. Portanto, a elaboração e formalização da política arquivística nacional em Moçambique mostra-se mais uma vez oportuna.

8.2.2 Revisão do sistema nacional de arquivos de Moçambique

Depois de propormos a elaboração e formalização de uma política arquivística em Moçambique, na qual prevê-se o desenho de um sistema nacional de arquivos, relembremos aqui que esse sistema é o meio de operacionalização de uma política nacional de arquivos e, por essa razão, não deve preceder, mesmo em termos formais, a política arquivística, como contrariamente se assiste em Moçambique desde 1992.

Se a política nacional de arquivos é um pré-requisito em relação a um sistema nacional de arquivos, o cenário atual moçambicano, demanda a revisão do SNAE 2018 e tal revisão deve acontecer sob alçada de uma política arquivística nacional, elaborada e formalizada previamente, emanando as premissas para a arena arquivística moçambicana. Portanto, decorrente do espírito de um sistema nacional de arquivos, espera-se que o SNAE revisto não só apresente as facetas teóricas, jurídicas e operacionais, como também através dele próprio, sejam visualizadas e mantidas relações de interdependência com a administração. Em síntese, deve haver uma articulação entre as instituições arquivísticas e os serviços arquivísticos.

Para isso, devem ser criadas instituições arquivísticas que correspondam à configuração político-administrativa do Estado moçambicano. Como já apontamos, o AHM é o arquivo nacional de Moçambique e, em termos efetivos, é a única instituição arquivística pública nacional. Quer dizer, o pressuposto impingido no SNA de 1992, de criação de outros arquivos públicos, os de nível provincial em particular, não se concretizou.

Lembremos que Schellenberg (2006) apontou razões para a criação de arquivos públicos. Partindo do exame dos motivos que levaram a criação dos primeiros arquivos nacionais da história, com exemplos de França, Inglaterra e Estados Unidos, o autor aponta quatro grandes razões. A primeira ligada a necessidade de se incrementar a eficiência governamental, a segunda ligada a razões culturais pois esses arquivos são uma fonte de cultura, a terceira razão ligada a interesses pessoais e a quarta razão derivada de motivos oficiais pois os documentos são necessários as atividades do governo, constituindo-se em sua principal fonte de informação.

Para além da criação de instituições arquivísticas de nível provincial e distrital, por exemplo, devem ser institucionalizados os serviços arquivísticos no seio das instituições públicas, em particular.

Com um sistema nacional de arquivos funcional, espera-se que a perspectiva que se tem de documentos e de arquivos, seja mais alargada, tendo a legislação cobertura sobre os documentos nas instituições não arquivísticas, ou seja, o sistema nacional de arquivos estará abrangendo os serviços de arquivo, mas também as instituições arquivísticas, abarcando assim os documentos que darão entrada nos arquivos distritais, provinciais ou no arquivo nacional de Moçambique. Portanto, a legislação vai descrever o sistema nacional de arquivo.

Ora, para a criação do sistema nacional de arquivos em Moçambique, entendendo que a lógica imposta no SNAE não corresponde politicamente, nem tecno-cientificamente à lógica de sistema nacional de arquivos, será preciso adotar uma série de medida, entre elas: 1) (r)estabelecer o AHM como o órgão arquivístico da administração central pois nele residem os conhecimentos técnicos e científicos da Arquivística em Moçambique; 2) impor às instituições públicas não arquivísticas a obrigação de criarem e institucionalizarem

serviços de arquivo; 3) promover o recolhimento de documentos às instituições arquivísticas provinciais; 4) impor a proteção dos documentos e dos arquivos face à deterioração e destruição intencional ou venda. Essas medidas vão se traduzir num modelo de gestão de documentos e de arquivos que inclua no cenário moçambicano a representação de entidades arquivísticas dos níveis central, provincial e local.

Não obstante, julgamos ser imperioso reforçar o papel do AHM também por via da alteração da sua posição funcional e estrutural na UEM. Temos compreendido que a sua posição na hierarquia daquela universidade tem enfraquecido a sua atuação como Arquivo Nacional. Para que os recursos cheguem até ele, percorrem uma complexa estrutura. Ora, antes de mais, a UEM deve responder ao ministério que a tutela. O que queremos dizer é que, o AHM deve estar numa posição que lhe confira autonomia e independência, de fato. Ainda que permaneça sob alçada do ministério que superintende a área da educação, o AHM não deve continuar administrativamente ligada à UEM como uma das suas unidades orgânicas.

Um sistema nacional de arquivos estabelecido como produto de uma política arquivística nacional, abrirá espaço para a melhor institucionalização dos serviços de arquivos nas instituições públicas e, portanto, das atividades de gestão de documentos nessas instituições.

A proposta seguinte visa, justamente, olhar as questões arquivísticas nessa dimensão operacional.

8.2.3 Institucionalização da gestão de documentos em Moçambique

Já se constatou através da literatura que não se tem a mesma compreensão do termo gestão de documentos, sobretudo devido às especificidades que cada país tem decorrente de suas tradições arquivísticas, história, tipos de governo, cultura etc. Geralmente os países adotam uma abordagem de gestão de documentos dita americana ou uma dita europeia, se as principais razões que lhes levam a adotá-la forem econômico-administrativa ou histórico-arquivística, respetivamente. O primeiro modelo coloca ênfase nos documentos nas instituições não arquivísticas, e o segundo

coloca ênfase nos documentos nas instituições arquivísticas (arquivos distritais, arquivos provinciais, arquivos nacionais, etc.).

Quando observamos o cenário arquivístico de Moçambique, percebemos que este país parece adotar uma abordagem com dupla tendência, europeia e americana. A gestão arquivística é tomada por uma orientação patrimonial(ista), consciente ou não. Mesmo assim, vários aspectos não são atendidos por esse modelo que, como já apontamos, não é constituído por arquivos públicos, aliás a única instituição arquivística que conhecemos a sua existência é o AHM. Pensamos que a inexistência da política arquivística nacional, que definiria os recursos financeiros, humanos, infraestruturais, tecnológicos, etc., condiciona este *status quo*. O que não permitirá, por exemplo, o recolhimento, significando que não haverá a separação de documentos que deverão ir aos arquivos permanentes (sobretudo enquanto instituições), daqueles que deverão ser eliminados e provavelmente, não haverá uma garantia do direito individual de controle e acesso à informação, não sendo respeitadas, conseqüentemente, as restrições temporais e eventuais de acesso.

O que estamos a dizer no parágrafo anterior é que a gestão de documentos compreende uma série de atividades relacionadas aos documentos antes destes chegarem aos arquivos permanentes e/ou históricos. Assim, essas atividades devem ocorrer nas diversas instituições públicas moçambicanas, para que a seleção daqueles documentos que devem ser recolhidos às instituições arquivísticas, pelo menos às provinciais ou a nacional, ocorra. Todas essas atividades deverão ser desenvolvidas por arquivistas, isto é, antes de saírem das instituições não arquivísticas moçambicanas e depois de chegarem nas instituições arquivísticas. E ao longo desse processo deverá estar acautelada a proteção dos dados pessoais contidos nestes documentos.

Portanto, no seio das diferentes instituições públicas moçambicanas, deverão ser desenvolvidos um conjunto de procedimentos e operações técnicas atinentes à produção de documentos (que inclui elaboração e recebimento), à tramitação, ao uso, à avaliação e ao arquivamento de documentos em fase corrente e intermediária, de modo que os documentos que já perderam o seu valor primário possam ser eliminados, caso também não tenham ganho o valor secundário, e os que ganharam o valor secundário possam ser recolhidos aos arquivo permanente, o que poderá

igualmente favorecer à eliminação de dados pessoais que não mais devem ser preservados pela instituição produtora de documentos.

Este conjunto de procedimentos e operações técnicas que devem ser desenvolvidas nas diferentes instituições públicas (em particular) não arquivísticas, acomoda igualmente a noção de ciclo vital de documentos, ou seja documentos nascem sendo elaborados ou recebidos pelas instituições, vivem e envelhecem sendo utilizados e distribuídos para atender os propósitos que ditaram a sua elaboração ou recebimento e preservados em razão do seu valor e, finalmente, morrem sendo eliminados em razão da perda daquele valor. Nesse ciclo, os documentos nas diferentes instituições não arquivísticas moçambicanas passam, como já vimos, por três estágios: “de um estágio corrente para um estágio semi corrente e, finalmente, para um estágio não corrente” (Beckles, 2014, p. 239).

Por sua vez, no ciclo vital dos documentos encontram-se as bases da teoria das três idades, fundamentando que os documentos de arquivo, em razão do seu uso e do seu valor para a instituição não arquivística que os elaborou ou recebeu ou para terceiros, eles podem sofrer intervenções em uma ou mais fases (corrente, intermediária e permanente). Essas intervenções nas duas primeiras fases, são os procedimentos e operações da gestão de documentos. Ora, a gestão de documentos, ela mesma tem seus procedimentos e operações técnicas distribuídos em fases que representam o ciclo de vida dos documentos, ou seja, fases de produção (elaboração e recebimento), de utilização e conservação, e, de eliminação.

Na fase de produção de documentos, as instituições não arquivísticas moçambicanas, ou seja, as instituições do poder executivo, legislativo e judiciário, nos seus diferentes níveis, devem conceber e gerir formulários, preparar e gerir correspondências, gerir relatórios e orientações, aplicar tecnologias para estes processos, entre outras atividades. Na fase de utilização e conservação dos documentos, as instituições não arquivísticas moçambicanas devem criar (se não existirem) e/ou melhorar os seus sistemas de arquivo e de recuperação de informação, gerir o seu correio e telecomunicações, gerir as reproduções e a automação do processo. Os sistemas de arquivo e de recuperação de informação aqui indicados devem ser ajustados às necessidades operacionais e antecipar a necessidade de proteger qualquer informação que o necessite em particular (Rhoads, 1989). Na fase de eliminação as instituições devem identificar e descrever as séries documentais,

estabelecer os prazos de guarda, avaliar e eliminar os documentos, bem como efetuar o recolhimento dos documentos de valor secundário.

Para atender à estas operações fazem-se necessários os instrumentos de gestão de documentos. O plano de classificação e a tabela de temporalidade de documentos proporcionam a simplificação e a racionalização dos procedimentos de gestão, proporcionando agilidade na recuperação da informação, eliminação criteriosa de documentos que perderam o seu valor primário e não ganharam o valor secundário, e para os de valor secundário, conduz à preservação permanente.

O SNAE, em vigor em Moçambique desde 2018, apresenta um plano de classificação e uma tabela de temporalidade de documentos, bem como um classificador de informação classificada. Com a revisão deste sistema que estamos a sugerir, esperamos que estes instrumentos sejam igualmente revistos de modo a espelhar a realidade moçambicana e ser capaz de, recuperar o contexto de produção documental e a atividade que justificou a sua elaboração ou recebimento através do novo plano de classificação e da nova tabela de temporalidade ter a definição de prazos de guarda que se desvinculem da cultura de sigilo, refletindo os valores dos documentos (primário ou secundário), orientar a eliminação desses documentos com vista a eliminar igualmente os dados pessoais contidos nos documentos que já atenderam suas obrigações administrativo-legais e/ou determinar que sejam guardados permanentemente. Ou seja, o princípio de finalidade e o princípio da duração do período de conservação, como dois dos princípios que embasam a proposta de lei de proteção de dados pessoais de Moçambique, estarão a ser respeitados.

Ao pensarmos nos instrumentos de gestão de documentos, consideramos igualmente a implementação de programas de gestão de documentos. Nesta senda, atendendo ao cenário arquivístico atual de Moçambique, exige-se, para a implementação desses programas de gestão de documento, que o AHM tome a liderança como uma autoridade pública central, e, participem ativamente, outros atores da arena arquivística moçambicana. Os programas de gestão de documentos podem ser implementados em 4 níveis, como vimos, o nível mínimo, nível mínimo ampliado, nível intermediário e nível máximo, de forma escalonada.

Face à configuração arquivística moçambicana atual, orienta-se a implementação do nível mínimo de programa de gestão de documentos, pois ainda não se pode falar de um nível mínimo ampliado ou outros superiores, se o Estado moçambicano não conta, de fato, com sistemas para preparar listas de conservação e eliminação de documentos, não elimina documentos e não recolhe os documentos de valor permanente às instituições arquivísticas. Aliás, estas instituições arquivísticas devem ser criadas para poderem receber os documentos objeto de recolhimento. Portanto, ao se formular uma política arquivística nacional em Moçambique, deve-se identificar o programa de gestão de documentos a ser implementado, conforme o nível visto acima, tomando-o como uma parte fundamental dessa política.

Ademais, como apontou Lowry (2020), a qualidade dos dados, e aqui sublinhamos a qualidade de dados pessoais, depende da qualidade dos documentos originais de onde são extraídos esses dados. Portanto, a fiabilidade, a exatidão e a fidedignidade dos documentos determinam a fiabilidade, a exatidão e a fidedignidade dos dados pessoais. Significa que documentos mal conservados podem resultar em dados pessoais imprecisos, incompletos ou não verificáveis, o que pode levar as instituições moçambicanas a desperdiçarem recursos, desde tempo e dinheiro, tentando processar dados pessoais de má qualidade.

Cenários como o descrito acima, podem induzir as instituições do poder executivo, legislativo e/ou judiciário à erros e tomada de decisões mal informadas possibilidades de violar os direitos fundamentais dos cidadãos moçambicanos. É neste contexto que os procedimentos utilizados pelo arquivista moçambicano ou que opera em Moçambique são incontornáveis para o controlo e a segurança dos dados pessoais e a garantia dos direitos fundamentais resulta da eficácia de um programa de gestão de documentos e do desempenho eficaz do arquivista moçambicano.

Em Moçambique, o arquivista é, até ao momento que apresentamos esta tese, formado apenas em uma das cerca de 56 IES existentes no país. Ou seja, somente a UEM é que oferece um curso de graduação em Arquivologia, oferecido na Escola de Comunicação e Artes, na cidade de Maputo, a capital de Moçambique, sem representação noutras partes deste país.

O curso denominado Licenciatura em Arquivística que começou a ser operacionalizado em 2016, tem lançado arquivistas para a atuação profissional desde

de 2020. Estes arquivistas foram formados dentro de um quadro curricular em que os planos temáticos das disciplinas não apresentam, de forma explícita, o tema proteção de dados pessoais, embora tenham disciplinas de gestão de documentos e de política de informação (não especificamente política arquivística). Como apontamos na subseção 5.1.1, temos consciência de que os planos temáticos são moldados e desenvolvidos em planos analíticos pelos docentes, mas a falta de conteúdo programático sobre proteção de dados pessoais, pode fazer com que a proteção de dados pessoais não seja abordada em sala de aulas ou seja discutida com pouca profundidade. Daí que achamos que tendo o tema “proteção de dados pessoais” patente no plano temático, vai obrigar o docente a desenvolvê-lo em sala de aulas, não se tornando “facultativo”, conforme a afinidade ou não do docente à temática, domínio, etc. A falta de tópicos específicos de proteção de dados pessoais nos leva a inferir que os arquivistas que estão sendo formados dentro deste quadro curricular podem apresentar algum despreparo para lidar, de forma mais profissional com a proteção de dados pessoais, seja no setor público ou privado, olhando para aspectos técnicos e legais.

Abre-se assim, junto da diretriz que orienta a institucionalização da gestão de documentos, a necessidade de se criarem mais cursos de graduação em Arquivologia em Moçambique, por um lado. Por outro lado, o curso existente e estes que poderão ser criados ao longo do país, deverão contemplar de forma explícita, a temática de proteção de dados pessoais, inclusive na sua forma transversal, pois atravessa diferentes disciplinas, com destaque aqui para a disciplina de gestão de documentos (digitais e tradicionais). Portanto, atendendo estas condições, o arquivista moçambicano, formado num quadro que dá conta da questão de proteção de dados pessoais, este profissional deverá ter um caráter proativo e preventivo, e se revestir de um papel jurídico, ético e de comunicação através do qual lhe caberá:

- Informar os titulares de dados moçambicanos sobre a intenção subjacente à utilização das suas informações pessoais e o compromisso que a instituição, seja ela do poder executivo, legislativo ou judiciário, tem em assegurar um tratamento justo e legal;
- Realizar avaliação regular dos riscos de privacidade para os documentos da instituição; e,

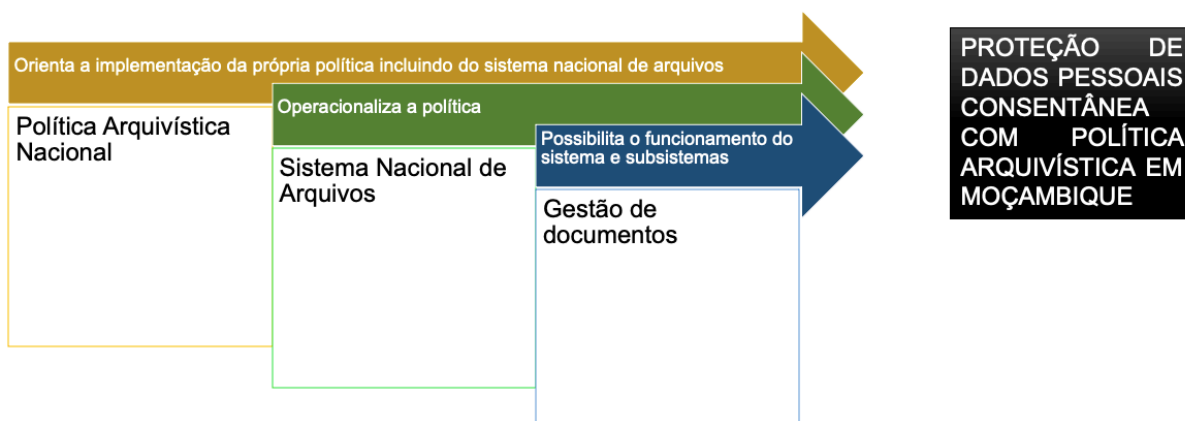
- Capacitar e sensibilizar sobre a legislação, políticas e procedimentos de proteção de dados, o pessoal dessa instituição, a todos os níveis. Portanto, o arquivista deverá ser proativo para a inclusão da temática nas formações que ocorrem na instituição em que estiver a exercer as suas funções.

