23° enancib
ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO
06 a 10 de novembro de 2023
ARACAJU-SE

GT-5 – Política e Economia da Informação

ISSN 2177-3688

GESTÃO DE DADOS PESSOAIS EM MOÇAMBIQUE: DA DIPLOMÁTICA À LEGISLAÇÃO

PERSONAL DATA MANAGEMENT IN MOZAMBIQUE: FROM DIPLOMATICS TO LEGISLATION

Cecília Preciosa Cabsela - Universidade Estadual Paulista (UNESP)
Sonia Maria Troitiño Rodriguez - Universidade Estadual Paulista (UNESP)

Modalidade: Trabalho Completo

Resumo: Atendendo o cenário hodierno da crescente coleta e partilha de dados pessoais, por diversas entidades, entre públicas e privadas, em diversos contextos, com normativas de proteção de dados pessoais ou não, com políticas de informação estabelecidas ou não e práticas arquivísticas consolidadas ou não, indaga-se se é feita a gestão de dados pessoais em Moçambique e que qualidades da diplomática arquivística (não)são preservadas no processo de gestão de dados pessoais. Busca-se compreender a gestão de dados pessoais com enfoque no contexto moçambicano através da legislação, relacionando-a com a diplomática. De forma especifica visa discutir o processo de gestão de dados pessoais diante da diplomática; identificar legislação moçambicana conexa à gestão de dados pessoais; e, levantar e analisar as qualidades diplomáticas de dados pessoais na legislação. O artigo é fruto de uma pesquisa qualitativa descritiva-exploratória que recorre à revisão da literatura e pesquisa documental. Apresentam-se as relações entre os dados pessoais e sua gestão; diplomática arquivística e a legislação sobre dados pessoais em Moçambique. São identificadas qualidades diplomáticas na legislação moçambicana. Conclui-se que a legislação moçambicana, na sua maioria aponta apenas as qualidades de autenticidade e integridade de documentos e/ou informação, apresentando estas e/ou outras qualidades diplomáticas para os dados pessoais nas entrelinhas ou indiretamente.

Palavras-chave: política de informação; gestão de dados pessoais; autenticidade; confiabilidade; Moçambique.

Abstract: Regarding the current scenario of the growing collection and sharing of personal data, by various entities, public and private, in different contexts, with or without personal data protection regulations, with or without established information policies and with or without consolidated archival practices, we wonder whether personal data management is carried out in Mozambique and which diplomatics qualities are (not) preserved in the personal data management. We seek to understand the personal data management with a focus on the mozambican context through legislation, relating it to diplomatics. Specifically, it aims to discuss the process of personal data management in the face of diplomacy; identify Mozambican legislation related to personal data management; and survey and analyse the diplomatic qualities of personal data in legislation. The article is the result of a descriptive-exploratory qualitative study that uses a literature review and documentary research. The relationships between personal data and its management; archival diplomatics and legislation on personal data in Mozambique are presented. Diplomatics qualities referenced in mozambican legislation are identified. It is concluded that the mozambican legislation, in its majority, points only to the qualities of authenticity and integrity of documents and/or information, presenting these and/or other diplomatic qualities for personal data between the lines or indirectly.

Keywords: information policy; personal data management; authenticity; reliability; Mozambique.

1 INTRODUÇÃO

A gestão de dados pessoais ela pode ser discutida dentro do escopo de uma política de informação, entendida por Jardim; Silva; Nharreluga, (2009) como um conjunto de premissas, decisões e ações (produzidas pelo Estado e inseridas nas agendas governamentais em nome do interesse social) que contemplam os diversos aspetos legais, administrativos, científicos, culturais, tecnológicos, entre outros, relativos à produção, uso e preservação da informação de natureza pública e privada. Portanto, essa informação de natureza privada, contempla os dados pessoais.

Alias, em 2000, Daniel apresentou o conceito de política de informação como conjunto de regras formais e informais que diretamente, restringindo, impulsionando ou de outra maneira, formam fluxos de informação e inclui a literacia, privatização e distribuição da informação governamental, liberdade de acesso à informação, proteção da privacidade individual e direitos de propriedade intelectual. Como notamos, os dados pessoais e a sua gestão estão presentes nas definições apresentadas.