Esse mesmo arquivista moçambicano deverá cumprir um papel técnico e tecnológico pelo qual ele deverá:

- Mapear a utilização dos documentos digitais nas plataformas electrónicas da instituição;
- Atribuir a devida autorização de segurança apenas aos funcionários autorizados a aceder aos documentos que contêm dados pessoais;
- Utilizar métodos de redação para permitir que a informação sensível seja visualmente bloqueada a pessoas não autorizadas, permitindo-lhes visualizar a informação solicitada. O arquivista moçambicano poderá utilizar para esta tarefa, programas informáticos, se se tratarem de documentos digitais. E no contexto de documento dito tradicional, impresso ou em papel, o arquivista moçambicano terá de ocultar manualmente as os dados pessoais antes de fornecer os documentos ao requerente;
- No contexto digital, o arquivista moçambicano deverá anonimizar, pseudonomizar e utilizar cifragem, de modo que as pessoas deixem de ser identificáveis. Sublinha-se aqui a utilização da encriptação como medida de segurança para proteger dados sensíveis, sobretudo quando os documentos que os contenham forem arquivados eletronicamente;
- Fazer auditorias regulares que incluam a coleta de metadados que mostrem quem viu o documento; quem o modificou; em que data; quem o imprimiu; quem o retirou do sistema ou quem tentou destruir, alterar ou exportar ilegalmente dados pessoais do documento;
- Deverá gerir os documentos, incluindo conceber sistemas de classificação, de modo a facilitar, ao mesmo tempo, a recuperação rápida dos dados e/ou documentos, e, o controle dos documentos que contêm dados pessoais.

As diretrizes apresentadas acima, podem ser representadas na figura 12, na página que se segue.

Figura 12 – Diretrizes arquivísticas para a elaboração de normativas de proteção de dados pessoais



Fonte: Elaborado pela autora

Diante dessas diretrizes e considerando um cenário arquivístico moçambicano ideal, onde não só exista uma política arquivística nacional formalizada e dialogante, como também uma entidade coordenadora do sistema nacional de arquivo que seja uma instituição arquivística dotada de autonomia, de conhecimento científico e técnico na área dos arquivos, assim como um cenário em que se tenham profissionais arquivistas atuantes, contribuindo nas diversas esferas moçambicanas para a proteção de dados pessoais, visualiza-se um novo cenário, semelhante ao representado na figura que apresentamos mais abaixo.

Em síntese, na figura 13 apresentada na página 228, propõe-se a integração explícita do profissional arquivista no processo de tratamento de dados pessoais. Porque a figura de operador corresponde ao ator que realiza o tratamento, julgamos que o perfil a desempenhar este papel é o perfil de um arquivista, que carrega em sua bagagem, a técnica, o conhecimento científico e a ética. Igualmente está sendo proposto um CNA atuante que tenha o AHM como presidente. Para além de presidir o conselho, o AHM, neste ecossistema que estamos a propor, deverá ser o coordenador do sistema nacional de arquivo, este último que deverá ser o produto da política arquivística nacional a ser definida pelo CNA. O AHM e o CPISE, que fazem

9 CONSIDERAÇÕES FINAIS

À medida que os anos, as décadas, os séculos e milénios se passam, várias transformações vão ocorrendo no mundo. De tais transformações, emergiu uma classificação de “mundos”, mundo digital e mundo analógico. Nesses “mundos”, com as suas peculiaridades, nasceram e recrudesceram preocupações variadas. Uma delas tem a ver com a proteção de dados pessoais dos indivíduos que habitam o mundo. A proteção de dados pessoais figura como um direito fundamental em vários instrumentos legais e ordenamentos mundo afora. A preocupação com a proteção de dados pessoais acentua-se é um direito que se violado, pode de forma mais leva às mais graves, afetar outros direitos fundamentais das pessoas. Portanto, é uma questão que toca a todos, pessoas singulares e coletivas, públicas e privadas, pequenas ou grandes. Toca a vários, senão todos os setores, profissionais, de saúde, de informática, de comunicação, de Direito, arquivistas, etc.

Portanto, a presente tese foi desenvolvida atenta a este cenário e com inquietações que orbitam em questionamentos como “de que forma se estabelece a relação da proteção de dados pessoais com a gestão de documentos dentro do escopo de uma política arquivística no cenário moçambicano? Os aspectos da gestão de documentos para a proteção de dados pessoais estão devidamente incorporados nas normativas moçambicanas atinentes à proteção de dados pessoais? Como é tratada a proteção de dados pessoais na legislação moçambicana?”.

Com estes questionamentos, formulamos, *a priori*, a hipótese segundo a qual “se a política arquivística deve orientar o desenvolvimento de atividades que dizem respeito à gestão de documentos, então na gestão de documentos residem as ações para o controle e proteção de dados pessoais contidos nos documentos, havendo assim uma relação indissociável entre a gestão de documentos e a proteção de dados pessoais, no escopo de uma política arquivística nacional”. Esta hipótese confirma-se com o culminar do processo desta pesquisa, e com os objetivos, geral e específicos, alcançados. Portanto, todo o exercício que conduziu este trabalho de pesquisa procurou, de forma geral, “estabelecer a relação da gestão de documentos e a proteção de dados pessoais no bojo de uma política arquivística e propor diretrizes arquivísticas para a elaboração de normativas de proteção de dados pessoais em Moçambique”. Especificamente, procurou-se compreender, na teoria, os conceitos de

política arquivística nacional (aqui, nacional não se refere à Moçambique ou Brasil, ou outro país, mas sim o nível de formulação desta política, que não é institucional e nem internacional), de gestão de documentos e de proteção de dados pessoais; analisar o cenário arquivístico moçambicano; levantar o quadro legal da proteção de dados pessoais no âmbito internacional, no Brasil e traçar uma linha de tempo da proteção de dados pessoais em Moçambique; identificar o papel da gestão de documentos e do seu profissional na proteção de dados pessoais; analisar a relação da gestão de documentos e proteção de dados pessoais; e, propor diretrizes para a elaboração de normativas de proteção de dados pessoais consentâneas com a gestão de documentos.

Considerando a tradução desses objetivos em objetivos de ordem teórica, operacional e analítica, eles nos levaram à concepção de seções com o mesmo cunho. Assim, as bases teóricas foram apresentadas nas seções, DOS DADOS AOS DOCUMENTOS DE ARQUIVO, DA GESTÃO DE DOCUMENTOS E POLÍTICA ARQUIVÍSTICA À PROTEÇÃO DE DADOS PESSOAIS e A PROTEÇÃO DE DADOS PESSOAIS DESDE UMA PERSPECTIVA ARQUIVÍSTICA, respondendo aos objetivos “compreender, os conceitos de política arquivística nacional, de gestão de documentos e de proteção de dados pessoais”; “identificar o papel da gestão de documentos e do seu profissional na proteção de dados pessoais”; e, “analisar a relação da gestão de documentos e proteção de dados pessoais”.

A seção A ARENA ARQUIVÍSTICA MOÇAMBICANA, onde foi apresentado e analisado o cenário arquivístico de Moçambique passando por uma breve ilustração da estrutura político-administrativa de Moçambique, responde ao objetivo “analisar o cenário arquivístico moçambicano”. Este objetivo conduziu-nos, entre outros aspetos, a conhecer o arquivista moçambicano, desde a sua formação à sua atuação profissional.

O objetivo “levantar o quadro legal da proteção de dados pessoais no âmbito internacional, no Brasil e traçar uma linha de tempo da proteção de dados pessoais em Moçambique” foi alcançado através das seção, PANORAMA INTERNACIONAL E BRASILEIRO DA PROTEÇÃO DE DADOS PESSOAIS, onde mapeou-se a legislação de proteção de dados pessoais no mundo (exceto Moçambique), passando pela legislação brasileira e finalizando com um olhar geral à proteção de dados pessoais em África, e da seção O QUADRO LEGAL MOÇAMBICANO DA PROTEÇÃO DE

DADOS PESSOAIS, onde para além do levantamento legal que foi feito, são identificados os principais atores do cenário de proteção de dados pessoais em Moçambique.

A seção POR UMA PROTEÇÃO DE DADOS PESSOAIS CONSENTÂNEA COM UMA POLÍTICA ARQUIVÍSTICA EM MOÇAMBIQUE, foi concebida para responder ao objetivo “propor diretrizes para a elaboração de normativas de proteção de dados pessoais consentâneas com a gestão de documentos”. Antes disso, exatamente para viabilizar a proposta de diretrizes feitas, foi analisada nessa seção, sob um olhar arquivístico, a Proposta de Lei de Proteção de Dados Pessoais, elaborada pelo INTIC em 2024.

A elaboração destas seções e consequente consecução dos objetivos e prossecução da tese, foi mediante a adoção de procedimentos metodológicos que julgamos adequados. Assim relembramos aqui que esta tese, pela sua finalidade, insere-se nas pesquisas aplicadas. A pesquisa desenvolvida classifica-se como sendo qualitativa e dentro desta abordagem ou natureza qualitativa, a pesquisa realizada é do tipo documental e igualmente exploratório-descritiva. Esta tese reveste-se de estudo de caso como método de pesquisa e utilizou-se da análise de conteúdo como método de tratamento e análise de dados, que foram levantados através da revisão de literatura, da observação indireta e da pesquisa documental. Ora, um dos nossos maiores constrangimentos no desenvolvimento desta tese foi a impossibilidade de realização de entrevistas e aplicação de questionário, devido a convulsões sociais decorrentes de tensões políticas que se romperam em Moçambique desde 2023 com as eleições autárquicas e que recrudesceu com as tensões políticas pós-eleitorais de 2024.

Com o trabalho desenvolvido para a realização desta tese percebe-se que desde que Moçambique nasceu como um país independente, há sementes de respeito à privacidade através do Artigo 33º da CRPM (Moçambique, 1975). Estas sementes lançadas em 1975 foram germinando e crescendo, ainda que lentamente e sob diferentes vieses. A proteção de dados pessoais começa a ficar mais explícita na CRM de 1990. Aliás essa CRM de 1990 inaugurou vários aspectos no contexto moçambicano. A questão do direito à informação começa a se vislumbrar aqui, embora com uma parcial ou total orientação virada à comunicação social, interpretação que pode ser reforçada com a política de informação de 1997.

Ao observarmos a arena arquivística moçambicana, é perceptível a sua fraqueza. Na verdade, ela sofre de várias fragilidades. Uma institucional, que parece ter sido ainda mais enfraquecida ao longo dos últimos 18 anos, período em que se assistiu a uma “usurpação” das atribuições de arquivo nacional do AHM, como também a estagnação hierárquico-estrutural dele. A fraqueza institucional também se manifesta pelo, praticamente inexistente CNA, que não parece, sequer, se reunir regularmente. As associações profissionais são igualmente e cumulativamente, fracas e inexistentes.

Outra fraqueza tem que ver com o curso de graduação em Arquivística. Até ao momento que escrevemos este trabalho, o curso lecionado pela UEM é o único no país e o currículo deste parece necessitar de reforço em matéria de proteção de dados pessoais.

Uma terceira fraqueza, decorre das anteriores. É uma fraqueza de ordem humana, na medida em que, poucos são os arquivistas formados ao longo do país para fazer face à demanda, atendendo que apenas um curso de graduação existe. Estes mesmos, são formados dentro de um currículo que carece de reforma a fim de dotar os seus formandos de habilidades e competências diante da proteção de dados pessoais. Ora, já formados estes arquivistas não encontram uma associação em que possam, por exemplo, se reciclarem em matérias emergentes da área, ou ainda discutir com seus pares sobre aspectos prementes como a proteção de dados pessoais.

Podemos ir mais longe e entender que diante de tudo, há uma fraqueza maior, na verdade “uma força que enfraquece” a área arquivística em Moçambique. Parece não haver da parte de quem decide, alguma vontade para alterar esta (des)ordem rumo à um bom porto. Parece que, os ainda poucos, arquivistas altamente capacitados com altos graus académicos, não são capitalizados ocupando lugares de gestão, nas principais instituições da arena arquivística moçambicana com vista a inverter o cenário nebuloso, parece mesmo que os alertas que estes levanta(ra)m não ecoa aos ouvidos do executivo e do legislador. Podemos entender um pouco disso observando os perfis daqueles que dirigem, hoje, as principais instituições desta arena, ou seja, não estiveram lá e, até aqui não estão, os arquivistas. Ademais, a alteração deste cenário implica a alteração da posição hierárquico-administrativa do

AHM e, a não tomada de decisão da(s) entidade(s) competente(s) para tal, é uma decisão com todos condimentos possíveis e interpretáveis.

Certamente, todo este cenário tem implicações para e na formulação de uma política arquivística nacional em Moçambique. Os principais atores arquivísticos tornam a área opaca, com ou sem intenção. Isto pode levar à que normativas de proteção de dados pessoais que estão em elaboração, não contemplem estes atores da área arquivística e não se observem os ditames arquivísticos nessas normativas, colocando em risco os direitos fundamentais dos cidadãos.

Concluimos que, diante do quadro legal moçambicano da proteção de dados pessoais e considerando o *status quo* da arena arquivística moçambicana, há bases legais, técnicas e humanas para uma proteção de dados pessoais à luz de uma política arquivística nacional. Carece, contudo, de ser assumida e com carácter urgente esta questão ao mais alto nível executivo e legislativo, uma formulação e formalização da política arquivística nacional envolvendo os arquivistas, pesquisadores e técnicos, bem como profissionais afins. Sem dúvidas que neste contexto o sistema nacional de arquivos deverá ser (re)desenhado nesta qualidade de sistema e com características que espelham um sistema de arquivos a este nível. Aliás, a análise à Proposta de Lei de Protecção de Dados Pessoais reforça a ideia da necessidade de inclusão de atores arquivísticos na preparação de normativas de proteção de dados pessoais, com vista a assegurar as qualidades de integridade, confidencialidade, acurácia e autenticidade dos dados pessoais presentes numa panóplia de documentos de arquivo impressos e/ou digitais (natos ou digitalizados) durante todo o ciclo vital desses documentos.

Atendendo e considerando as diferentes versões do sistema nacional de arquivos, ou se quisermos os projetos de sistema como aponta Nharreluga (2021), não vemos verdadeiramente Arquivos públicos sendo criados desde a versão de SNA 1992, que aliás deixou à sua sorte toda a implementação do dito sistema, embora fizesse indicação dessas instituições. Ora, o que veio a ser plasmado nas versões posteriores criou e cria ruídos na compreensão do que é considerado um sistema nacional de arquivos em Moçambique.

Os, assim chamados, sistema nacional de arquivos do Estado em Moçambique não contemplam, na sua estrutura nuclear, instituições arquivísticas e nem serviços

arquivísticos. A única instituição arquivística que se vê é o AHM que tem um papel à margem, enquanto “órgão de gestão de documentos na fase permanente e de assessoria ao órgão director central do Sistema”. Como se nota, esta formulação é em si confusa, denotando até falta de auscultação aos arquivistas que já existem em Moçambique desde os tempos da vigência do SNA 1992. É uma formulação que a dada altura parece resgatar o papel de um Arquivo Nacional que deveria orientar e assistir técnica e cientificamente toda a gestão arquivística. Essa formulação é mesmo contraditória à orientação patrimonial que se infere do SNAE 2018 ao colocar a gestão de documentos na fase permanente, não apontando para a gestão de arquivos.

Como dissemos, não conseguimos vislumbrar no suposto sistema nacional de arquivos de Estado em vigor, serviços arquivísticos que, no seio das instituições não arquivísticas, seriam os responsáveis pela orientação e assistência técnica e científica da gestão de documentos. Ora, sem se realizarem operações da gestão de documentos, que documentos serão acessados livremente através da Lei do Direito à Informação? Como serão recuperados estes documentos? Que documentos serão objeto de operações para a proteção de dados pessoais neles contidos? Que documentos serão recolhidos ao arquivo permanente? Que documentos serão recolhidos ao AHM? Que documentos serão recolhidos ao Arquivo Nacional? Mas também podemos questionar que documentos serão eliminados? Quando? Como? Num cenário como o de Moçambique, a resposta para estas perguntas é o desconhecimento.

Assim, se o sistema nacional de arquivo que operacionaliza uma política nacional de arquivo é inexistente em termos práticos e lógicos, como também a própria política arquivística nacional em Moçambique não existe em termos formais, o que podemos “prognosticar” em relação à proteção de dados pessoais em Moçambique? Considerando que os dados pessoais são parte integrante de imensurável quantidade de documentos de arquivo que se encontram nas diferentes instituições privadas e, sobretudo, públicas em que não são adotados os princípios arquivísticos, não é colocada em prática a gestão de documentos, aliás por sua falta, e falta de um sistema nacional de arquivos fruto de uma política arquivística nacional inexistente, essas instituições não conhecem a sua produção documental, consequentemente, não consegue dar acesso aos que precisam de fruir o seu direito à informação e elas mesmas não têm acesso ao que produziram para apoiar a tomada de decisão, o que

denuncia “janelas” para violações aos dados pessoais. Entenda-se que, parte dos que não conseguem exercer o seu direito à informação são os próprios titulares de dados.

Considerando os níveis de aplicação de um sistema de gestão de documentos ou simplesmente de um programa de gestão de documentos que Rhoads apontou em 1989, podemos dizer que nenhum deles está em implementação em Moçambique, nem sequer o nível mínimo onde “Nível mínimo: não se pode dizer que um governo tem um programa de gestão de documentos si não conta, no mínimo, com sistemas para preparar listas de conservação e eliminação de documentos, eliminar documentos conforme ao indicado na lista e recolher aos arquivos nacionais os documentos de valor permanente” (Rhoads, 1989, p. 16). Com as palavras de Heredia Herrera (1991), parece que Moçambique encontra-se do lado da pior das hipóteses em que conta mais, quando existem, com depósitos de documentos e não com arquivos. Esta situação configura-se em um “atentado” à proteção de dados pessoais.

Considerando a definição de Cunha e Cavalcanti (2008) “política de arquivo como um documento formal que define a missão, os objetivos, tipos de serviços e demais informações pertinentes às atividades do arquivo.”, podemos afirmar que em termos formais Moçambique não conta com uma política arquivística formalizada em um documento o que põe em causa os objetivos, a missão, dos serviços e instituições arquivísticas e pode significar que estão ocorrendo violações de direitos dos cidadãos, desde o direito à informação, à proteção dos seus dados pessoais. Aliás, estes cidadãos têm o mesmo direito à informação sobre o tratamento dos seus dados.

Ligado a isto está a insistência no desenho e implementação (se de fato atingem este estágio), de sistema nacional de arquivos de Estado que não encontra alicerces numa política formulada pautando pela harmonia dos diversos aspectos que deve atender.

Como aludido acima, foi analisado o currículo do único curso de graduação em Arquivística em Moçambique, ministrado na ECA da UEM. Constatou-se que nos planos temáticos das disciplinas nucleares deste curso, não aparecem previstas temáticas sobre proteção de dados pessoais. Entendemos que a ausência de um tópico formalizado em plano temático pode levar a proteção de dados pessoais a ser negligenciada como um tema a discutir, ou o que achamos mais provável nos dias que correm, a proteção de dados pessoais pode não ser discutida em profundidade

junto dos alunos, fazendo as devidas relações com a gestão de documentos e políticas arquivísticas. Este hipotético cenário, pode revelar que os arquivistas formados e em formação dentro deste quadro curricular, apresentem algum despreparo para lidar, de forma mais completa possível com a proteção de dados pessoais, em seus aspectos técnicos, tecnológicos e legais.