Estas políticas de informação, na dimensão que estamos aqui a apresentar, *policy* (política pública), pode ser formulada e desenvolvida, segundo Montviloff (1990) em nível institucional, nacional, regional ou internacional. Elas mesmas tem interfaces com outras políticas públicas, como as políticas de educação, de comunicação, de cultura, de telecomunicações, de preservação digital, de inclusão digital, de segurança cibernética, de arquivos, etc. E ainda, estas políticas devem se traduzir, como vimos, em decisões, ações, mas também em programas. Podemos indicar aqui, programas de gestão de documentos, seja tradicional ou eletrónico.

Neste artigo, nos concentramos ao nível nacional da política de informação, observando-a concretamente em Moçambique. Neste contexto procuramos compreender a gestão de dados pessoais, buscando elementos no aparato legal oferecido pela(s) política(s) existente(s) e nas qualidades diplomáticas que este quadro legal apresenta.

Em termos metodológicos, conforme Gil (2022), toda pesquisa tem seus objetivos a serem diferentes dos objetivos de outras, sendo que em seus propósitos elas podem ser classificadas em exploratórias, descritivas e explicativas. Atendendo aos objetivos do presente trabalho, realizamos uma pesquisa qualitativa descritiva-exploratória, através da

qual recorremos à revisão da literatura, que segundo Severino (2017), é o processo necessário para poder se avaliar o que já foi produzido sobre o assunto e daí situar a contribuição que a pesquisa pode dar ao conhecimento do objeto de pesquisa, e pesquisa documental para a obtenção dos dados que passaram por uma análise de conteúdo e sua interpretação. Ora, 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". Para a realização deste trabalho foram identificadas e analizadas 11 normativas moçambicanas atinente à temática estudada.

2 DIPLOMÁTICA

A diplomática nasceu no século XVII como uma técnica analítica para determinar a autenticidade de documentos emitidos por autoridades soberanas em séculos anteriores. Alias, o primeiro diplomatista, Mabillon, definiu a diplomática como o estabelecimento de termos e regras precisas pelas quais os instrumentos autênticos podem ser distinguidos dos outros. No final do século XX, os arquivistas descobriram novos usos para essa antiga ciência, com base em seu potencial como padrão para garantir a confiabilidade dos documentos modernos em geral e dos documentos eletrônicos em particular, começando a usá-la como uma ferramenta para entender os documentos atuais e as tecnologias relacionadas a documentos, fazendo um uso universalizado (MACNEIL, 2000, p. 86). Duranti (1989) já havia avançado que é apropriado que os arquivistas extraiam diretamente da ciência original da diplomática os elementos e perceções que podem ser usados em seu trabalho e os desenvolvam para atender às necessidades contemporâneas.

No momento que se segue, passamos a discutir fundamentalmente, duas qualidades ou elementos diplomáticos que são a autenticidade e confiabilidade (dois conceitos que permitem a verificação da genuinidade de um documento). Estas qualidades são abordadas no âmbito diplomático e arquivístico.

Logo de início Lauriault *et al.* (2007) nos chamam a atenção para o fato de autenticidade estar intimamente ligada ao conceito de confiabilidade. Acrescentam que um objeto que se acredita e se prova ser autêntico é considerado confiável e que a confiança geralmente é construída ou erguida com base nas garantias de que os dados ou documentos são autênticos, confiáveis e precisos.

Na ciência arquivística, a autenticidade é uma característica de todos os documentos de arquivo, que são a expressão da entidade que os produziu no curso normal e ordinário de seus negócios. Na diplomática, um documento passa a ser considerado autêntico se ele tiver todos os elementos formais que deveria apresentar quando foi feito ou recebido pela primeira vez, ou seja, esse documento é o que pretende ser e seu conteúdo pode ser confiável. Portanto, na diplomática a autenticidade está ligada ao estado do documento, ao modo e à forma de transmissão, bem como à maneira de sua preservação e custódia (DURANTI; EASTWOOD; MACNEIL, 2002).