Ora, traçamos diretrizes arquivísticas com vista a fazer face ao atual cenário da proteção de dados pessoais em Moçambique. São diretrizes em prol de uma normativa de proteção de dados pessoais consentânea com a política arquivística. Neste âmbito, e dada a inexistência formal da política arquivística nacional, as diretrizes traçadas tomam três principais dimensões, das quais a primeira engloba as duas últimas. Assim, as diretrizes arquivísticas para a elaboração de normativas de proteção de dados pessoais, são igualmente diretrizes para a reversão do cenário arquivístico moçambicano.

A primeira diretriz, é a elaboração e formalização de política arquivística em Moçambique”, em que se toma a política arquivística como uma política pública, o que significa que ela é consubstanciada por ações (e inações), decisão (e não-decisão), sendo que a inexistência de uma política arquivística nacional em Moçambique formalizada em algum documento, como uma resolução aprovada pelo Conselho de Ministros, por exemplo, não significa que ela não existe, pois a sua inexistência formal emite significados e propicia o *status quo* arquivístico em Moçambique. Nestes termos orienta-se a adoção formal de uma política arquivística nacional que instruirá a identificação e utilização sistemática de recursos necessários para a implementação da mesma. Essa mesma política de dimensão nacional compreenderá, para além de definir a missão, o objeto, os objetivos, tipos de serviços e demais aspectos pertinentes à produção, uso e preservação da informação arquivística de natureza pública e privada como as questões de privacidade e de proteção de dados pessoais, compreenderá programas, estratégias, incluindo o sistema nacional de arquivos, que é a segunda diretriz que elaboramos. Com a política arquivística formulada, espera-se que a legislação dela decorrente acomode, explicitamente, a proteção de dados pessoais.

A segunda diretriz, é a revisão do sistema nacional de arquivos em Moçambique. Com esta diretriz, parte-se do princípio que Moçambique não tem, verdadeiramente, um sistema nacional de arquivos (do Estado), embora tenham sido

aprovados, revogados e revistos ao longo dos tempos, instrumentos legais com esta designação. Assim, orienta-se que seja desenhado um sistema nacional de arquivos, que seja, antes de mais, fruto da política arquivística nacional previamente formulada, aprovada e formalizada. Com um sistema nacional de arquivos funcional, haverá cobertura sobre os documentos nas instituições não arquivísticas moçambicanas, ou seja, cobrindo os serviços de arquivo, mas também cobrindo as instituições arquivísticas moçambicanas, quer dizer, cobrindo os documentos que darão entrada nos arquivos distritais, provinciais ou no arquivo nacional de Moçambique. Portanto, a legislação de que fizemos menção acima, irá descrever o sistema nacional de arquivo.

Para este sistema será preciso (r)estabelecer o AHM como o órgão coordenador do sistema e presidente do conselho nacional de arquivos (órgão que deverá ser atuante), criação de instituições arquivísticas e institucionalização de serviços de arquivo. Quer seja nas instituições arquivísticas, quer seja nas instituições não arquivísticas, também chamadas de instituições produtoras, que integram esse sistema nacional de arquivo, será imposta a proteção dos documentos (digitais ou analógicos), não só contra a deterioração por agentes biológicos, químicos e/ou humanos, mas também proteção contra acesso não autorizado, modificação maliciosa, destruição intencional ou venda dos documentos, como um todo ou dos dados pessoais neles contidos. Essas medidas demandam, inequivocamente, a adoção da gestão de documentos e de arquivos.

Porque o nosso centro de atenções está na gestão de documentos, a diretriz terceira, é a institucionalização da gestão de documentos em Moçambique. Importa referenciar que a ordem de colocação das diretrizes não reflete, necessariamente, a ordem de importância. Esta colocação reflete o encadeamento que as diretrizes apresentam e uma lógica gerencial-operacional. Portanto, nesta diretriz orienta-se, numa fase inicial, a implementação do nível mínimo de programa de gestão de documentos, pois ainda não se pode falar de um nível mínimo ampliado ou outros superiores, se o Estado moçambicano não conta, de fato, com sistemas para preparar listas de conservação e eliminação de documentos, não elimina documentos e não recolhe os documentos de valor permanente às instituições arquivísticas. Neste exercício devem estar devidamente arrolados os documentos contendo dados pessoais que continuarão sendo conservados em razão do seu valor e os que serão

eliminados, cumprindo com os princípios de finalidade e de duração da conservação da proteção de dados pessoais.

Para o desempenho destas atividades, requer-se arquivistas moçambicanos de qualidade. Portanto junto da diretriz que orienta a institucionalização da gestão de documentos, devem ser criados mais cursos de graduação em Arquivologia em Moçambique que contemplem em suas disciplinas e planos temáticos, de forma explícita, a temática de proteção de dados pessoais, no entorno digital e analógico. Isto significará que o arquivista formado nesse quadro, terá, *à priori*, um caráter proativo e preventivo, e estará munido de competências e habilidades jurídicas, éticas e comunicacionais, bem como competências e habilidades técnicas e tecnológicas. Ademais, olhando para aqueles que são os principais atores apontados pela Proposta de Lei de Proteção de Dados Pessoais no processo de tratamento, julgamos que o “operador” deve ser um arquivista justamente porque este ator faz o tratamento de dados pessoais, e o tratamento, na nossa compreensão é um exercício, antes de mais, de gestão de documentos, e portanto o arquivista é o profissional em melhores condições para desempenhar este papel. Não obstante a qualidade de dados pessoais, isto é, a sua fiabilidade, acurácia, fidedignidade, integridade, autenticidade, etc., depende da qualidade dos documentos de arquivo onde estão contidos e/ou de onde são extraídos esses dados pessoais. Significa que dados pessoais mal geridos podem ser resultado da inexistente ou má gestão de documentos e pode acarretar fraudes e violações graves aos direitos fundamentais dos cidadãos moçambicanos.

Assim, Moçambique deve rever a sua legislação de modo a sanar as incongruências e contradições entre as diversas normativas sobre a proteção de dados pessoais e o acesso à informação, específicas e conexas, e concebê-las como parte de uma política arquivística nacional, da qual não só a infraestrutura legal faz parte, como também integra um programa de gestão de documentos. Aliás, em 1989 Rhoads já apontava que um programa bem concebido de acesso e difusão precisa, entre outros aspectos, da “eliminação de toda contradição que se coloca entre o direito de acesso à informação do público e os direitos à vida privada dos particulares” (Rhoads, 1989, p. 22). Nessa revisão que estamos a sugerir, pensamos ser uma oportunidade para ser revista igualmente a Constituição da República de Moçambique e fazer-se a integração do *habeas data*.

Diante do exposto acima, podemos dizer que é defendida a tese segundo a qual não se pode garantir a efetiva proteção de dados pessoais (dos moçambicanos e outros) sem, junto a outras ações, realizar efetivamente a gestão de documentos, pois esses dados pessoais são parte indissociável da composição documental, sejam eles documentos digitais ou não. E para que a gestão de documentos ocorra, a política arquivística, em particular a nacional, deve ser elaborada, formalizada em documento e implementada, orientando entre outras, o desenvolvimento de atividades de gestão de documentos.

Ao terminarmos, voltamos a sublinhar o cunho social desta tese e a nossa esperança que ela possa suscitar maior cuidado para a proteção de dados pessoais dos cidadãos moçambicanos (tendo sido este o nosso terreno) observando-se um direito fundamental e um direito humano. Mas também como já foi apontado acima, a contribuição desta tese ultrapassa os muros de Moçambique e se releva capital para o aprofundamento mais universal do campo teórico da Arquivologia e da Ciência da Informação destacando elementos que colocam mais evidente a relação indissociável da gestão de documentos e a proteção de dados pessoais.

Pelos constrangimentos e limitações enfrentados no desenvolvimento desta tese, cientes de que um trabalho desta natureza quase sempre, senão sempre, é inacabado, bem como convictos de que esta tese é o passo inicial para o aprofundamento do debate sobre a proteção de dados pessoais numa perspectiva arquivística em Moçambique, sobre o “balanço” entre o acesso à informação e à proteção de dados, abrem-se, através desta tese, caminhos para produções científicas (regulamentares e curriculares) na Ciência da Informação, na Arquivologia e no cruzamento destas com outras ciências, em Moçambique e noutras esferas, com envolvimento mais direto de diversos segmentos que perfazem o ecossistema arquivístico.

REFERÊNCIAS

- ADAM, W. Archivística para Bibliotecarios: Puente conceptual entre dos mundos. **Serie N° 90**. 2014. Disponível em: <https://repositorio.utem.cl/handle/30081993/870>. Acesso em: 13 nov. 2024.
- AFRICAN DECLARATION ON INTERNET RIGHTS AND FREEDOMS COALITION. **Declaração Africana sobre Direitos e Liberdades na Internet**. 2014
- ALVES, I. *et al.* **Dicionário de Terminologia Arquivística**. Instituto da Biblioteca Nacional e do Livro, Lisboa, 1993. *E-book*.
- AMARAL, W. Sistemas e serviços de informação em Moçambique. Maputo, 1994
- AMARAL, W. **Vocabulário básico de documentação**. Maguezo editores, Maputo, 2003.
- ARQUIVO NACIONAL. **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro: Arquivo Nacional, 2005. *E-book*.
- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Titular de Dados**. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/titular-de-dados-1/titular-de-dados> . Acesso em: 23 dez. 2024.
- BAGATINI, J. A.; GUIMARÃES, J. A. A vulnerabilidade dos dados pessoais: um iminente desafio ao fazer arquivístico. *In* **MEMORIAS DEL XIII CONGRESO DE ARCHIVOLOGÍA DEL MERCOSUR** 21- 25 de octubre de 2019. Montevideo-Uruguay (p. 709).
- BARDIN, L. **Análise de conteúdo**. Lisboa: edições, v. 70, p. 225, 1977. *E-book*.
- BECKLES, C-A. **International perspectives on data protection and its relationship to records management: recommendations for emerging practice in the West Indies**. Ph.D., University of Dundee, 2014. Disponível em: <https://discovery.dundee.ac.uk/en/studentTheses/34dcc74f-52ca-4189-a663-ec3ffd2de13b> Acesso em: 29 ago. 2023.
- BELLOTTO, H. L. **Arquivos permanentes: tratamento documental**. Rio de Janeiro: FGV editora, 2006.
- BERNARDES, I. P.; DELATORRE, H. Gestão documental aplicada. **Arquivo Público do Estado de São Paulo**, São Paulo, 2008. Disponível em: <https://ria.ufrn.br/jspui/handle/123456789/1377> . Acesso em: 11 dez. 2024.
- BITTENCOURT, P. R. Seguindo rastros e encontrando vestígios: Um mapeamento da teoria das três idades dos arquivos. **Boletim do Arquivo da Universidade de Coimbra**, v. 35, n. 1, p. 161–188, 30 jun. 2022.

BOFF, S. O.; FORTES, V. B. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. **Sequência** (Florianópolis), p. 109–127, jun. 2014.

BUCKLAND, M. Information as thing. **Journal of the American Society of Information Science**, v.42, n.5, p. 351-360, jun. 1991.

CABSELA, C. P.; SILVA, L. C.; TROITIÑO, S. BRASIL E PORTUGAL NA FORMAÇÃO DE MOÇAMBIKANOS EM CIÊNCIA DA INFORMAÇÃO. In: SILVA, C. G. D.; REVEZ, J.; CORUJO, L. **Diálogos na Ciência da Informação: Atas do XIV Encontro EDICIC**. 2024. *E-book*.

CAPURRO, R.; HJORLAND, B. O conceito de informação, **Perspectivas em Ciência da Informação**, v. 12, p. 148–207, 2007.

CHIZZOTTI, A. **Pesquisa em ciências humanas e sociais**. São Paulo: Cortez. 4ª edição. 2000. *E-book*.

CONSELHO DA EUROPA. Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. 1950.

CONSELHO DA EUROPA. Convenção 108+: Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados Pessoais. 2018

CONSELHO INTERNACIONAL DE ARQUIVOS. **Declaração Universal Sobre os Arquivos**. 2010.

CONSELHO INTERNACIONAL DE ARQUIVOS. **Multilingual Archival Terminology Database**. Disponível em: <http://www.ciscra.org/mat/mat/term/1136> . Acesso em: 24 jul. 2024.

COMISSÃO INTERMINISTERIAL DA REFORMA DO SECTOR PÚBLICO. **Estratégia da Reforma e Desenvolvimento da Administração Pública – ERDAP (2012-2025)**, aprovada pelo Conselho de Ministros na sua 29ª Sessão Ordinária, de 14 de agosto de 2012.

COMISSÃO INTERMINISTERIAL DA REFORMA DO SECTOR PÚBLICO. **Estratégia Global da Reforma do Sector Público – EGRSP (2001-2011)**. Maputo, 25 de junho de 2001.

COMISSÃO EUROPEIA. **Guidance on data protection for archive services**. Disponível em: https://commission.europa.eu/about-european-commission/service-standards-and-principles/transparency/access-documents/information-and-document-management/archival-policy/european-archives-group/guidance-data-protection-archive-services_en . Acesso em: 10 ago. 2024.

COMMONWEALTH. **Mozambique**. Disponível em: <https://thecommonwealth.org/our-member-countries/mozambique> . Acesso em: 10 jan. 2025.

CUESTA, F. F. Protección de datos en archivos públicos. **Tábula**, n. 15, 1 maio 2012.

CUNHA, M. B.; CAVALCANTI, C. R. O. **Dicionário de biblioteconomia e arquivologia**. Brasília: Briquet de Lemos, 2008. *E-book*.

DESPACHO do ministro da Justiça, Assuntos Constitucionais e Religiosos, 28 de maio de 2018.

DIAZ, J. A. S. B. A INVENÇÃO COLONIAL DE MOÇAMBIQUE: DOS IMPÉRIOS AFRICANOS À COLÔNIA E PROVÍNCIA ULTRAMARINA. **Revista Brasileira de Estudos Africanos**, v. 8, n. 16, 2023. Disponível em: <https://seer.ufrgs.br/index.php/rbea/article/view/134080> . Acesso em: 10 jan. 2025.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico: Journal of Law**, v. 12, n. 2, p. 91–108, 2011.

DONEDA, D. Da privacidade à proteção de dados pessoais. [s.l.] **Renovar Rio de Janeiro**, 2006.

DUCHEIN, M. O respeito aos fundos em arquivística: princípios teóricos e problemas práticos. **Arquivo & Administração**, v. 10-14, n. 2, 1986. Disponível em: <https://brapci.inf.br/v/49818>. Acesso em: 2 set. 2025.

DURANTI, L. Registros documentais contemporâneos como provas de ação. **Revista Estudos Históricos**, v. 7, n. 13, p. 49–64, 1994.

DURANTI, L. From Digital Diplomats to Digital Records Forensics. **Archivaria**, p. 39–66, 2009. Disponível em: <https://archivaria.ca/index.php/archivaria/article/view/13229> . Acesso em: 3 set. 2025.

ESTATUTO da Associação dos Arquivistas de Moçambique.

FERREIRA, D. A. A.; PINHEIRO, M. M. K.; MARQUES, R. M. Privacidade e proteção de dados pessoais: perspectiva histórica. **InCID: Revista de Ciência da Informação e Documentação**, v. 12, n. 2, p. 151–172, 30 nov. 2021.

FORNASIER, M. O.; KNEBEL, N. M. P. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados, **Revista Direito e Práxis**, v. 12, p. 1002–1033, 2021.

FRAZÃO, A. Fundamentos da proteção dos dados pessoais Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. Thomson Reuters Brasil. 2019

GARCIA, R. D. Os direitos à privacidade e à intimidade: origem, distinção e dimensões. **Revista da Faculdade de Direito do Sul de Minas**, v. 34, n. 1, 2018. Disponível em: <https://revista.fdsu.edu.br/index.php/revistafdsu/article/view/257> . Acesso em: 10 nov. 2024.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. Rio de Janeiro: Grupo GEN, 2022. E-book. ISBN 9786559771653. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559771653/> Acesso em: 27 ago. 2023.

GIL, A. C. **Como elaborar projetos de pesquisa**. 7. ed. [3ª Reimp.]. - Barueri [SP]: Atlas, 2025.

GOMES, G. M. Uma abordagem jurídica das políticas públicas: elementos formadores, base legal e controle pelo Judiciário. 2019. 156 f. Dissertação (Mestrado em Direito) – Faculdade de Direito de Alagoas, Programa de Pós-Graduação em Direito, Universidade Federal de Alagoas, Maceió, 2013. Disponível em: <http://www.repositorio.ufal.br/jspui/handle/riufal/4379> . Acesso em: 4 set. 2025.

GONZÁLEZ, J. A. M.; MANGUE, M. V. **Perfil profissional na área de ciência da informação em Moçambique**. Maputo: UEM/ECA; Madrid: UC3M/DBD, 2014.

GRÁCIO, J. C. A. Metadados para a descrição de recursos da Internet: o padrão Dublin Core, aplicações e a questão da interoperabilidade. 2002. 127 f. Dissertação (mestrado) - Universidade Estadual Paulista, Faculdade de Filosofia e Ciências, 2002. Disponível em: <http://hdl.handle.net/11449/93722> . Acesso em: 04 set. 2025.

GRÁCIO, J. C. A. **Preservação digital na gestão da informação: um modelo processual para as instituições de ensino superior**. São Paulo: Cultura Acadêmica, 2012. Disponível em: <http://hdl.handle.net/11449/113727> . Acesso em: 4 set. 2025.

GREENLEAF, G.; COTTIER, B. International and regional commitments in African data privacy laws: A comparative analysis. **Computer Law & Security Review**, v. 44, p. 105638, 2022.

HEREDIA HERRERA, A. (1991). **Archivística General: teoría y práctica**. ampl. Sevilla: Servicio de Publicaciones de la Diputación de Sevilla. 1991.

HEREDIA HERRERA, A. Política de gestión de documentos electrónicos: análisis del marco jurídico para su aplicación. **Boletín de la ANABAD**, v. 64, n. 1, p. 11–36, 2014.

HEREDIA HERRERA, A.; RODRIGUEZ, S. M. T. Em torno do tipo documental. OFFICINA - Revista da Associação de Arquivistas de São Paulo, v. 1, n. 1, 20 jun. 2022. Disponível em: <https://revista.argsp.org.br/index.php/revista-da-associacao-de-arquivi/article/view/8>>. Acesso em: 29 ago. 2025.

INDOLFO, A. C. Gestão de documentos: uma renovação epistemológica no universo da arquivologia. **Arquivística. net**, 2007, vol. 3, no 2, p. 28-60.