Em 2002 Duranti e seus colegas, compreenderam que procedimentos específicos para proteger a integridade do componente eletrônico do sistema de documentos são necessários porque a prova da integridade do sistema eletrônico implica a prova da integridade dos documentos criados e/ou armazenados nele. Tais procedimentos associados à proteção da integridade do sistema eletrônico incluem a determinação dos requisitos do sistema. A determinação dos requisitos do sistema eletrônico inclui a identificação de (1) requisitos funcionais; (2) padrões nacionais e internacionais de documentação e comunicação; (3) metadados do sistema eletrônico; (4) aplicativos de escritório e software de comunicação a serem usados para criar, manipular e preservar documentos; e (5) requisitos de interoperabilidade de aplicativos de escritório, software de comunicação e software de manutenção de documentos (DURANTI; EASTWOOD; MACNEIL, 2002, p. 40).

Estes autores também abordaram, no mesmo documento, à questão dos privilégios de acesso que se referem à autoridade concedida aos funcionários de um órgão para compilar, classificar, anotar, ler, recuperar, transferir e destruir documentos. As regras que regem o estabelecimento e a implementação de privilégios de acesso têm como objetivo afirmar o grau máximo de controle sobre os documentos no sistema de documentos como o meio mais eficaz de garantir sua confiabilidade durante sua criação e proteger sua autenticidade durante seu uso e transmissão.

Dessa forma, as regras atribuem privilégios de acesso à escritórios ou funcionários específicos para cada classe de documentos com base em sua competência; permitem que apenas o escritório ou funcionário que cria os documentos tenha acesso irrestrito a eles; proíbem a modificação de documentos depois de classificados; permitem que o escritório ou funcionários responsáveis pelo manuseio e *record office* anotem os documentos; permitem que o *record office* tenha acesso aos documentos para fins de classificação; e dão ao *record*

office autoridade exclusiva para acessar os documentos para fins de transferência ou destruição (DURANTI; EASTWOOD; MACNEIL, 2002, p. 41).

Ora, o grau de integridade e o grau de controle do procedimento de criação são os dois únicos fatores que determinam a confiabilidade dos documentos. A confiabilidade não depende, de forma alguma, do status de transmissão dos documentos. O status da transmissão refere-se à fase de desenvolvimento de um documento, ou seja, se ele é um rascunho, um original ou uma cópia. Assim, a confiabilidade é fornecida à um documento por sua forma e procedimento de criação. A forma de um documento é o conjunto de suas características que podem ser separadas da determinação dos assuntos, pessoas ou lugares sobre os quais o documento trata. Um documento é considerado confiável quando sua forma é completa, ou seja, quando possui todos os elementos exigidos pelo sistema sociojurídico no qual o documento é criado para que possa gerar consequências reconhecidas pelo próprio sistema (DURANTI, 1995, p.6).

Diplomaticamente, um documento digital é confiável se for preciso, confiável e autêntico. A precisão ou acurácia dos documentos nunca foi levada em consideração na diplomática geral porque, como conceito, ela foi incluída na confiabilidade e na autenticidade. A acurácia é a confiabilidade dos dados (ou seja, as menores, significativas e indivisíveis informações) em um documento e é definida como sua veracidade, exatidão, acurácia ou completude. Este elemento é importante quando nos debruçamos sobre os dados pessoais e sua proteção. No ambiente digital, é necessário considerar e avaliar a acurácia como uma qualidade separada de um documento devido à facilidade com que os dados podem ser corrompidos durante a transmissão no espaço (entre pessoas e/ou sistemas) e no tempo (quando os sistemas digitais são atualizados ou os documentos são migrados para um novo sistema). Consequentemente, a acurácia é uma responsabilidade mutável que, com o tempo, passa do criador de documento de confiança para o custodiador de confiança (DURANTI, 2009, p. 52).

3 GESTÃO DE DADOS PESSOAIS

Nesta sessão, vamos nos debruçar sobre a gestão de dados pessoais, partindo, antes de mais do conceito de dados e dados pessoais, observando o quesito proteção.

Para Roje (2023, p. 67) “os dados são todos os fatos não organizados que precisam de algum processamento e organização para se tornarem informações”. Esta abordagem

reflete-se quando consideramos a dimensão identificável dos dados pessoais, ao fazermos um paralelo com a necessidade de processamento dos dados. Os dados pessoais, como acabamos de introduzir, são, conforme Madsen (1992, p. 205) “dados relacionados à um indivíduo que pode ser identificado a partir dos dados ou dos dados em conjunto com outros dados disponíveis”.

Doneda (2011) levantou especificações em relação à utilização dos termos “dado” pessoal e “informação” pessoal, dando indicação de que o conteúdo dos dois se sobrepõe em várias circunstâncias. Ele aponta que o “dado” apresenta conotação um pouco mais primitiva e fragmentada e “informação”, alude a algo além da representação contida no dado, chegando ao limiar da cognição.

Nolasco e Silva (2022) percebem que a informação pessoal é definida comumente como a informação referente a uma pessoa determinada ou determinável, apresentando uma ligação concreta com a pessoa. Para eles, esta modalidade de informação vem se tornando constantemente mais disponível para uma miríade de utilizações, basicamente por conta da facilidade e do baixo custo de sua coleta e armazenamento com os meios digitais hoje disponíveis.

Ora, não só os dados e informações são valorizados pelo alvorecer do meio cibernético, mas também o direito à privacidade, que, agora, descobre-se em um novo paradigma (NOLASCO; SILVA, 2022, p. 2359). Como indicam Efing e Catuzo (2016) a crescente utilização das novas tecnologias estabelece múltiplas dinamicidades às relações sociais contemporâneas. […] Esse novo paradigma de inter-relacionamento caracteriza a sociedade da informação, em que a gestão de dados imateriais e conhecimentos científicos e tecnológicos são propulsores da articulação social.

Através de Roberts (1994), entendemos a gestão de dados como "a função de controlar a aquisição, análise, armazenamento, recuperação e distribuição de dados". Portanto, ela pode envolver uma grande variedade de funções, como proteger a segurança física dos dados por meio de procedimentos adequados de backup e de recuperação, proteção da confidencialidade e privacidade dos dados, estabelecendo e reforçando a responsabilidade dos usuários pela acurácia dos dados, redução da redundância ou duplicação de dados, organizando-os de forma racional e consistente e garantindo a preservação dos dados pelos períodos necessários. Roberts (ibid.) Ele aponta ainda que nas organizações, a gestão de dados é normalmente considerada como parte da gestão dos

recursos de tecnologia da informação, embora não seja necessariamente reconhecido organizacionalmente como uma unidade específica responsável pela função.

Considerando que o maior problema da segurança dos dados e sua privacidade se dá no ambiente virtual, entende-se que a importância da Diplomática Contemporânea no assunto se dá no tratamento do documento arquivístico digital. Isso porque os dados não podem ser considerados isoladamente, pois são partes que se constituem no âmbito de um documento, seja ele arquivístico ou não (SILVEIRA; KARPINSKI, 2023, p.13).

É imperioso destacar, através de Godinho *et al.* (2020) que o armazenamento de dados abrange não só o que encontramos na rede mundial de computadores interligados, mas também os chamados bancos de dados. O armazenamento de dados diz respeito a informações pessoais que ficam arquivadas por entes públicos, privados ou pelo próprio indivíduo, para serem acessados posteriormente. Este armazenamento, outrora inofensivo, passou a ameaçar direitos e garantias fundamentais, tais quais a privacidade, a imagem e a honra (EFING; CATUZO, 2016).

É de destacar também o direito à eliminação dos dados que assegura ao respetivo titular a faculdade de solicitar ao agente controlador, a qualquer momento, a eliminação de suas informações pessoais dos bancos de dados. Mas esse direito não é absoluto. É preciso ser analisado o impacto que o direito à eliminação de dados causa tanto sobre a atividade econômica desempenhada pelos agentes de tratamento, quanto sobre os direitos fundamentais das pessoas envolvidas, como os direitos à privacidade e ao esquecimento (GODINHO; NETO; TOLÊDO, 2020, p. 8).