INTERNET SOCIETY. **Glossary of Internet Terms**. [s.d.]. Disponível em: <https://www.internetsociety.org/internet/glossary-internet-terms/>>. Acesso em: 14 nov. 2024

JARDIM, J. M. A face oculta do Leviatã: gestão da informação e transparência administrativa. <http://seer.enap.gov.br/index.php/RSP/article/view/141/146>, 2008. Disponível em: <<http://repositorio.enap.gov.br/jspui/handle/1/1486>>. Acesso em: 3 nov. 2024.

JARDIM, J. M. Caminhos e perspectivas da gestão de documentos em cenários de transformações. **Acervo**, v. 28, n. 2, p. 19–50, 2015.

JARDIM, J. M. Políticas públicas arquivísticas: princípios, atores e processos. **Arquivo & Administração**, v. 5, n. 2, 2006.

JARDIM, J. M.; SILVA, S. C. A.; NHARRELUGA, R. S. Análise de políticas públicas: uma abordagem em direção às políticas públicas de informação. **Perspectivas em Ciência da Informação**, v. 14, p. 2–22, 2009.

JONES-EVANS, A. Data Protection—Issues and implications for records managers in the UK. **Records Management Journal**, 6(1), 33–40. <https://doi.org/10.1108/eb027084>.1996;

LE COADIC, Y.-F. Pandémie du Covid-19 et crise d'information: la réponse de la science de l'information. **Informação em Pauta**, Revista Informação em Pauta agora publica em fluxo contínuo. v. 6, n. especial, p. 9–23, dez. 2021.

LESCA, H., LESCO, E. **Gestion de l'information : Qualité de l'information et performances de l'entreprise**. EMS Editions, 2010.

LOWRY, J. Data, information and records: exploring definitions and relationships. In: Thurston, A. (Ed.). **A Matter of Trust: Building Integrity into Data, Statistics and Records to Support the Achievement of the Sustainable Development Goals**. University of London Press. 2020. <https://doi.org/10.14296/1220.9781912250356>

MACHADO, J. G. N. Um perfil de padrões de metadados de preservação para documentos arquivísticos audiovisuais. **Revista Brasileira de Preservação Digital**, v. 4, p. e023011, 12 fev. 2023. Disponível em: <https://econtents.bc.unicamp.br/inpec/index.php/rebpred/article/view/17991> . Acesso em: 31 ago. 2025.

MARCONI, M. A.; LAKATOS, E. M. **Metodologia Científica**. Rio de Janeiro: Grupo GEN, 2022. *E-book*. ISBN 9786559770670. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559770670/> Acesso em: 27 ago. 2023.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de Metodologia Científica**. São Paulo: Grupo GEN, 2023. *E-book*. ISBN 9788597026580. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597026580/> Acesso em: 25 ago. 2023.

MARTINS, P. L. Acesso à Informação: Um direito fundamental e instrumental. **Acervo**, v. 24, n. 1, p. 233–244, 14 fev. 2012. Disponível em:

<https://revista.an.gov.br/index.php/revistaacervo/article/view/381> . Acesso em: 3 set. 2025.

McGARRY, K. **O contexto dinâmico da informação: uma análise introdutória. In O contexto dinâmico da informação: uma análise introdutória** (pp. vi-206). 1999.

MENDES, L. S. **A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: UM MODELO DE APLICAÇÃO EM TRÊS NÍVEIS**. Thomson Reuters Brasil. 2019.

MINISTÉRIO DA ADMINISTRAÇÃO ESTATAL E FUNÇÃO PÚBLICA; MINISTERIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR. **INFORMAÇÃO SOBRE O DESENVOLVIMENTO DO SISTEMA NACIONAL DE GESTÃO DOCUMENTAL (e-SNGD)**. Maputo, julho de 2022.

NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. 1948.

NAÇÕES UNIDAS. **Objetivos de Desenvolvimento Sustentável**. 2015

NHARRELUGA, R. S. A DIMENSÃO INFORMACIONAL DO ESTADO MOÇAMBICANO À LUZ DOS PROGRAMAS GOVERNAMENTAIS. **PontodeAcesso**, v. 3, n. 1, p. 34–45, 2009.

NHARRELUGA, R. S. **O Estado e a construção da ordem arquivística em Moçambique (1975-2010)**. Orientador(res) Heymann, Luciana Quillet; Jardim, José Maria. Tese (Doutorado em História, Política e Bens Culturais). Escola de Ciências Sociais, FGV CPDOC, Rio de Janeiro, 2014. Disponível em: <http://bibliotecadigital.fgv.br:80/dspace/handle/10438/13303> Acesso em: 13 out. 2023.

NHARRELUGA, R. S. O projeto de Sistema Nacional de Arquivos em Moçambique e o desafio na estruturação da área. **Em Questão**, p. 132–159, 2021.

NHARRELUGA, R. S; SILVA, L. C. **ARQUIVOS: paradoxos e desafios frente à organização e acesso à informação**. Promédia, Maputo, 2002.

PAES, M. L. **Arquivo: teoria e prática**. Fundação Getúlio Vargas. 2004. *E-book*.

PAES, M. L. O Conselho Nacional de Arquivos, o Sistema Nacional de Arquivos e os Arquivos Municipais. **ÁGORA: Arquivologia em debate**, n. 8, p. 230–249, 1998.

PARLAMENTO EUROPEU. Regulamento (UE) 2016/679 (RGPD). Bruxelas, 2016.

PINHEIRO, L. V. R. Informação: esse obscuro objeto da Ciência da Informação. **Revista Morpheus – Estudos Interdisciplinares em Memória Social**, v. 3, n. 4, 2004.

PNUD (Programa das Nações Unidas para o Desenvolvimento). **Relatório de Desenvolvimento Humano 2023-24: Quebrando o impasse: Reimaginando a cooperação em um mundo polarizado**. Nova York. 2024

RHOADS, J. B. **La Función de la gestión de documentos y archivos en los sistemas nacionales de información: un estudio del RAMP** - UNESCO Digital Library. 1989. *E-book*. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000084735_spa . Acesso em: 24 out. 2024.

RABELLO, R. Informação institucionalizada e materializada como documento: caminhos e articulações conceituais. **Brazilian Journal of Information Science**, v. 13, n. 2, p. 5–25, 2019. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=6980028> . Acesso em: 1 set. 2025.

RODRIGUES, A M. L. A teoria dos arquivos e a gestão de documentos. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 11, n. 1, p. 102–117, abr. 2006.

RODRIGUES, A. M. L. **A construção de uma política nacional de arquivos: bases conceituais, ações e problemas**. Orientador: Renata Maria Abrantes Baracho Porto 2012. Tese (Doutorado em Ciência de Informação). Universidade Federal de Minas Gerais, Escola de Ciência da Informação. Belo Horizonte. 2012. Disponível em: <https://repositorio.ufmg.br/handle/1843/ECIC-9AHPQY> . Acesso em: 17 maio 2024.

RONCAGLIO, C.; SZVARÇA, D. R.; BOJANOSKI, S. F. Arquivos, gestão de documentos e informação. **Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação**. 2004. Disponível em: <http://repositorio.unb.br/handle/10482/913> . Acesso em: 10 dez. 2024.

ROUSSEAU, J. Y.; COUTURE, C. **Os fundamentos da disciplina Arquivística**. Publicações Dom Quixote, 1998, 356 p.

SADC. **Mozambique**. Disponível em: <https://www.sadc.int/pt-pt/node/12> . Acesso em: 10 jan. 2025.

SANTOS, H. M.; FLORES, D. O DOCUMENTO DIGITAL NO CONTEXTO DAS FUNÇÕES ARQUIVÍSTICAS. **Páginas a&b: arquivos e bibliotecas**, p. 165–177, 27 jul. 2016. Disponível em: <https://ojs.letras.up.pt/index.php/paginasueb/article/view/1477> . Acesso em: 3 set. 2025.

SAMPAIO, R. C.; LYCARIÃO, D. **Análise de conteúdo categorial: manual de aplicação**. Brasília: Enap, 2021. *E-book*.

SCHÄFER, M. B.; MARTINS, P. R.; SILVA, E. C. L. Gestão de documentos arquivísticos voltada à proteção de dados pessoais. **Acervo**, v. 37, n. 3, p. 1–23, 2024.

SCHELLENBERG, T. R. **Arquivos modernos: princípios e técnicas**. 6.ed. Rio de Janeiro: Editora FGV, 2006.

SCHWAITZER, L.; NASCIMENTO, N.; COSTA, A. Reflexões sobre a contribuição da gestão de documentos para programas de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD). **Acervo**, v. 34, n. 3, p. 1–17, 2021.

SEMIDÃO, R. A. M. DADOS, INFORMAÇÃO E CONHECIMENTO ENQUANTO ELEMENTOS DE COMPREENSÃO DO UNIVERSO CONCEITUAL DA CIÊNCIA DA INFORMAÇÃO: CONTRIBUIÇÕES TEÓRICAS. **CIÊNCIA DA INFORMAÇÃO**, 2014.

SEVERINO, A. J. **Metodologia do trabalho científico**. São Paulo: Cortez, 2017. *E-book*. ISBN 9788524925207. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788524925207/> Acesso em: 27 ago. 2023.

SHEPHERD, E.; YEO, G. **Managing records: a handbook of principles and practice**. Facet publishing. 2003. *E-book*.

SILVA, C. R.; GOBBI, B. C.; SIMÃO, A. A. O uso da análise de conteúdo como uma ferramenta para a pesquisa qualitativa: descrição e aplicação do método. **Organizações rurais & agroindustriais**, v. 7, n. 1, p. 70–81, 2005.

SILVA, E. P. DA. A temporalidade como constituinte do documento de arquivo: problematizando relações entre os contextos de geração, de tratamento e de uso dos documentos. **Revista Morpheus - Estudos Interdisciplinares em Memória Social**, v. 8, n. 14, 2012.

TEMBE, O. E.; WAETE, R. Z. A sociedade da informação e o profissional de informação em Moçambique. A questão social no novo milénio, 2004, pág. 256. Anais... *In: A QUESTÃO SOCIAL NO NOVO MILÉNIO*. 2004. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=4631664> . Acesso em: 14 nov. 2024

TRAÇA, J. L.; NEVES, L. **Data Protection in Mozambique: Inception Phase. African Data Privacy Laws**, 2016, p. 363-367.

TROITIÑO, S. Atribuir nomes a tipos, séries e unidades documentais: dialogando com Mariano Garcia Ruipérez. *In: Dar nome aos documentos: da teoria à prática*. São Paulo: Fundação FHC, 2015, p. 158-181. Disponível em: <http://arquivistica.fci.unb.br/au/atribuir-nomes-a-tipos-series-e-unidades-documentais-dialogando-com-mariano-garcia-ruiperez/> . Acesso em: 11 dez. 2024.

TROITIÑO, S. **Patrimônio documental e arquivologia: fundamentos para o reconhecimento e a organização de acervos permanentes**. Tese (livre-docência). Faculdade de Filosofia e Ciências, Universidade Estadual Paulista (Unesp), Marília, 2023.

VIEGAS, E. R. S.; SANTANA, C. F. P. A.; NODA, C. M. C. O conceito de política pública e suas ramificações: alguns apontamentos / The concept of public policy and its ramifications: some notes. **Brazilian Journal of Development**, v. 6, n. 7, p. 43415–43425, 5 jul. 2020. Disponível em: <https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/12662> . Acesso em: 4 set. 2025.

UNIÃO AFRICA. **Member States**. Disponível em: <https://au.int/pt/node/3678> . Acesso em: 10 jan. 2025.

UNIVERSIDADE EDUARDO MONDLANE. **Currículo do curso de Arquivística**. 2014.

VALENTIM, M. L. P. **Métodos qualitativos de pesquisa em Ciência da Informação**. São Paulo: Polis, 2005. *E-book*.

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

Legislação

AFRICA DO SUL. **Act n.º 4 of 2013, Protection of Personal information Act**. 2013. Disponível em: <https://www.dataguidance.com/legal-research/protection-personal-information-act-2013-act-4-2013> Acesso em: 27 jan. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 19 jan. 2025.

BRASIL. **Emenda Constitucional nº 115**. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm Acesso em: 16 nov. 2023.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm Acesso em: 27 jan. 2025.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. (a Lei do Cadastro Positivo). 2011a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm Acesso em: 27 jan. 2025.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. 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 (Lei de acesso à informação). 2011b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm Acesso em: 16 nov. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco civil da internet). 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 19 jan. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/l13709.htm Acesso em: 19 jan. 2025.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm Acesso em: 19 jan. 2025.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997.** Regula o direito de acesso a informações e disciplina o rito processual do habeas data. 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm Acesso em: 27 jan. 2025.

ESWATINI. **Act No.5 of 2022, Data Protection.** 2022. Disponível em: <https://www.dataguidance.com/jurisdictions/eswatini> Acesso em: 27 jan. 2025.

INTIC. **Proposta de Lei de Protecção de Dados.** 2024. Disponível em: <https://intic.gov.mz/propostas-de-lei-em-curso/>. Acesso em: 23 maio 2025.

MALAWI. **Act No. 3 of 2024, Data Protection.** 2024. Disponível em: <https://www.dataguidance.com/jurisdictions/malawi> . Acesso em: 27 jan. 2025.

MARROCOS. **Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data.** 2009. Disponível em: <https://www.dataguidance.com/jurisdictions/morocco> . Acesso em: 27 jan. 2025.

MOÇAMBIQUE. **Constituição da República de Moçambique.** 1990.

MOÇAMBIQUE. **Constituição da República de Moçambique.** Boletim da República, 1ª Série, n. 51, de 22 de dezembro de 2004.

MOÇAMBIQUE. **Constituição da República Popular de Moçambique.** 1975.

MOÇAMBIQUE. **Decreto n. 84/2018, de 26 de dezembro.** Aprova a revisão do Sistema Nacional de Arquivos do Estado (SNAE). Boletim da República, Maputo, n. 252, p. 2-35, 26 dez. 2018a. Série I.

MOÇAMBIQUE. **Decreto n.º 22/92 de 11 de novembro de 1992.** Cria o Instituto Nacional das Comunicações de Moçambique (INCM). Boletim da República, Maputo, n.º 46, 11 de nov. 1992b. Série I.

MOÇAMBIQUE. **Decreto n.º 30/2001, de 15 de outubro de 2001.** Aprova Normas de Funcionamento dos Serviços da Administração Pública. Boletim da República, Maputo., n. 41, 15 de out. 2001b. Série I.

MOÇAMBIQUE. **Decreto n.º 32/2001, de 6 de novembro.** Define a forma de organização e o modo de funcionamento do Instituto Nacional das Comunicações de Moçambique, e revoga o Decreto n.º 22/92. Boletim da República, Maputo, N.º 44, 6 de nov. 2001a, Série I.

MOÇAMBIQUE. **Decreto n.º 33/92, de 26 de outubro de 1992.** Institui o Sistema Nacional de Arquivos. Boletim da República, Maputo, de 26 de out. 1992a. Série I.

MOÇAMBIQUE. **Decreto n.º 35/2022, de 22 de julho.** Ajusta as atribuições, competências, autonomia, regime orçamental, organização e funcionamento do Instituto Nacional de Governo Electrónico, criado pelo Decreto n.º 61/2017, de 6 de novembro e revoga o Decreto n.º 61/2017, de 6 de novembro, com excepção do Art. 1 que cria o INAGE. Boletim da República, Maputo, n.º 141, 22 de jul. 2022. Série I.

MOÇAMBIQUE. **Decreto n.º 36 /2007, de 27 de agosto de 2007.** Aprova o Sistema Nacional de Arquivos do Estado. Boletim da República, Maputo,

MOÇAMBIQUE. **Decreto n.º 39/2021, de 17 de junho.** Aprovado o Estatuto Orgânico do Instituto Nacional das Comunicações de Moçambique, abreviadamente designado por INCM e revoga o Decreto n.º 32/2001, de 6 de novembro. Boletim da República, Maputo, N.º 116. 2021b, Série I.

MOÇAMBIQUE. **Decreto n.º 59/2019, de 3 de julho.** Cria o Sistema de Certificação Digital de Moçambique e aprova o Regulamento do Sistema de Certificação Digital de Moçambique. Boletim da República, Maputo, n.127, p. 2505-2516, 2019a. Série I.

MOÇAMBIQUE. **Decreto n.º 59/2023, 27 de outubro de 2023.** Aprova o Regulamento de Registo e Licenciamento de Provedores Intermediários de Serviços Electrónicos e de Operadores de Plataformas Digitais. 2023a.

MOÇAMBIQUE. **Decreto n.º 6/2000, de 4 de abril.** Cria a Unidade Técnica da Reforma do Sector Público – UTRESP. 2000b

MOÇAMBIQUE. **Decreto n.º 61/2017, 6 de novembro.** Cria o Instituto Nacional de Governo Electrónico. Boletim da República, Maputo, n.º 173, Série I.

MOÇAMBIQUE. **Decreto n.º 82/2020, de 10 de setembro.** Aprova o Regulamento do Uso do Domínio “.mz” Moçambique. Boletim da República, Maputo, Número 174, Série I.

MOÇAMBIQUE. **Decreto n.º 84/2018, de 26 de dezembro de 2018.** Aprova a revisão do Sistema Nacional de Arquivos do Estado. Boletim da República, Maputo, 2018a. Série I.

MOÇAMBIQUE. **Decreto n.º 9/2011, 4 de maio.** Cria o Instituto Nacional de Tecnologias de Informação e Comunicação, abreviadamente designado por INTIC, e extingue a UTICT, criada pelo Decreto n.º 50/2002, de 26 de dezembro. Boletim da República, Maputo, n.º 18. Série I

MOÇAMBIQUE. **Decreto n.º 98/2021, 31 de dezembro de 2021.** Aprova o Regulamento Interno da Comissão Interministerial da Reforma da Administração Pública, abreviadamente designada por CIRAP e revoga o Decreto n.º 73/2016, de 30 de dezembro. 2021a

MOÇAMBIQUE. **Decreto Presidencial n.º 2/2016, de 20 de maio de 2016.** Cria a Comissão Interministerial da Reforma da Administração Pública, abreviadamente designada por CIRAP e revoga o Decreto Presidencial n.º 2/2007, de 8 de março, e o Decreto Presidencial n.º 3/2015, de 20 de fevereiro.

MOÇAMBIQUE. **Decreto Presidencial n.º 5/2000 de 4 de abril de 2000.** Cria a Comissão Interministerial da Reforma do Sector Público – CIRESP. 2000a

MOÇAMBIQUE. **Diploma Ministerial n.º 34/2022, de 28 de março.** Aprova o Regulamento Interno do Instituto Nacional de Tecnologia de Informação e Comunicação IP. Boletim da República, Maputo, n.º 60, Série I.

MOÇAMBIQUE. **Diploma Ministerial n.º 35/2010, 16 de fevereiro de 2010.** Cria o Conselho Nacional de Arquivos.

MOÇAMBIQUE. **Diploma Ministerial n.º 36/2010, 16 de fevereiro de 2010.** Cria a Comissão Nacional de Avaliação de Documentos (CNAD)

Moçambique. **Diploma Ministerial n.º 45/2017, de 21 de junho.** Altera os artigos 3, 4 e 6 do Diploma Ministerial n.º 36/2010, de 16 de fevereiro, que estabelecem a composição, as funções e o apoio técnico administrativo à Comissão Nacional de Avaliação de Documentos. Boletim da República, Maputo, N.º 96. Série I. 2017a.

MOÇAMBIQUE. **Diploma Ministerial n.º 9/2017, 19 de janeiro.** Aprova o Regulamento Interno do Instituto Nacional de Tecnologia de Informação e Comunicação. Boletim da República, Maputo, N.º 11. Série I.

MOÇAMBIQUE. **Diploma Ministerial n.º 93/2018, 2 de novembro.** Aprova o Regulamento Interno do Instituto Nacional de Governo Electrónico. Boletim da República, Maputo, n.º 214, Série I.

MOÇAMBIQUE. **Estratégia de Governo Electrónico de Moçambique.** Maputo, 2006.

MOÇAMBIQUE. **Lei n. 12/79, de 12 de dezembro.** Protege o segredo do estado. Boletim da República, Maputo, n. 109, p. 330, 12 dez. 1979. Série I.

MOÇAMBIQUE. **Lei n. 3/2017, de 9 de janeiro.** Aprova a Lei de Transacções Electrónicas. Boletim da República, Maputo, n.5, 2017. Série I.

MOÇAMBIQUE. **Lei n. 34/2014, de 31 de dezembro.** Lei do direito à informação. Boletim da República, Maputo, n. 105, p. 33-37, 2014. Série I.

MOÇAMBIQUE. **Lei n.º 1/2018, de 12 de junho.** Lei da Revisão Pontual da Constituição da República de Moçambique. Boletim da República, Maputo, Maputo, n.º 115. 12 de jun. Série I.

MOÇAMBIQUE. **Lei n.º 1/2023, 17 de março de 2023.** Lei que estabelece o regime jurídico do Subsistema do Ensino Superior e revoga a Lei n.º 27/2009, de 29 de setembro.

MOÇAMBIQUE. **Lei n.º 12/79, de 12 de dezembro.** Visa proteger o segredo estatal relativamente a todos os documentos contendo dados e informações classificados. I Série - Número 109

MOÇAMBIQUE. **Lei n.º 13/2023, 25 de agosto.** Aprova Lei do Trabalho e revoga a Lei n.º 23/2007, de 1 de agosto. Boletim da República, Maputo, n.º 165, Série I. 2º suplemento.

MOÇAMBIQUE. **Lei n.º 24/2019, de 24 de dezembro de 2019.** Lei de Revisão do Código Penal. Boletim da República, Maputo, n. 248, p. 5699-5752, 2019. Série I.

MOÇAMBIQUE. **Lei n.º 34/2014, 31 de dezembro de 2014.** Lei do Direito à Informação. Boletim da República, Maputo, n.º 105. Série I.

MOÇAMBIQUE. **Lei n.º 4/2016, de 3 de junho.** Altera a Lei n.º 8/2004, de 21 de junho, Lei das Telecomunicações. Boletim da República, Maputo, N.º 66, Série I.

MOÇAMBIQUE. **Lei n.º 6/2022, 20 de junho de 2022.** Estabelece o Regime Jurídico de Identificação Civil e do Bilhete de Identidade do Cidadão Nacional

MOÇAMBIQUE. **Lei n.º 8/2024, de 7 de junho de 2024.** Estabelece o regime jurídico da tramitação electrónica de processos jurisdicionais e cria o Centro de Gestão de Tecnologias do Sector da Justiça, abreviadamente designado CGTSJ. Boletim da República, Maputo, n.º 111, Série I.

MOÇAMBIQUE. **Lei nº 18/2018, de 28 de dezembro.** Estabelece o regime jurídico do Sistema Nacional de Educação (SNE) na República de Moçambique e revoga a Lei nº 6/92 de 6 de maio, Lei do Sistema Nacional de Educação.

MOÇAMBIQUE. **Resolução n. 17/2018, de 12 de dezembro.** Aprova a Política para a Sociedade de Informação de Moçambique. Boletim da República, Maputo, n. 122, 2018. Série I.

MOÇAMBIQUE. **Resolução n. 46/2006, de 26 de dezembro.** Aprova a estratégia para a gestão de documentos e arquivos do estado (EGDAE). Boletim da República, Maputo, n. 51, p. 122-127, 26 dez. 2006. Série I.

MOÇAMBIQUE. **Resolução n.º 12/97, de 10 de Junho de 1997.** Aprova a Política Cultural e Estratégia de sua Implementação. 1997a

MOÇAMBIQUE. **Resolução n.º 2/2015, de 24 de junho.** Aprova o Estatuto Orgânico do Ministério da Administração Estatal e Função Pública. Boletim da República, Maputo, n.º 50, Série I.

MOÇAMBIQUE. **Resolução n.º 3/97, de 25 fevereiro de 1997.** Aprova a Política e Estratégias da Informação. 1997b

MOÇAMBIQUE. **Resolução n.º 5/2019, de 20 de junho de 2019.** Ratifica a Convenção da União Africana Sobre Cibersegurança e proteção de dados pessoais. 2019

MOÇAMBIQUE. **Resolução n.º 6/2024, de 6 de maio.** Aprova o Estatuto Orgânico do Instituto Nacional de Governo Electrónico, Instituto Público, abreviadamente designado por INAGE, IP. Boletim da República, Maputo, n.º 87, 2024b. Série I.

MOÇAMBIQUE. **Resolução n.º 69/2021, de 31 de dezembro de 2021.** Aprova a Política de Segurança Cibernética e Estratégia da sua Implementação. Boletim da República, Maputo, n. 253, p. 303-330, 2021. Série I

MOÇAMBIQUE. **Resolução n.º 8/2023, de 9 de maio de 2023.** Aprova o Estatuto Orgânico do Centro Nacional de Documentação e Informação de Moçambique e revoga o Estatuto Orgânico do Centro Nacional de Documentação e Informação de Moçambique, aprovado pela Resolução n.º 20/2017, de 15 de novembro.

MOÇAMBIQUE. **Resolução n.º 42/2015 de 31 de dezembro.** Cria as carreiras de Informação e Documentação e aprova os respetivos qualificadores profissionais.

NIGÉRIA. **Nigeria Data Protectio Act.** 2023. Disponível em: <https://www.dataguidance.com/legal-research/nigerian-data-protection-bill-2023>
Acesso em: 27 jan. 2025.

PORTUGAL. **Decreto n. 42:030, de 31 de dezembro de 1958.** Insere disposições relativas ao funcionamento do Arquivo Histórico de Moçambique e do Museu Histórico Militar da Fortaleza de Nossa Senhora da Conceição, de Lourenço Marques. Boletim Oficial, Série I, n. 52. Lourenço Marques. 1958.

PORTUGAL. **Decreto-Lei n. 41:472, de 23 de dezembro de 1957.** Insere disposições relativas ao ordenamento das actividades de natureza cultural e pedagógica exercidas no ultramar e do funcionamento dos respectivos órgãos. 1957.

PORTUGAL. **Diploma-Legislativo n. 635, de 19 de abril de 1939.** Define as funções do Arquivo Histórico de Moçambique. 1939.

TANZANIA. **Act No. 11 of 2022, Personal Data Protection Act.** 2022. Disponível em: <https://www.dataguidance.com/jurisdictions/tanzania> Acesso em: 27 jan. 2025.

ZAMBIA. **Act No. 3 of 2021, Data Protection.** 2021. Disponível em: <https://www.dataguidance.com/jurisdictions/zambia> Acesso em: 27 jan. 2025.

ZIMBABWE. **Act No. 5/2021, Data Protection.** 2021. Disponível em: <https://www.dataguidance.com/jurisdictions/zimbabwe> Acesso em: 27 jan. 2025.

APÊNDICES

Apêndice A – Legislação moçambicana de arquivos e de proteção de dados pessoais

Ano	Documento	Formato (I/E)	Local de recuperação
2024	1. Lei n.º 8/2024, de 7 de junho de 2024, estabelece o regime jurídico da tramitação electrónica de processos jurisdicionais e cria o Centro de Gestão de Tecnologias do Sector da Justiça, abreviadamente designado CGTSJ.	E	Gazettes.Africa
2024	2. Resolução n.º 6/2024, de 6 de maio	E	Gazettes.Africa
2023	3. Decreto n.º 59/2023, 27 de outubro de 2023, aprova o Regulamento de Registo e Licenciamento de Provedores Intermediários de Serviços Electrónicos e de Operadores de Plataformas Digitais.	E	Portal do INTIC
2023	4. Lei n.º 13/2023: Lei do Trabalho e revoga a Lei n.º 23/2007, de 1 de Agosto	E	Gazettes.Africa
2023	5. Resolução n.º 8/2023, de 9 de Maio de 2023. Aprova o Estatuto Orgânico do Centro Nacional de Documentação e Informação de Moçambique e revoga o Estatuto Orgânico do Centro Nacional de Documentação e Informação de Moçambique, aprovado pela Resolução n.º 20/2017, de 15 de novembro.	E	Gazettes.Africa
2023	6. Lei n.º 1/2023, 17 de março de 2023, Lei que estabelece o regime jurídico do Subsistema do Ensino Superior e revoga a Lei n.º 27/2009, de 29 de Setembro	E	Gazettes.Africa
2022	7. Decreto n.º 35/2022, de 22 de julho	E	Gazettes.Africa
2022	8. Lei n.º 6/2022, 20 de junho de 2022, estabelece o Regime Jurídico de Identificação Civil e do Bilhete de Identidade do Cidadão Nacional	E	Gazettes.Africa
2022	9. Diploma Ministerial n.º 34/2022, de 28 de março de 2022, aprova o Regulamento Interno do Instituto Nacional de	E	Portal do INTIC

	Tecnologia de Informação e Comunicação IP.		
2021	10. Resolução n.º 69/2021, de 31 de dezembro de 2021, aprova a Política de Segurança Cibernética e Estratégia da sua Implementação.	E	Portal do INTIC
2021	11. Decreto n.º 98/2021, 31 de dezembro de 2021. Aprova o Regulamento Interno da Comissão Interministerial da Reforma da Administração Pública, abreviadamente designada por CIRAP e revoga o Decreto n.º 73/2016, de 30 de Dezembro.	E	Gazettes.Africa
2021	12. Decreto n.º 39/2021, de 17 de Junho	E	Gazettes.Africa
2020	13. Decreto n.º 82/2020, de 10 de setembro, aprova o Regulamento do Uso do Domínio “.mz” Moçambique. Boletim da República, Maputo, Número 174, Série I.	E	Gazettes.Africa
2019	14. Decreto n.º 59/2019, de 1 de Dezembro, aprova Regulamento do Sistema de Certificação Digital de Moçambique,	E	Gazettes.Africa
2019	15. Lei n.º 24/2019, Lei de Revisão do Código Penal e revoga o Art. 2 do Decreto-Lei n.º 182/74, de 2 de Maio e o Código Penal aprovado pela Lei n.º 35/2014 de 31 de Dezembro.	E	Gazettes.Africa
2019	16. Decreto n.º 59/2019, de 3 de julho de 2019, cria o Sistema de Certificação Digital de Moçambique e aprova o Regulamento do Sistema de Certificação Digital de Moçambique.	E	Portal do INTIC
2019	17. Resolução n.º 5/2019, de 20 de junho de 2019, ratifica a Convenção da União Africana Sobre Cibersegurança e proteção de dados pessoais	E	Portal do INTIC
2018	18. Lei n.º 18/2018, de 28 de dezembro, estabelece o regime jurídico do Sistema Nacional de Educação (SNE) na República de Moçambique e revoga a Lei n.º 6/92 de 6 de maio,	E	Gazettes.Africa

	Lei do Sistema Nacional de Educação		
2018	19. Decreto n.º 84/2018, de 26 de dezembro de 2018, aprova a revisão do Sistema Nacional de Arquivos do Estado	E	Gazettes.Africa
2018	20. Diploma Ministerial n.º 93/2018, 2 de Novembro, aprova o Regulamento Interno do Instituto Nacional de Governo Electrónico	E	Gazettes.Africa
2018	21. Resolução n.º 17/2018, de 21 de junho de 2018, aprova a Política para a Sociedade da Informação de Moçambique	E	Portal do INTIC
2018	22. Lei n.º 1/2018, de 12 de junho, Lei da Revisão Pontual da Constituição da República de Moçambique	E	AR Fornecido pela
2018	23. Resolução n.º 15/2018, de 24 de Maio de 2018 que aprova o Código de Conduta do Funcionário e Agente do Estado.	E	Gazettes.Africa
2017	24. Decreto n.º 67/2017 de 1 de dezembro. Aprova o Regulamento do Quadro de Interoperabilidade.	E	Gazettes.Africa
217	25. Decreto n.º 61/2017, 6 de novembro Cria o INAGE	E	Gazettes.Africa
2017	26. Lei n.º 3/2017, 9 de janeiro de 2017, Lei de Transacções Electrónicas.	E	Portal do INTIC
2016	27. Lei n.º 4/2016, altera a lei das telecomunicações	E	Gazettes.Africa
2015	28. Resolução n.º 42/2015 de 31 de dezembro, cria as carreiras de Informação e Documentação e aprova os respetivos qualificadores profissionais.	E	Arquivo pessoal
2014	29. Lei n.º 34/2014, de 31 de dezembro, aprova a Lei do Direito à Informação	E	Portal do CEDIMO
2011	30. Decreto n.º 9/2011, de 4 de maio de 2011, cria o Instituto Nacional de Tecnologias de Informação e Comunicação, abreviadamente designado por INTIC.	E	Portal do INTIC

2010	31. Diploma Ministerial 35/2010, cria o Conselho Nacional de Arquivos	E	Portal do AHM
2007	32. Decreto n.º 36 /2007, de 27 de agosto de 2007, aprova o Sistema Nacional de Arquivos do Estado	I	Portal do CEDIMO
2006	33. Resolução n. 46/2006, de 26 de dezembro. Aprova a estratégia para a gestão de documentos e arquivos do estado (EGDAE)	E	Portal do CEDIMO
2004	34. Constituição da República de Moçambique	I	Arquivo pessoal
2003	35. Resolução n.º 2/2003, de 23 de Julho. Aprova o estatuto orgânico do CEDIMO	E	Gazettes.Africa
	36. Decreto n.º 32/2001, de 6 de novembro	E	Gazettes.Africa
2001	37. Decreto n.º30/2001, de 15 de outubro de 2001, aprova Normas de Funcionamento dos Serviços da Administração Pública	E	Portal do CEDIMO
2000	38. Decreto Presidencial n.º 5/2000 de 4 de Abril de 2000. Cria a Comissão Interministerial da Reforma do Sector Público – CIRESP	E	Gazettes.Africa
1997	39. Resolução n.º 12/97, de 10 de Junho de 1997. Aprova a Política Cultural e Estratégia de sua Implementação.	E	Gazettes.Africa
1997	40. Resolução n.º 3/97, de 25 fevereiro de 1997. Aprova a Política e Estratégias da Informação	E	Arquivo pessoal
1993	41. Decreto presidencial n.º 9/93, de 29 de dezembro de 1993, cria a Comissão Nacional para Implementação das Normas do Segredo do Estado—CPISE, e revoga o Decreto Presidencial no 5/79 de 29 de Março	E	Gazettes.Africa
1992	42. Decreto n.º 22/92 de 11 de novembro	E	Arquivo pessoal
1992	43. Decreto n.º 33/92, de 26 de outubro de 1992, institui o Sistema Nacional de Arquivos	E	Portal do CEDIMO

1990	44. Constituição da República de Moçambique	E	Arquivo pessoal
1979	45. Lei n.º 12/79, de aprova o Segredo de Estado	E	Arquivo pessoal
1975	46. Constituição da República Popular de Moçambique	E	Arquivo pessoal

Fonte: Elaborada pela autora

Apêndice B – Mapeamento de rol de matérias da Assembleia da República de Moçambique

	Ano	Referencia do livro/ brochura	Nr. Total de matérias arroladas	Matéria de interesse	Observação
	1992	Não recuperado	N/A	N/A	
	1993				
	1994				
	1995	IV Legislatura, III Sessão ordinária: 15 de setembro de 1995	24	N/A	
	1995	IV Legislatura, III Sessão ordinária: 17 de outubro de 1995	23	N/A	
	1996	IV Legislatura, V Sessão ordinária: 24 de Setembro de 1996	32	N/A	
	1996	IV Legislatura, V Sessão ordinária: 09 de outubro de 1996	34	N/A	
	1997	IV Legislatura, VI Sessão ordinária: 08 de Janeiro de 1997	22	N/A	
	1997	IV Legislatura, VII Sessão ordinária: 04 de novembro de 1997	Não apurado	N/A	
	1998	IV Legislatura, IX Sessão ordinária: Junho de 1998	12	N/A	
	1998	IV Legislatura, IX Sessão ordinária: 18 de Setembro de 1998	17	N/A	
	1998	IV Legislatura, IX Sessão ordinária: 07 de outubro de 1998	17	N/A	
	1998	IV Legislatura, IX Sessão ordinária: 20 de outubro de 1998	18	N/A	
	1998	IV Legislatura, X Sessão ordinária: 29 de Dezembro de 1998	17	N/A	
	1999	IV Legislatura, III Sessão extraordinária: 19 de Agosto de 1999	13	Proposta de lei das telecomunicações	Lei aprovada em

	1999	IV Legislatura, X Sessão ordinária: 26 de fevereiro de 1999	33	N/A	
	2000	V Legislatura, I Sessão ordinária: 14 de Janeiro de 2000	Não apurado		
	2000	V Legislatura, II Sessão Ordinária: 29 de fevereiro	Não apurado	N/A	
	2000	V Legislatura, III Sessão Ordinária: 13 de outubro	Não apurado	N/A	
	2001	V Legislatura, IV Sessão ordinária: 28 de fevereiro	Não apurado	N/A	
	2001	V Legislatura, V Sessão Ordinária: 16 de Outubro à 14 de Dezembro de 2001	35	N/A	
	2002	V Legislatura, VI Sessão: 01 de Março à 03 de Maio de 2002	32	N/A	
	2002	V Legislatura, VII Sessão: 16 de Outubro à 17 de Dezembro	27	Não apurado	
	2003	V Legislatura, VIII Sessão ordinária: 03 de Março à 06 de Maio de 2003	31	Proposta de Lei das Telecomunicações	
	2003	V Legislatura, IX Sessão ordinária: 16 de Outubro à 2ª de Dezembro de 2003	7	N/A	
	2004	V Legislatura, III Sessão extraordinária: 23 de Agosto à 01 de Setembro de 2004	7	N/A	
	2004	V Legislatura, IV Sessão extraordinária: 16 de Novembro de 2004	1	N/A	Adoptou e assinou a Constituição da República de 2004 (16 de novembro)
	2005	VI legislatura, I Sessão ordinária: 31 de Janeiro de 2005	Não apurado	N/A	Eleição e investidura do presidente da AR