Ademais, quando os dados pessoais são mantidos em um banco de dados por um período excessivo, os indivíduos podem ser vítimas de discriminação e assédio. Os dados pessoais tendem a permanecer inalterados depois de inseridos em um sistema. Informações desatualizadas geralmente tendem, com o passar do tempo, a se tornar informações incorretas. Madsen (1992) chama atenção à necessidade de atualizar constantemente os arquivos de dados pessoais e acrescenta, mesmo que os dados pessoais sejam alterados de forma autorizada em um arquivo de dados, não há garantia razoável de que essa alteração será refletida em outros arquivos e bancos de dados para os quais os dados possam ter sido transferidos.

4 QUALIDADES DIPLOMÁTICAS NA LEGISLAÇÃO MOÇAMBICANA DE PROTEÇÃO DE DADOS PESSOAIS

No continente americano assim como europeu, as leis relacionadas à proteção de dados encontravam-se pulverizadas por todo o ordenamento jurídico. A partir da metade dos anos 2000, motivados pela massificação do uso da internet, observaram a necessidade de uma regulamentação mais específica na proteção de dados para maior segurança jurídica (SILVA; CARDOSO, 2022, p. 142).

Madsen (1992) deu indicação de que em países que não desenvolveram governos democráticos de acordo com as linhas parlamentares tradicionais, a aquisição de tecnologia da informação tinha sido usada para realizar operações que as leis de proteção de dados do modelo europeu foram claramente projetadas para evitar. O autor continua dizendo que muitos governos da América Latina, África e Ásia forneceram sistemas de computador para serviços de segurança repressivos com o único propósito de monitorar determinados setores da população.

Ora, em Moçambique a questão da proteção de dados pessoais encontra fundamentos da Constituição da República nos artigos 41°, 68° e 71°, assim como noutras normativas não específicas que passamos a analisar enfocando as qualidades diplomáticas.

A, dita, Política de Informação (PI) e sua estratégia foram aprovadas pela Resolução nº 3/97 de 18 de fevereiro. Nela está plasmado que a PI refere-se ao conjunto de medidas ou atividades, baseadas no programa do Governo, visando impulsionar o desenvolvimento da Comunicação Social. Como se pode perceber, a PI em Moçambique está concebida como uma política de comunicação social o que tem implicações nefastas para a área da gestão da informação, gestão de documentos e gestão de dados, que vai (sobre)vivendo sem políticas e nem programas.

Em 2006 foi traçada a Estratégia para a Gestão de Documentos e Arquivos do Estado (EGDAE), pela Resolução n.º 46/2006, de 26 de dezembro, embora não incorporada numa política de arquivos e/ou de informação. Nessa altura foi indicado que os meios físicos e organizacionais de recolha, produção, difusão, uso e preservação da documentação e informação constituíam um dos problemas que se levantavam na área de gestão documental em Moçambique, sendo que todo este cenário requer(ia) documentalistas e arquivistas capacitados, para além de técnicos informáticos e profissionais de outras áreas afins.

Das diferentes ações estratégicas arroladas, uma visa(va) o desenvolvimento de recursos humanos, por forma a profissionalizar os técnicos das unidades documentais e

arquivísticas, estabelecendo formas de reconhecimento e valorização destes profissionais na Administração Pública, como incentivo para garantir a proteção da integridade dos documentos. Pressupõe-se com isto que, todos os instrumentos normativos, atinentes aos arquivos e à gestão de documentos, promulgados posteriormente, sejam fruto desta estratégia e que tomam em consideração as questões de integridade, confiabilidade, autenticidade, e outras qualidades diplomáticas.

Na Lei do Direito à Informação, Lei n.º 34/2014, de 31 de dezembro, não encontramos a ocorrência das qualidades diplomáticas, sendo, contudo, uma norma que regula o acesso às informações de interesse público e que, na nossa perceção, por ser igualmente uma norma conexa à legislação arquivística, essas informações de interesse público devem ser acessadas enquanto informações confiáveis, autênticas e íntegras. Sublinhamos também que esta é uma normativa conexa à proteção de dados pessoais.