	2005	VI legislatura, II Sessão ordinária: 01 de Março à 06 de Maio de 2005	18	N/A	
	2005	VI legislatura, III Sessão ordinária: 17 de Outubro à 8 de Novembro de 2005	27	Proposta de resolução que ratifica o protocolo da Carta Africana dos Direitos do Homem e dos Povos relativamente aos Direitos da Mulher em Africa	
	2006	VI legislatura, IV Sessão ordinária: 01 de Março à 05 de Maio de 2006	12	N/A	
	2006	VI legislatura, V Sessão ordinária: 16 de Outubro à	24	N/A	
	2007	VI legislatura, VI Sessão ordinária: 26 de Março à 01 de Abril de 2007	Não apurado	N/A	
	2007	VI legislatura, VII Sessão ordinária: 08 de outubro à 30 de Novembro de 2007	21	N/A	
	2008	VI legislatura, VIII Sessão ordinária: 10 de Março à 13 de Maio de 2008	19	N/A	
	2008	VI legislatura, IX Sessão ordinária: 02 de Outubro à 17 de Dezembro de 2008	40	N/A	
	2009	VI legislatura, X Sessão ordinária: 11 de Março à 20 de Maio de 2009	23	N/A	
	2010	VII Legislatura, I Sessão ordinária: 22 de Março à 24 de Maio de 2010	29	N/A	

	2010	VII Legislatura, II Sessão ordinária: 18 de outubro à 20 de dezembro de 2010	27	N/A	
	2011	VII legislatura, III Sessão ordinária: 09 de Março à 12 de Maio de 2011	20	N/A	
	2011	VII Legislatura, IV Sessão ordinária: 24 de outubro à 17 de dezembro	35	-Proposta de Lei Orgânica do Serviço de Informação e Segurança do estado (SISE)	
	2012	VII legislatura, V Sessão ordinária: 12 de março à 14 de Maio de 2012	28	-Proposta de Lei de Protecção de vítimas, denunciante e outros sujeitos processuais -Proposta de Lei que aprova o Código de ética do Servidor Público	
	2012	VII Legislatura, VI Sessão ordinária: 22 de outubro à 04 de novembro de 2012	52	Proposta de Resolução que ratifica a Carta africana sobre os Valores e Princípios da Função e Administração Públicas	
	2013	VII Legislatura, VII Sessão ordinária: 13 de março à 24 de Maio de 2013	47	Projecto de Lei do Direito à Informação	Aprovado em a 30 de dezembro de 2014
	2013	VII Legislatura, II Sessão extraordinária: 1 à 15 de Agosto de 2013	7	Projecto de Lei do Direito à Informação	Aprovado em a 30 de dezembro de 2014
	2013	VII Legislatura, VIII Sessão ordinária: 16 de Outubro à 20 de Dezembro	34	Projecto de Lei do Direito à Informação	Aprovado em a 30 de dezembro de 2014

	2014	VII Legislatura, IX Sessão ordinária: 19 de Fevereiro à 31 de Julho de 2014	30	Projecto de Lei do Direito à Informação	Aprovado em a 30 de dezembro de 2014
	2015	VIII Legislatura, I Sessão Ordinária: 31 de março à 05 de Abril de 2015	25	N/A	
	2015	VIII Legislatura, II Sessão Ordinária: 21 de Outubro à 23 de Dezembro	27	Proposta de Revisão da Lei n.º 8/2004, de 21 de Junho, Lei das Telecomunicações.	
	2016	VIII Legislatura, III Sessão Ordinária: 17 de fevereiro à	23	N/A	
	2016	VIII Legislatura, IV Sessão Ordinária: 19 de outubro à 20 de dezembro	33	Proposta de Lei de Transações Electronicas	Aprovada em 2017
	2017	VIII Legislatura, V Sessão Ordinária: 27 de fevereiro à 11 de maio	32	N/A	
	2017	VIII Legislatura, VI Sessão Ordinária: 23 de outubro	28	N/A	Digitalizado
	2018	VIII Legislatura, VII Sessão Ordinária: 28 de fevereiro à 24 de Maio de 2018	29	N/A	
	2018	VIII Legislatura, VIII Sessão Ordinária: 18 de outubro à 20 de Dezembro	32	N/A	
	2019	VIII Legislatura, IX Sessão Ordinária: 28 de fevereiro à 23 de maio	30	N/A	
	2019	Não apurado	Não apurado	N/A	COVID 19
	2020	IX Legislatura, I Sessão Ordinária: 25 de Março à 20 de Maio de 2020	20	N/A	

	2020	IX Legislatura, IV Sessão Extraordinária: 7 a 10 de agosto de 2020	2	N/A	
	2021	IX Legislatura, III sessão ordinária: 25 de fevereiro	26	N/A	
	2021	IX Legislatura, IV sessão ordinária: 20 de outubro	42	N/A	
	2022	IX Legislatura, V sessão ordinária: 28 de fevereiro à 13 de maio de 2022	24	Proposta de Lei que Estabelece o regime jurídico de Identificação Civil e do Bilhete de Identidade do Cidadão Nacional	
	2022	IX Legislatura, VI sessão ordinária: 06 de outubro à 15 de Dezembro de 2022	30	N/A	
	2023	IX Legislatura, VII sessão ordinária: 22 de fevereiro à 31 de Maio de 2023	29	Proposta de Lei da Autorização Legislativa para a Criação da Infra-estrutura Nacional de Dados Específicos de Moçambique (IDEMOC)	Aprovado pelo Decreto-Lei 2/2023 de 06 de novembro, Cria a Infra-estrutura de Dados Espaciais de Moçambique, abreviadamente designada por IDEMOC.
	2023	IX Legislatura, V sessão extraordinária: 03 à 07 de Agosto de 2023	4	N/A	
	2023	IX Legislatura, VI sessão extraordinária: 10 à 11 de Agosto de 2023	2	N/A	
	2023	IX Legislatura, VIII Sessão Ordinária: 19 de Outubro à 21 de Dezembro de 2023	23	N/A	

	2024	IX Legislatura, IX Sessão Ordinária: 22 de Fevereiro à 30 de Maio de 2024	24	Proposta de Lei de Tramitação Electronica dos processos Judiciais.	Aprovada pela Lei n.º 8/2024, de 7 de junho de 2024, que estabelece o regime jurídico da tramitação electrónica de processos jurisdicionais e cria o Centro de Gestão de Tecnologias do Sector da Justiça, abreviadamente designado CGTSJ.

ANEXOS

Anexo A – Proposta de Lei de Protecção de Dados Pessoais**Versão 1**

República de Moçambique
Assembleia da República

Lei nº /2023

de de

Lei de Protecção de Dados Pessoais

Havendo necessidade de garantir os direitos fundamentais, privacidade bem como salvaguardar os direitos dos cidadãos reconhecidos pela Declaração Universal dos Direitos do Homem e pela Carta Africana dos Direitos do Homem e dos Povo, na ordem jurídica interna, relativo à protecção dados pessoais, ao abrigo do disposto do número 1, do artigo 178, da Constituição da República, a Assembleia da República determina:

CAPÍTULO I**Disposições Gerais****Artigo 1****(Objecto)**

A presente Lei estabelece o regime jurídico aplicável ao tratamento e à livre circulação de dados pessoais nos meios físicos e digitais, que visa garantir o respeito pelas liberdades públicas e os direitos fundamentais das pessoas singulares.

Artigo 2

(Âmbito)

1. A presente lei aplica-se:

- a) a qualquer recolha, processamento, armazenamento ou utilização de dados pessoais realizados no território nacional, por uma pessoa singular, independentemente da natureza pública ou privada do responsável pelo tratamento;
- b) qualquer processamento automatizado ou não de dados contidos ou que devem figurar num ficheiro;
- c) aos dados processados nas embaixadas e consulados de que sejam titulares Moçambicanos residentes no estrangeiro.

2. A presente lei não se aplica:

- a) ao processamento de dados feitos por uma pessoa singular no quadro exclusivo das suas actividades pessoais ou domésticas, desde que esses dados não sejam destinados a uma comunicação sistemática a terceiros ou a difusão;
- b) as cópias temporárias feitas no quadro das actividades técnicas de transmissão e acesso a uma rede digital, com o objectivo de armazenamento automático, intermédio e temporário de dados, tendo como finalidade exclusiva permitir aos destinatários do serviço o melhor acesso possível as informações enviadas;
- c) processamento, recolha ou divulgação electrónica de dados pessoais para efeitos de jornalismo, expressão artística, literária ou quando decidido pelas autoridades competentes para a salvaguarda da segurança pública e defesa nacional;
- d) processamento de dados em que o fornecimento da informação ao titular seja impossível, envolva um esforço desproporcional, o seu registo ou divulgação seja permitido por lei e, ainda, nos casos de registo de dados para efeitos estatísticos históricos ou científicos.
- e) redes e sistemas de informação directamente relacionados com o comando e controlo das entidades que superintendem as áreas de Defesa e Segurança;

- f) redes e sistemas de informação que processem informação classificada conforme a legislação específica.

Artigo 3

(Definições)

Para efeitos da presente Lei, as definições dos termos e acrónimos, constam no glossário em anexo, que dela é parte integrante.

CAPÍTULO II

Princípios de Base que regem o Processamento de Dados Pessoais

Artigo 4

(Princípios)

Constituem princípios a presente Lei:

- a) **Princípio do Consentimento** é considerado legítimo quando o titular dos dados der o seu consentimento.
- b) **Princípio de Legalidade** é a recolha, o registo, o processamento, o armazenamento e a transmissão de dados pessoais devem ser feitos de uma forma lícita, justa e não fraudulenta;
- c) **Princípio da finalidade** é a realização de tratamento para propósitos legítimos específicos, explícitos e informados ao titular sem possibilidade de tratamento posterior de forma incompatível com esses fins;
- d) **Princípio de exactidão**. Os dados pessoais, devem ser exactos actualizados, tendo em conta os fins para os quais foram recolhidos e posteriormente processados;
- e) **Princípio de transparência** o tratamento de dados pessoais deve ser processado de forma transparente, em estrito respeito pelo princípio de reserva

da vida privada, bem como pelos direitos, liberdades e garantias públicas fundamentais previstos na constituição da República de Moçambique e na presente lei.

- f) **Princípio de Confidencialidade e de Segurança** os dados pessoais devem ser processados num ambiente confidencial e serem protegidos, principalmente quando o processamento envolve transmissão de dados através de uma rede.
- g) **Princípio da proporcionalidade** os dados Pessoais sujeitos a tratamentos devem ser pertinentes, adequados e não excessivos relativamente a finalidade que legitimaram a sua recolha e tratamento.
- h) **Princípio da duração do período de conservação** os dados pessoais devem ser conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário a prossecução das finalidades que originaram a sua recolha ou tratamento, devendo ser posteriormente eliminados ou tornados anónimos. A conservação de dados pessoais para fins históricos, estatísticos, de investigação criminal e segurança nacional pode ser autorizada pela agência Nacional de Protecção de Dados por período superior mediante requerimento do responsável pelo tratamento.
- i) **Princípio da legalidade** a recolha, o registo, o processamento, o armazenamento e a transmissão de dados pessoais devem ser feitos de uma forma lícita, justa e não fraudulenta.
- j) **Princípio de exactidão** os dados recolhidos devem ser exactos e actualizados, tendo em conta os fins para os quais foram recolhidos e posteriormente processados e possam ser apagados ou rectificados.
- k) **Princípio da transparência** o tratamento de dados pessoais deve processar-se de forma transparente, em estrito respeito pelo princípio de reserva da vida privada, bem como pelos direitos, liberdades e garantias públicas fundamentais previstos na constituição da República de Moçambique e na presente lei. Para efeito de disposto no número anterior, os dados pessoais devem ser conservados de forma a permitir o exercício aos seus titulares de acesso, informação, rectificação, cancelamento e oposição, conforme na presente lei.

- l) Princípio da licitude** o tratamento de dados pessoais deve ser efectuado de forma lícita e leal, com respeito pelo princípio da boa-fé. O tratamento de dados pessoais que conduza a uma discriminação arbitrária e ilícita em relação ao seu titular é considerado ao princípio da boa-fé.
- m) Princípio da proporcionalidade** os dados Pessoais sujeitos a tratamentos devem ser pertinentes, adequados e não excessivos relativamente a finalidade que legitimaram a sua recolha e tratamento.
- n) Princípio de livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre integralidade de seus dados pessoais;
- o) Princípio de qualidade de Dados:** garantia, aos titulares, de exactidão, clareza, relevância e actualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento
- p) Princípio Responsabilidade e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de protecção de Dados pessoais e, inclusive, da eficácia dessas medidas.

Capítulo III

Autoridade Nacional de Protecção de Dados

Artigo 5

(Natureza)

1. A Autoridade Nacional de Protecção de Dados é um órgão de Aparelho do Estado, independente dotada de autonomia administrativa, financeira e patrimonial e com poderes de autoridade.
2. A Autoridade Nacional de Protecção de Dados controla e fiscaliza o cumprimento da presente Lei, bem como das demais disposições legais e regulamentares em matéria de protecção de dados pessoais, a fim de defender os

direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais.

3. A Autoridade Nacional de Protecção de Dados age com independência na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos pela presente lei.
4. Os membros de uma Autoridade Nacional de Protecção de Dados não devem ser membros do Governo, nem pessoas que exercem funções executivas e possuem acções em empresas no sector de Tecnologias de Informação; não podendo, durante o seu mandato, desempenhar outra actividade, remunerada ou não, com excepção da actividade de docência no ensino superior e de investigação.

Artigo 6

(Composição)

A Autoridade Nacional de Protecção de Dados tem a seguinte composição:

- a) três cidadãos designados pelo Presidente da República, dos quais nomeia o Presidente da Autoridade;
 - b) três cidadãos eleitos pela Assembleia da República;
 - c) dois magistrados, sendo um magistrado judicial, designado pelo Conselho Superior da Magistratura, e um magistrado do Ministério Público, designado pelo Conselho Superior do Ministério Público.
1. O mandato dos membros da ANPD é de cinco anos, renovável duas vezes, e cessa com posse dos novos membros.
 2. A designação dos membros da ANPD consta de lista publicada no Boletim da República.
 3. Os membros da ANPD tomam posse perante o Presidente da República nos 10 dias seguintes à publicação da lista referida no número anterior.

Artigo 7

(Competências)

Compete a Autoridade Nacional de Protecção de Dados:

- a) zelar pela protecção de dados pessoais nos termos da legislação aplicável;
- b) elaborar diretrizes para Política Nacional de Protecção de Dados Pessoais e da Privacidade;
- c) fiscalizar, auditar e aplicar sanções em caso de tratamento de dados realizados em incumprimento da legislação aplicável;
- d) receber reclamações, petições e as queixas relativas ao processamento de dados pessoais e informar os seus actores sobre os resultados inerentes a esta matéria;
- e) Comunicar às autoridades competentes as infracções penais das quais tiver conhecimento;
- f) autorizar o processamento de ficheiros, em determinados casos, especialmente os ficheiros sensíveis;
- g) promover o conhecimento dos instrumentos normativas e da cultura da protecção de dados pessoais e das medidas de segurança;
- h) promover e elaborar os estudos sobre as práticas Nacionais e Internacionais de protecção de dados pessoais e privacidade;
- i) dispor sobre as formas de publicidade das operações de tratamento de dados pessoais respeitados os segredos comerciais industriais;
- j) realizar auditorias ou determinar a sua realização no âmbito da actividade de fiscalização de que trata o artigo
- k) receber as formalidades previas para o processamento de dados pessoais;
- l) autorizar a transferência transfronteiriça de dados pessoais;
- m) Arrecadar e aplicar suas receitas e publicar no relatório de actividades
- n) Estabelecer mecanismos de cooperação com as autoridades de protecção de dados pessoais;
- o) Participar em negociações internacionais em matéria de protecção de dados pessoais;
- p) Informar de imediato, a autoridade judiciária sobre determinados tipos de infrações de que tiver conhecimento
- q) elaborar relatórios anuais de actividades.

Capítulo IV

Encarregados de Protecção de Dados

Artigo 8

(Encarregados de Protecção de Dados)

1. O encarregado de protecção de dados é a pessoa indicada pelo controlador e operador para actuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Protecção de Dados (ANPD).
2. O encarregado de protecção de dados é designado com base nos requisitos previstos na presente Lei, não carecendo de certificação profissional para efeito. Independentemente da natureza da sua relação jurídica, o encarregado de protecção de dados exerce a sua função com autonomia técnica perante a entidade responsável pelo tratamento ou subcontratante.
 - a) O controlador deve indicar encarregado pelo tratamento de dados pessoais;
 - b) A identidade e as informações de contacto de encarregado devem ser divulgadas publicamente, de forma clara e objectiva, preferencialmente no sítio electrónico do controlador;
3. Aceitar as actividades de controlador do encarregado consiste em:
 - a) aceitar reclamação e comunicações dos titulares, prestar esclarecimento e adoptar providencias;
 - b) orientar os funcionários e os controladores da entidade a respeito das práticas a serem tomadas em relação a protecção de dados pessoais; e
 - c) Executar as demais atribuições determinadas pelo controlador

Artigo 9

(Dever de sigilo e confidencialidade)

1. O encarregado de protecção de dados está obrigado a um dever de sigilo profissional em tudo o que diga respeito ao exercício dessas funções, que se mantém após o termo das funções que lhes deram origem.
2. O encarregado de protecção de dados, bem como os responsáveis pelo tratamento de dados, incluindo os subcontratantes, e todas as pessoas que intervenham em qualquer operação, de tratamento de dados, estão obrigados a um dever de confidencialidade que acresce aos deveres de sigilo profissional previsto na lei.

Artigo 10

(Funções do encarregado de protecção de dados)

1. São funções do encarregado de protecção de dados:
 - a) Assegurar a realização de auditorias, quer periódicas, quer não programadas;
 - b) Sensibilizar os utilizadores para a importância da detecção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança;
 - c) Assegurar as relações com os titulares dos dados nas matérias abrangidas pela legislação nacional em matéria de protecção de dados.

Artigo 11

(Encarregados de protecção de dados em entidades públicas)

1. **É obrigatória a designação de encarregados de protecção de dados nas entidades públicas, de acordo com o disposto nos números seguintes.**
2. **Para efeitos do número anterior, entende-se por entidades públicas:**
 - a) **O Estado;**
 - b) **As regiões autónomas;**
 - c) **As autarquias locais e as entidades supranacionais previstas na lei;**
 - d) **As entidades administrativas independentes e o Banco de Moçambique;**
 - e) **Os institutos públicos;**
 - f) **As instituições de ensino superior públicas, independentemente da sua natureza;**
 - g) **As empresas do sector empresarial do Estado e dos sectores empresariais regionais e locais;**
 - h) **As associações públicas.**
3. **Independentemente de quem seja responsável pelo tratamento, existe pelo menos um encarregado de protecção de dados:**
 - a) **Por cada ministério ou área governativa, no caso do Estado, sendo designado pelo respectivo ministro, com faculdade de delegação em qualquer secretário de Estado que o coadjuvar;**
 - b) **Por cada secretaria regional, no caso das regiões autónomas, sendo designado pelo respectivo secretário regional, com faculdade de delegação em dirigente superior de 1.º grau;**
 - c) **Por cada município, sendo designado pela câmara municipal, com faculdade de delegação no presidente e subdelegação em qualquer vereador;**
4. **Por cada entidade, no caso das demais entidades referidas no número anterior, sendo designada pelo respectivo órgão executivo, de administração ou gestão, com faculdade de delegação no respectivo presidente.**

Artigo 12

(Encarregado de Protecção de Dados Entidades Privadas)

1. **O responsável pelo tratamento e o subcontratante designam um encarregado de protecção de dados sempre que a actividade privada desenvolvida, a título principal, implique:**
 - a) **operações de tratamento que, devido à sua natureza, âmbito e ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou**
 - b) **Operações de tratamento em grande escala das categorias especiais de dados nos termos do artigo 9.º do RGPD, ou de dados pessoais relacionados com condenações penais e contra ordem nacionais nos termos do artigo 10.º do RGPD**

Capítulo IV

Requisitos para o tratamento de dados pessoais

Artigo 13

(Requisitos Gerais)

1. Salvo disposição legal em contrário, o tratamento de dados pessoais só pode ser efectuada verificadas as seguintes circunstâncias:
 - a) Consentimento inequívoco e expresso do seu titular;
 - b) Pela notificação da Autoridade Nacional de Protecção de Dados
2. Sem prejuízo do direito à informação, o consentimento do titular dos dados é dispensável quando o tratamento for necessário para:
 - a) cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito;
 - b) protecção de interesses vitais do titular dos dados, pelo seu representante legal se aquele estiver física ou legalmente incapaz de dar o seu consentimento;
 - c) execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

- d) prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados.
- e) execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contracto ou declaração negocial efectuadas a seu pedido;
- f) Para a realização de estudos por órgãos competentes garantida, sempre que possível, a anonimização dos dados pessoais;

Artigo 14

(Requisitos de tratamento de dados sensíveis saúde e da vida sexual)

1. É proibido o tratamento de dados pessoais que revelam origem racial, étnica, filiação, ideológica, políticas, crenças religiosas ou convicções filosóficas, filiação em associação política ou sindical, vida sexual, informação genética ou, de uma forma geral, as informações relativas ao estado de saúde do titular dos dados.
2. A proibição estabelecida no número 1 do presente artigo, não se aplica para as categorias de processamento que se seguem, quando:
 - a) o tratamento dos dados a serem efectuados com o consentimento inequívoco, expresso e escrito do seu titular ou do seu representante legal;
 - b) o processamento for necessário para o cumprimento de uma obrigação legal ou regulamentar ao qual o sujeito titular dos dados está vinculado;
 - c) Autorização da Agencia Nacional de Protecção de Dados Pessoas quando for por motivo de interesse público.

- d) O processamento de dados pessoais for necessário para proteger os interesses vitais do titular dos dados ou de uma outra pessoa, se o sujeito titular dos dados estiver física ou juridicamente incapacitado para dar o seu consentimento.
- e) um processo judicial ou uma investigação penal tiver sido iniciado;
- f) o processamento for necessário no interesse público, especialmente para fins históricos, artísticos, estatísticos, científicos, jornalísticos e de investigação;
- g) o processamento de dados for necessário para execução de uma missão no interesse público;
- h) O tratamento dos dados referente a saúde e a vida sexual incluindo os dados genéticos pode ser efectuados quando for necessário para fins de medicina preventiva, de diagnósticos médicos de tratamentos médicos que seja efectuado por um profissional de saúde sujeito a segredo profissional.

Artigo 15

(Dados de Crianças e Adolescentes)

1. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
2. O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
3. No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados colectados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

4. Poderão ser colectados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a colecta for necessária para contactar os pais ou o responsável legal, utilizada uma única vez e sem armazenamento, ou para sua protecção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
5. Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras actividades ao fornecimento de informações pessoais além das estritamente necessárias à actividade.
6. O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
7. As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Artigo 16

(Tratamento para fins de interesse público)

O tratamento para fins de tratamento interesse pública deve respeitar o princípio da minimização dos dados e incluir a anonimização ou a pseudominizacão dos mesmos sempre que os visados possam ser atingidos por uma destas vias.

Artigo 17

(Requisitos específicos para o tratamento de dados relativos a actividades ilícitas, crimes e contravenções)

1. O tratamento de dados pessoais relativos a pessoas suspeitas de actividades ilícitas, infracções penais, contravenções e de aplicação de penas, medidas de segurança, multas e sanções acessórias, os quais são considerados dados sensíveis, só pode ser efectuado por autoridade pública, verificadas as seguintes circunstâncias:
 - a) disposição legal que permita tal tratamento por autoridades com competência específica, em respeito das normas procedimentais e de protecção de dados previstas por lei e mediante prévio parecer da Autoridade de Protecção de Dados; ou
 - b) Autorização da Autoridade de Protecção de Dados, a qual só pode ser concedida quando tal tratamento for necessário à execução de finalidades legítimas do seu responsável e sejam observadas as normas de protecção de dados e de segurança da informação.
2. Sem prejuízo do disposto em legislação específica, o tratamento de dados pessoais para fins de investigação policial deve limitar-se ao necessário para o cumprimento de finalidades de prevenção geral e especial ou repressão de uma infracção determinada, nos termos da presente lei e de legislação específica (rever).

Artigo 18

(Requisitos específicos para o tratamento de dados em sistemas de videovigilância e outros meios de controlo electrónica)

1. O tratamento de dados pessoais no âmbito da instalação de sistemas de videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas, incluindo os sistemas de vigilância electrónica, está sujeita ao disposto ao artigo 4.º da presente Lei.

2. O responsável pelo tratamento de dados pessoais deve disponibilizar, nos locais com sistemas de videovigilância, informação relativa à existência dos mesmos, à captação de som e de imagem e o nome do responsável pelo tratamento dos dados, seu endereço, número de telefone e e-mail.
3. As regras aplicáveis à instalação de sistemas de videovigilância e ao tratamento de dados recolhidos neste âmbito são objecto de regulamentação específica.

(Capítulo V)

(Direitos de Titular dos dados)

Artigo 19

(Direito de informação)

1. Sem prejuízo do disposto em outros artigos da presente lei, o responsável pelo tratamento deve disponibilizar aos titulares dos dados pelo menos a seguinte informação:
 - a) a identidade e endereço do responsável pelo tratamento
 - b) as finalidades do tratamento e a criação de um ficheiro com a referida finalidade;
 - c) os destinatários ou categorias de destinatários dos dados;
 - d) o carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências de não responder;
 - e) existência e condições do direito de acesso e de rectificação, actualização, eliminação e oposição;
 - f) as consequências da recolha dos dados sem o consentimento do titular ou, em caso de incapacidade deste, pelo seu representante legal;
 - g) outras informações necessárias para garantir o tratamento lícito de tais dados pessoais.

2. Quando os dados pessoais sejam recolhidos directamente do titular dos dados, a informação deve ser prestada no momento da recolha, excepto se já tiver sido prestada em momento prévio.
3. Caso os dados pessoais não sejam recolhidos directamente do titular dos dados, o responsável pelo tratamento deve prestar-lhe a informação referida no momento do registo dos dados ou o mais tardar no prazo de trinta dias após a sua recolha, salvo se dele já for conhecida.
4. A informação deve ser prestada de maneira clara, precisa e objectiva em particular quando tenha como destinatários menores e pessoas com necessidades especiais.
5. A obrigação de informação pode ser dispensada mediante disposição legal ou deliberação da Agência de Protecção de Dados, nos seguintes casos:
 - a) por motivos de segurança do Estado e prevenção ou investigação criminal;
 - b) quando a prestação de informação ao titular dos dados se revelar impossível ou implicar esforços desproporcionados, nomeadamente nos casos de tratamento de dados com finalidades estatísticas, históricas ou de investigação científica; ou
 - c) quando a lei determinar expressamente o registo dos dados ou a sua divulgação.
6. A obrigação de informação, nos termos do número anterior, não se aplica ao tratamento de dados efectuado para fins exclusivamente jornalísticos ou de expressão artística ou literária.
7. No caso de recolha de dados em redes abertas, considera-se prestado o direito de informação através da publicação e disponibilização de políticas de privacidade que sejam de fácil acesso e incluam:
 - a) as informações descritas no n.º 1 do presente artigo;
 - b) a informação de que os seus dados pessoais podem circular na rede sem condições de segurança, correndo o risco de serem vistos e utilizados por terceiros não autorizados.

Artigo 20
(Direito de acesso)

1. O titular dos dados tem o direito de obter do responsável pelo tratamento, livremente, sem restrições, demoras ou custos excessivos, informação sobre se são ou não tratados dados que lhe digam respeito, as finalidades desse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados.
2. O responsável pelo tratamento deve ainda comunicar ao titular os dados específicos objecto de tratamento, bem como quaisquer informações disponíveis sobre a origem desses dados.
3. Sem prejuízo do disposto em legislação específica, no tratamento de dados pessoais relativos à segurança do Estado, à prevenção ou investigação criminal e ao segredo de justiça, o direito de acesso é exercido através da Agência de Protecção de Dados.
4. No tratamento de dados pessoais efectuado para fins exclusivamente jornalísticos, o direito de acesso é exercido pela Agência de Protecção de Dados com salvaguarda das normas constitucionais aplicáveis, designadamente as que garantem a liberdade de expressão e a liberdade de imprensa.
5. Nos casos previstos nos n.ºs 3 e 4, se o acesso aos dados pelo seu titular puder prejudicar a segurança do Estado, a prevenção ou a investigação criminal, o segredo de justiça ou ainda a liberdade de expressão e a liberdade de imprensa, a Agência de Protecção de Dados limita-se a informar o titular dos dados das diligências efectuadas.
6. lei pode restringir o direito de acesso verificadas as seguintes circunstâncias:
 - a) os dados não serem utilizados para tomar medidas ou decisões relativamente a pessoas determinadas, mas exclusivamente para fins de investigação científica ou conservados sob forma de dados pessoais durante um período que não exceda o necessário à finalidade exclusiva de elaborar estatísticas;

- b) não existir qualquer perigo de violação dos direitos, liberdades e garantias fundamentais do titular dos dados pessoais, designadamente do direito à reserva de intimidade da vida privada.
7. O direito de acesso do titular dos dados à informação sobre os dados de saúde e vida sexual, incluindo os dados genéticos, é exercido por intermédio de médico escolhido pelo titular dos dados ou de seu representante legítimo.

Artigo 21

(Direito de oposição)

1. O titular dos dados tem o direito de:
- a) salvo disposição legal em contrário, e pelo menos nas situações referidas acima se opor em qualquer altura a que os dados que lhe digam respeito sejam objecto de tratamento quando existam razões ponderosas e legítimas relacionadas com a sua situação particular, devendo neste caso o responsável excluir do tratamento tais dados;
 - b) se opor ao tratamento dos seus dados em outras circunstâncias previstas na presente lei e em outra legislação específica.

Artigo 22

(Direito de rectificação, actualização e eliminação)

1. É assegurado ao titular dos dados pessoais os direitos de rectificação, actualização ou eliminação dos seus dados pessoais cujo tratamento não cumpra o disposto na presente lei, nomeadamente devido ao carácter incompleto ou inexacto desses dados.
2. O responsável pelo tratamento é obrigado, nos termos da presente lei e legislação especial, a assegurar o direito de rectificação, actualização e eliminação de dados num período de sessenta dias úteis.
3. Se os dados objecto de rectificação, actualização ou eliminação tiverem sido previamente comunicados a destinatário, o responsável pelo tratamento fica

obrigado a notificar a este tal rectificação, actualização ou eliminação, salvo se isso for comprovadamente impossível, devendo o destinatário agir em conformidade.

4. No caso previsto no número anterior, o destinatário que tratar os dados para os seus próprios fins ou para fins de um terceiro pode não proceder à eliminação dos dados, devendo neste caso tal destinatário informar o titular dos dados desta situação e confirmar se este pretende também rectificar, actualizar ou eliminar os seus dados dos ficheiros respectivos.
5. O responsável pelo tratamento deve, contudo, bloquear e/ou conservar os dados pessoais nos seguintes casos:
 - a) disposição legal ou ordem de autoridade competente que obrigue o responsável pelo tratamento a bloquear e/ou conservar os dados por um determinado período de tempo;
 - b) se o bloqueamento e/ou conservação dos dados for necessário à prossecução de um interesse legítimo do responsável pelo tratamento, designadamente para o exercício de um direito ou para o cumprimento de obrigações legais;
 - c) se os dados estiverem a ser utilizados para efeitos de investigação criminal;
 - d) se os dados se tratarem de dados relativos ao crédito e à solvabilidade, enquanto a situação creditícia do titular não estiver regularizada.

Artigo 23

(Direito dos incapazes)

Quando os titulares dos dados sejam incapazes, os direitos previstos nos artigos anteriores são exercidos por intermédio dos respectivos representantes legais.

Artigo 24

(Direitos do titular dos dados em casos especiais)

Os direitos de informação, de acesso, de rectificação, de apagamento e de limitação do tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, detenção, investigação ou repressão de infracções penais ou de execução de sanções

penais, incluindo a salvaguarda e a prevenção de ameaças a segurança pública são exercidos nos termos da lei processual pela, demais legislações aplicáveis e da presente Lei.

Transferência Internacional de Dados Pessoais

Artigo 25

(Transferência de Dados para Países que assegurem um nível de Protecção adequado)

1. A transferência internacional de dados para países que assegurem nível de Protecção adequado esta sujeita a notificação à Autoridade Nacional de Protecção de Dados.
2. Entende-se que um país assegura um nível de protecção adequado quando o mesmo garante, no mínimo, um nível de protecção igual ao estabelecimento presente na lei.
3. Cabe à Autoridade Nacional de Protecção de Dados decidir se um estado assegura um nível de protecção adequado, mediante a emissão de parecer a este respeito.
4. A adequação do nível de protecção de dados num Estado é apreciada pela Autoridade Nacional de Protecção de Dados em função de todas as circunstâncias que rodeiam a transferência ou o conjunto de transferência de dados, atendendo em especial à natureza dos dados, à finalidade e à duração do tratamento ou tratamentos projectados, aos países de destino final e às regras de direito, gerais ou sectoriais em vigor no Estado em causa, incluindo as regras profissionais e as medidas de segurança que são respeitadas nesse Estado.

Artigo 26

(Avaliações prévias de impacto)

Artigo 27

Dever de Colaboração

Capítulo VI

Transferência de dados pessoais para local situado fora da República de Moçambique

Artigo 28

(Transferência de Dados para Países que não asseguram um nível de Protecção Adequado)

1. A transferência internacional de dados para um país que não assegure um nível de protecção adequado está sujeita a autorização da Autoridade Nacional de Protecção de Dados, a qual só pode ser concedida verificada uma das seguintes circunstâncias constantes de legislação específica:
 - a) se o titular de dados tiver dado o seu consentimento inequívoco, expresso e escrito;
 - b) se a transferência internacional de dados decorrer da aplicação de tratados ou acordos internacionais em que a República de Moçambique seja parte;
 - c) se a transferência de dados tiver como finalidade exclusiva a resposta ou pedido de ajuda humanitária;
 - d) se a transferência de dados for necessária para a execução de um contrato entre titulares de dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido titular dos dados;

- e) se a transferência dos dados for necessária para a execução ou celebração de um contrato do titular dos dados, entre o responsável pelo tratamento e um terceiro;
 - f) se a transferência de dados for necessária ou legalmente exigida para a protecção de um interesse público importante ou para a declaração, o exercício ou a defesa de um direito num processo judicial;
 - g) se a transferência de dados for necessária para proteger os interesses vitais do titular dos dados, ou para a prevenção, ou diagnóstico ou tratamento médico e o titular estiver física ou legalmente incapaz de dar o seu consentimento;
 - h) se a transferência de dados for realizada a partir de uma fonte acessível publicamente;
 - i) se o destinatário dos dados assegurar contratualmente, perante o responsável pelo tratamento, o nível de protecção adequado aos dados transferidos.
2. Incumbe à Autoridade Nacional de Protecção de Dados determinar as condições específicas que devem constar no contrato referido na alínea *i)* do nº anterior.
3. No caso de transferência internacional de dados entre empresas do mesmo grupo empresarial, a garantia de cumprimento de um nível de protecção adequado pode ser alcançada através da adopção de regras internas relativas à privacidade e protecção de dados cujo cumprimento seja obrigatório.

Capítulo VII

Notificação e autorização

Formalidades Para Notificação E Obtenção E Autorização Junto da Autoridade Nacional de Protecção de Dados

Artigo 29

(Obrigação de Notificação ou de Obtenção de Autorização)

1. Sem prejuízo do disposto na presente Lei, o tratamento de dados está sujeito a notificação prévia à Autoridade Nacional de Protecção de Dados ou autorização desta.
2. Se for necessária mera notificação, a Autoridade Nacional de Protecção de Dados deve pronunciar-se sobre o pedido do responsável pelo tratamento no prazo de 30 dias após a sua recepção, findo o qual se entende que o tratamento foi devidamente notificado.
3. A Autoridade Nacional de Protecção de Dados pode autorizar a simplificação ou isenção da notificação para determinadas categorias de tratamento que, atendendo a especialidade dos dados, não sejam susceptíveis de por em causa os direitos garantias e liberdades fundamentais dos titulares dos dados e tendo em conta pós créditos de celeridade, economia e eficiência.
4. A autorização de isenção deve, entre outros aspectos, especificar as finalidades do tratamento, os dados ou categorias de dados a tratar a categoria ou categorias de titulares dos dados, os destinatários ou categorias de destinatários a quem podem ser comunicados os dados e o período de conservação dos dados.
5. Estão isentos de notificação os tratamentos cuja única finalidade seja a manutenção de registos que se destinem a informação do público que possam ser consultadas pelo público em geral ou por qualquer pessoa que provar um interesse legítimo.
6. É dispensada a obtenção de autorização da Autoridade Nacional de Protecção de Dados se o tratamento decorrer de diploma legal, bastando neste caso, proceder a mera notificação, salvo se indicado em contrário em legislação específica.