A Lei n.º 3/2017, de 9 de janeiro, Lei de Transacções Electrónicas, é, até aqui, a lei que mais elementos de proteção de dados pessoais avança, mas também avança vários aspetos do ambiente eletrónico. No capítulo do "Sistema de Certificação Digital e Criptografia", aponta no art. 54° que a Entidade Reguladora de Tecnologias de Informação e Comunicação deve estabelecer os fundamentos técnicos e metodológicos do sistema e que estes fundamentos deverão garantir a autenticidade, integridade e validade jurídica de documentos em formato eletrónico, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrónicas seguras.

No capítulo IX da "Protecção de Dados Electrónicos Pessoais", estabelece a "Responsabilidade do processador de dados" (art. 65°), indicando que ele(a) deve colocar à disposição de qualquer pessoa, informação específica acerca das suas políticas e práticas relacionadas com a gestão de informação pessoal (*voire* gestão de dados pessoais).

No capítulo IV das "Mensagens de Dados e Comunicações Electrónicas", fala-se da "Aplicação de requisitos legais às mensagens de dados", onde no art. 23°, esta plasmado que sempre que a lei exigir que uma certa informação seja apresentada ou conservada na sua forma original, esta deve conter garantia fidedigna de que se preservou a integridade da informação desde o momento da sua geração em sua forma final. No mesmo capítulo também se fala da "Admissibilidade e força probatória das mensagens de dados" (art. 24°), onde "Na avaliação da força probatória de uma mensagem electrónica, a sua fiabilidade afere-se pela forma como foi gerada, armazenada, emitida, transmitida e recebida; pela

forma como foi conservada a integridade da informação"; entre outras. Outro aspeto que a lei estabelece é a "Conservação de mensagens de dados" (art. 25°) onde, sempre que a lei exigir que determinado documento, registro ou informação seja conservado, esta informação contida na mensagem eletrónica deve ser conservada no formato no qual tenha sido gerada, emitida, transmitida e recebida, ou num formato que se possa demonstrar que representa exatamente a informação gerada, emitida, transmitida e recebida, e toda a informação deve permitir determinar a origem, o destino, a data e a hora em que as mensagens foram enviadas ou recebidas.Esta lei, para além de apontar vários elementos para a proteção de dados pessoais, ela também avança vários elementos da gestão desses dados, no contexto moçambicano, apontando aspeto desde a receção, armazenamento, conservação, etc., e faz ainda alusão às qualidades diplomáticas inerente à informações e documentos que contém tais dados.

A antiga política de informática foi revogada e em seu lugar foi aprovada a Política para a Sociedade da Informação de Moçambique, pela Resolução n.º 17/2018, de 21 de junho. Esta política é orientada, entre outros, pelo "Princípio da Segurança da Informação", segundo o qual 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. A política apresenta um glossário onde é definido "Serviço de criptografia" como qualquer serviço que é prestado a um remetente ou a um destinatário da mensagem de dados ou a qualquer pessoa que armazene uma mensagem de dados, e que é concebido para facilitar a utilização de técnicas de codificação por forma a garantir que os referidos dados ou mensagens de dados possam ser acessados ou possam ser colocados em forma legível somente por certas pessoas; garantir que a autenticidade ou integridade dos referidos dados ou mensagem de dados é capaz de ser verificada; garantir a autenticidade dos dados ou da mensagem de dados, e; garantir que a fonte dos dados ou da mensagem de dados pode ser corretamente identificada.

O Sistema Nacional de Arquivos do Estado (SNAE) de 2007, um dos resultados da EGDAE apresentada acima, foi revisto pelo Decreto n.º 84/2018, de 26 de dezembro. Entre vários objetivos (art. 5°), o SNAE visa assegurar a proteção e preservação dos documentos gerados e recebidos nos órgãos e instituições públicos e privados, revestidos de valor administrativo, histórico e científico. Sobre a "Custódia e Gestão de Documentos", o sistema

indica, no art. 25°, que os órgãos e instituições a que se aplica o SNAE devem assegurar a proteção e conservação da sua integridade, fidedignidade e autenticidade.