(Conteúdo das Notificações e dos Pedido de Autorização)

As notificações e pedidos de autorização remetidos à Autoridade Nacional de Protecção de Dados devem conter as seguintes informações:

- a) o nome e endereço do responsável pelo tratamento e, se for o caso, do seu representante;
- b) finalidade do tratamento;

- c) a descrição da ou das categorias de titulares dos dados ou categorias de dados pessoais que lhes respeitem;
- d) destinatários ou categorias de destinatários a quem os dados podem ser comunicados e em que condições;
- e) entidade encarregada do processamento da informação, se não for o próprio responsável do tratamento;
- f) eventuais interconexões de tratamento de dados pessoais;
- g) tempo de conservação dos dados pessoais;
- h) forma e condições como os titulares dos dados podem exercer seus direitos;
- i) transferências de dados previstas para países terceiros;
- j) descrição geral que permita avaliar de forma preliminar a adequação das medidas tomadas para garantir a segurança do tratamento.

Artigo 31

(Indicações Obrigatórias)

1. Os registos de tratamento de dados pessoais e as autorizações da Autoridade Nacional de Protecção de Dados devem pelo menos indicar:
 - a) o responsável e, se for caso disso, o seu representante;
 - b) as categorias de dados pessoais tratados;
 - c) as finalidades a que se destinam os dados e as categorias de entidades a quem podem ser transmitidos;
 - d) a forma de exercício de direito de acesso, de rectificação, autorização e cancelamento;
 - e) eventuais interconexões de tratamento de dados pessoais;
 - f) transferência de dados previstas para países terceiros.
2. Qualquer alteração das indicações constantes do número anterior está sujeita aos procedimentos previstos no artigo 65º.

Artigo 32

(Publicidade dos Tratamentos)

1. O tratamento de dados pessoais, quando deva ser autorizado ou notificado, consta de registo da Autoridade Nacional de Protecção de Dados, aberto à consulta pública.
2. O registo contém as informações enumeradas nas alíneas a) a d) e i) do artigo 66º.
3. O responsável pelo tratamento não sujeito a notificação está obrigado a apresentar, de forma adequada, a qualquer pessoa que o solicite, pelo menos as informações indicadas no nº 1 do artigo 67º. O disposto no presente artigo não se aplica ao tratamento de dados em fontes acessíveis publicamente.

Capítulo VIII

Acreditação, certificação e código de conduta

Artigo 33

(Acreditação e Certificação)

1. A autoridade competente para a acreditação dos organismos de certificação em matéria de protecção de dados é Autoridade Certificadora...
2. O ato de acreditação emitido pela Autoridade Certificadora, deve tomar em consideração os requisitos previstos na presente Lei, bem como os requisitos estabelecidos pela Autoridade Nacional de Protecção de Dados.
3. A certificação, bem como a emissão de selos e marcas de protecção de dados, é efectuada por organismos de certificação acreditados nos termos do n.º 1, destinando-se a atestar que os procedimentos implementados cumprem o disposto na presente Lei.

Artigo 34.

(Códigos de Conduta)

1. Compete à ANPD promover a elaboração de códigos de conduta destinados a contribuir em função das características dos diferentes sectores, para boa execução das disposições da presente Lei.
2. O tratamento de dados pessoais no âmbito da presente Lei é objecto de código de conduta.
3. Os códigos de conduta devem ser registados na ANPD.
4. ANPD pode rejeitar o registo de Código de conduta quando considere os mesmos contrários às disposições da presente Lei e demais legislação aplicável.
5. Compete à ANPD emitir pareceres e recomendações para que os responsáveis pela criação dos códigos de conduta efectuem as correcções necessárias.

Capítulo IX

Tutela administrativa e jurisdicional

Secção I

Disposições Gerais

Artigo 35

Sem prejuízo do direito de apresentação de queixa à ANPD, qualquer pessoa pode, nos termos da lei, recorrer a meios administrativos ou jurisdicionais para garantir o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais.

Artigo 36

(Tutela jurisdicional)

1. Qualquer pessoa, pode nos termos da Lei, recorrer judicialmente da violação dos direitos previstos na presente Lei.
2. As acções propostas contra ANPD são da competência dos Tribunais Administrativos.
3. O titular dos dados pode propor acções contra o responsável pelo tratamento ou o subcontratante, incluindo acções de responsabilidade civil.
4. As acções intentadas contra o responsável pelo tratamento ou um subcontratante são propostas nos tribunais nacionais se o responsável ou subcontratante tiver o estabelecimento em território nacional ou se o titular dos dados residir habitualmente.

Artigo 37

(Legitimidade da Autoridade nacional de Protecção de dados)

A ANPD tem legitimidade para intervir em processos judiciais no caso de violação das disposições da presente lei, e deve denunciar ao Ministério Público as infracções penais de que tiver conhecimento, no exercício das suas funções e por causa delas, bem como praticar os atos cautelares necessários e urgentes para assegurar os meios de prova.

Secção II

Contraordenações

Artigo 38

(Contraordenações muito graves)

1. Constituem contraordenações muito graves:

- a) Os tratamentos de dados pessoais com inobservância dolosa dos princípios previstos no Artigo 4 da presente Lei.
- b) Os tratamentos de dados pessoais que não tenham por base o consentimento ou outra condição de legitimidade, nos termos do Artigo 13 da presente Lei;
- c) O incumprimento das regras relativas à prestação do consentimento previstas no artigo 19 da presente Lei.
- d) Os tratamentos de dados pessoais previstos no n.º 1 do Artigo 14 da presente Lei, sem que se verifique uma das circunstâncias previstas no n.º 2 do mesmo artigo.
- e) Os tratamentos de dados pessoais previstos no artigo 17 da presente Lei, que contrariem as regras estabelecidas.
- f) A exigência do pagamento de uma quantia em dinheiro fora dos casos previstos no artigo 19 da presente Lei.

Artigo 39.

(Contraordenações graves)

- 1 Constituem contraordenações graves:

Artigo 40.

(Determinação da medida das sanções)

Artigo 41.

(Prescrição do procedimento por contraordenação)

O procedimento por contraordenação extingue -se por efeito da prescrição logo que sobre a prática da contraordenação hajam decorrido os seguintes prazos:

- a) Três anos, quando se trate de contraordenação muito grave;
- b) Dois anos, quando se trate de contraordenação grave.

Artigo 42.

(Prazo de prescrição das sanções)

As sanções previstas na presente lei prescrevem nos seguintes prazos:

- a) Três anos, no caso de sanções com montante superior a
- b) Dois anos, no caso de sanções de montante igual ou inferior a

Artigo 43.

(Destino das Multas)

O montante das sanções cobradas reverte em 60 % para o Estado e em 40 % para a ANPD.

Artigo 44

(Cumprimento do dever omitido)

Sempre que a contraordenação resulte da omissão de um dever, a aplicação da sanção e o pagamento, não dispensam o infrator do seu cumprimento se este ainda for possível.

Artigo 45.

(Âmbito de aplicação das contraordenações)

1. As sanções previstas na presente lei aplicam -se de igual modo às entidades públicas e privadas.
2. Nos termos do disposto no n.º 7 do artigo 83.º do RGPD, as entidades públicas, mediante pedido devidamente fundamentado, podem solicitar à ANPD a dispensa da aplicação de sanção durante o prazo de três anos a contar da entrada em vigor da presente lei.
3. As entidades públicas estão sujeitas aos poderes de correção da ANPD, tal como previstos no RGPD e na presente lei, com exceção da aplicação de sanção nos termos definidos no número anterior.

Artigo 46.

(Regime subsidiário)

Em tudo o que não esteja previsto na presente lei em matéria contraordenacional, aplica -se o disposto no regime geral do ilícito de mera ordenação social.

SECÇÃO III

Crimes

Artigo 47.

(incumprimento das obrigações relativas a protecção de dados pessoais)

- 1 Sem prejuízo das demais obrigações reguladas na presente Lei, incorre em crime punível com pena de prisão de até 1 ano ou pena de multa de 120 dias, quem intencionalmente:
 - a) Omitir a notificação ou o pedido de autorização a ANPD;
 - b) Fornecer falsas informações na notificação ou nos pedidos de autorização para tratamento de dados pessoais, ou neste proceder a modificações consentidas pelo presente Lei;
 - c) Desviar ou utilizar dados pessoais de forma incompatível com finalidade determinante da recolha ou com base Legal
 - d) Promover ou efectuar uma interconexão ilegal de dados pessoais
 - e) Findo o prazo que estiver sedo fixado pela ANPD para cumprimento das obrigações previstas na presente Lei ou em outra legislação subsidiárias, as não cumprir
 - f) Apos a notificação pela ANPD para o não fazer, manter o acesso a redes abertas de transmissão de dados a responsável pelo tratamento de dados pessoais que não cumpram as disposições da presente Lei
- 2 A pena é agravada para o dobro nos seus limites quando se tratar dos dados pessoais a que se referem os artigos 9.º e 10.º do RGPD.

Artigo 48.

(Acesso indevido)

1. Quem, sem a devida autorização ou justificação, aceder, por qualquer modo, a dados

2. pessoais é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
3. A pena é agravada para o dobro nos seus limites quando se tratar dos dados pessoais a que se referem
4. A pena é também agravada para o dobro nos seus limites quando o acesso:
 - a) for conseguido através de violação de regras técnicas de segurança; ou
 - b) tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial.

Artigo 49.

(Desvio de dados)

1. Quem copiar, subtrair, ceder ou transferir, a título oneroso ou gratuito, dados pessoais
2. sem previsão legal ou consentimento, independentemente da finalidade prosseguida, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
3. A pena é agravada para o dobro nos seus limites quando se tratar dos dados pessoais a que se referem os
4. A pena é também agravada para o dobro nos seus limites quando o acesso:
 - a) for conseguido através de violação de regras técnicas de segurança; ou
 - b) tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial.

Artigo 50.

(Viciação ou destruição de dados)

1. Quem, sem a devida autorização ou justificação, apagar, destruir, danificar, ocultar, suprimir ou modificar dados pessoais, tornando-os inutilizáveis ou afetando o seu potencial de utilização, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.
2. A pena é agravada para o dobro nos seus limites se o dano produzido for particularmente grave.

3. Nas situações previstas nos números anteriores, se o agente atuar com negligência é punido com pena de prisão:
 - a) até 1 ano ou multa até 120 dias, no caso previsto no n.º 1;
 - b) até 2 anos ou multa até 240 dias, no caso previsto no n.º 2.

Artigo 51.

(Inserção de dados falsos)

1. Quem inserir ou facilitar a inserção de dados pessoais falsos, com a intenção de obter vantagem indevida para si ou para terceiro, ou para causar prejuízo, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.
2. A pena é agravada para o dobro nos seus limites se da inserção referida no número anterior resultar um prejuízo efetivo

Artigo 52.

(Violação do dever de sigilo)

1. Quem, obrigado a sigilo profissional nos termos da lei, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
2. A pena é agravada para o dobro nos seus limites se o agente:
 - a) for trabalhador em funções públicas ou equiparado, nos termos da lei penal;
 - b) for encarregado de proteção de dados;
 - c) for determinado pela intenção de obter qualquer vantagem patrimonial ou outro benefício ilegítimo;
 - d) puser em perigo a reputação, a honra ou a intimidade da vida privada de terceiros.
3. A negligência é punível com pena de prisão até 6 meses ou com pena de multa até 60 dias.

Artigo 53.

(Desobediência)

1. Quem não cumprir as obrigações previstas e na presente lei, depois de ultrapassado o prazo que tiver sido fixado pela ANPD para o respetivo

cumprimento, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2. A pena é agravada para o dobro nos seus limites se, depois de notificado para o efeito, o agente:
 - a) não interromper, cessar ou bloquear o tratamento ilícito de dados;
 - b) não proceder ao apagamento ou destruição dos dados quando legalmente exigível, ou findo o prazo de conservação fixado nos termos da presente lei; ou
 - c) recusar, sem justa causa, a colaboração que lhe for exigida nos termos do artigo 8.º da presente lei.

Artigo 54.

(Punibilidade da tentativa)

Nos crimes previstos na presente secção, a tentativa é sempre punível.

Artigo 55.

(Responsabilidade das pessoas coletivas)

As pessoas colectivas e entidades equiparadas, com excepção do Estado, de pessoas colectivas

no exercício de prerrogativas de poder público e de organizações de direito internacional público, são responsáveis pelos crimes previstos na presente secção, nos termos do artigo 11.º do Código Penal.

(Utilização de dados de forma incompatível com a finalidade de recolha)

Capítulo XI

Medidas de Segurança

Artigo 56

(Segurança de Tratamento)

1. O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas, e estabelecer níveis de segurança adequadas, para proteger os

dados pessoais contra destruição total ou parcial, acidental ou ilícita, a perda acidental, a alteração total ou parcial, a difusão ao acesso não autorizado, fundamentalmente quando o tratamento implicar a sua transmissão em rede, e contra qualquer outra forma de tratamento ilícito.

2. As medidas de segurança devem assegurar atendimento aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, o nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.
3. O responsável pelo tratamento deve elaborar um documento com medidas, normas e procedimento de segurança aplicáveis ao tratamento de dados pessoais, detalhando os níveis de segurança, os recursos a proteger e as funções e obrigações das pessoas com acesso aos dados, de acordo com as regras de segurança.

Artigo 57

(Medidas Especiais de Segurança)

1. O responsável pelo tratamento dos dados deve, relativamente aos dados indicados acima, tomar as medidas adequadas para:
 - a) impedir o acesso da pessoa não autorizada aos ficheiros e às instalações utilizadas para o tratamento dos dados;
 - b) impedir que suportes de dados passem a ser lidos, copiados, alterados ou retirados por pessoas não autorizadas;
 - c) impedir a introdução não autorizada bem como a tomada de conhecimento, a alteração ou eliminação não autorizada de dados pessoais inseridos;
 - d) impedir que os sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas através de instalação de transmissão de dados;
 - e) garantir que só as pessoas autorizadas possam ter acesso aos dados abrangidos pela autorização;
 - f) garantir a verificação das entidades a quem possam ser transmitidos os dados pessoais através das instalações de transmissão de dados;

- g) garantir que se possa verificar a posterior em prazo adequado à natureza do tratamento conforme fixado em regulamentação aplicável a cada sector, quais os dados pessoais introduzidos, quando e por quem;
 - h) impedir que na transmissão de dados pessoais bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada.
2. Os sistemas devem garantir a separação lógica entre os dados referentes à saúde e à vida sexual, incluindo os genéticos dos restantes dados pessoais.
 3. A Autoridade Nacional de Protecção de Dados pode determinar que, nos casos em que a circulação em rede de dados pessoais referidos nos artigos acima possam por em risco direitos, liberdades e garantias de respectivos titulares, a transmissão seja cifrada.

Artigo 58

(Sigilo Profissional)

1. Os responsáveis de tratamento de dados pessoais, bem como as pessoas que no exercício das suas funções, tenham conhecimento dos dados pessoais tratados, ficam obrigados a sigilo profissional, mesmo após o término das suas funções.
2. Aplica-se o disposto no nº anterior aos membros da Autoridade Nacional de Protecção de Dados, bem como aos funcionários, agentes ou técnicos que exerçam funções de assessoria à Autoridade Nacional de Protecção de Dados, mesmo após o término do mandato.
3. O disposto nos números anteriores não exclui o dever de fornecimento das informações obrigatórias, nos termos legais, excepto quando constem de ficheiros organizados para fins estatísticos.
4. A violação do sigilo profissional obriga os seus autores à responsabilidade criminal, nos termos do artigo 58 da presente Lei diploma , sem prejuízo da responsabilidade disciplinar ou civil, nos termos da presente Lei.

Capítulo XI

Disposições finais e transitórias

Artigo 59.

(Disposição transitória)

1. Os tratamentos de dados existentes em ficheiros manuais à data da entrada em vigor da presente Lei devem cumprir o disposto nos artigos 7.º (Artigo 7.º Tratamento de dados sensíveis), 8.º (Artigo 8.º Suspeitas de actividades ilícitas, infracções penais e infracções administrativas), 10.º (Artigo 10.º Direito de informação) e 11.º (Artigo 11.º Direito de acesso) no prazo de 2 anos.
2. Em qualquer caso, o titular dos dados pode obter, a seu pedido e, nomeadamente, aquando do exercício do direito de acesso, a rectificação, a eliminação ou o bloqueio dos dados incompletos, inexactos ou conservados de modo incompatível com os fins legítimos prosseguidos pelo responsável pelo tratamento.
3. A Agência Nacional de Protecção de Dados Pessoais pode autorizar que os dados existentes em ficheiros manuais e conservados unicamente com finalidades de investigação histórica não tenham que cumprir os artigos 7.º, 8.º e 9.º (Artigo 9.º Interconexão de dados pessoais), desde que não sejam em nenhum caso reutilizados para finalidade diferente.

Capítulo XII

Responsável dos Dados Pessoais?

Qualquer pessoa singular ou colectiva, pública ou privada, qualquer outra organização ou associação que sozinha ou em conjunto com outras pessoas decida recolher e processar dados pessoais e determinar a sua finalidade.

Artigo 60

(Obrigações de confidencialidade)

O processamento de dados pessoais é confidencial. É efectuado exclusivamente por indivíduos que agem sob a autoridade do responsável dos dados e somente sob as suas instruções

Artigo 61

(Obrigações de Segurança)

O responsável pelos dados deve tomar todas as precauções apropriadas, de acordo com a natureza dos dados e, em particular, evitar que esses dados sejam alterados ou destruídos, utilizados por pessoas não autorizadas.

Artigo 62

(Obrigações de Conservação)

Os dados pessoais não devem ser conservados para além do período necessário para fim pelo qual se fez a sua recolha e o seu processamento.

Artigo 63

(Obrigações de Manutenção)

1. O responsável pelos dados deve tomar todas as medidas necessárias com vista a assegurar que os dados pessoais processados possam ser explorados independentemente do dispositivo técnico utilizado no processo.
2. O funcionário que faz o processamento deve, em particular, assegurar que as mudanças tecnológicas não constituam um obstáculo para a utilização dos dados

Artigo 64

(Dados anonimizados)

1. Os dados anonimizados não serão considerados dados pessoais para os fins salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
2. A determinação do que seja razoável deve levar em consideração factores objectivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.
3. Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.
4. A autoridade nacional poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Protecção de Dados Pessoais.