Dois instrumentos legais que à semelhança da Lei de Transações Electrónicas, muito avançam sobre proteção de dados pessoais, são o Regulamento de Protecção do Consumidor do Serviço de Telecomunicações e Regulamento de Segurança de Redes de Telecomunicações. O primeiro, aprovado pelo Decreto n.º 44/2019, de 22 de Maio, dispões no art. 10° que o "consumidor deve ter direito à privacidade e protecção contra o uso não autorizado da sua informação pessoal". Sobre o "Registos de consumidor" (art. 17°), o regulamento aponta que o operador de telecomunicações, quando aplicável, deve possuir uma base de registro de clientes que sirva de fonte de informação para as autoridades competentes em caso de averiguações judiciais ou indícios criminais. Depreende-se assim que estas informações devem ter consigo preservadas as qualidades diplomáticas. O segundo, aprovado pelo Decreto n.º 66/2019, 1 de agosto, tem como objetivos (art. 4°) garantir a disponibilidade, integridade, confidencialidade e autenticidade; a proteção de dados, transparência, qualidade das comunicações e resiliência da infraestrutura de rede; entre outros. Das "Obrigações do operador de telecomunicações" (art. 8°), o operador de rede e de serviços públicos de telecomunicações baseados em nuvem deve assegurar a confidencialidade, integridade, disponibilidade e privacidade de todos os recursos e informações. À "todos recursos e informações" entendemos que os dados pessoais estejam inclusos. Desta feita, o regulamento indica as qualidades diplomática de integridade e autenticidade viradas aos dados, mas também à infraestrutura tecnológica.

A questão da certificação digital apresentada como parte da Lei das Transações Electrónicas, teve, em 2019 a sua criação em dispositivo específico, o Decreto n.º 59/2019, de 3 de julho, que Cria o Sistema de Certificação Digital de Moçambique e aprova o Regulamento do Sistema de Certificação Digital de Moçambique. O sistema estabelece uma estrutura de confiança eletrónica, de forma que as entidades certificadoras que lhe estão subordinadas disponibilizem serviços que garantam a realização de transações eletrónicas seguras; a autenticidade, integridade, confidencialidade, validade jurídica e não repúdio das assinaturas eletrónicas de transações ou informações em documentos eletrónicos (art. 4°).

O sistema é composto por um Comité Gestor (CG); Autoridade Certificadora Raiz do Estado (ACR); Entidades Certificadoras (EC), e; Entidades de Registo (ER) vinculadas às Entidades Certificadoras (art. 5°). Ora, na gestão das suas chaves a EC é responsável por

assegurar a integridade e autenticidade das chaves públicas e de qualquer parâmetro a elas associado durante a distribuição, e estabelecer um processo que permita autenticar a sua origem, bem como garantir a segurança e integridade do equipamento criptográfico durante a sua vida útil, e assegurar que o mesmo não seja acedido ou alterado por pessoal não autorizado. Quanto ao "Arquivo de Informação" (art. 32°), está decretado que a documentação referente ao funcionamento dos serviços de certificação, incluindo avarias, situações operacionais especiais, e a informação respeitante ao registro, é mantida em ficheiro eletrónico e conservada pelo período mínimo de 20 anos, sendo que a Entidade Certificadora assegura a confidencialidade e integridade da informação conservada em arquivo, relativa aos certificados qualificados.No art. 36° sobre "Preservação de Longo Prazo", o sistema aponta que Entidades Certificadoras devem informar os requerentes de certificados que para assegurar a preservação de longo prazo dos documentos eletrónicos aos quais tenham sido apostas assinaturas eletrónicas, será necessária a periódica aplicação de mecanismos que assegurem a sua integridade.

Foi aprovada pela Resolução n.º 69/2021, de 31 de dezembro, uma política bastante conexa à proteção de dados pessoais, a Política de Segurança Cibernética e Estratégia da sua Implementação. A resolução indica que um dos impactos que se espera com a implementação da mesma é "melhoria na integridade, autenticidade e segurança na tramitação de documentos oficias e na comunicação entre várias entidades." Alias, um dos pilares que regem esta política é a "Protecção de Activos de Informação". Aqui o objetivo é a proteção de informação e aplicações, através de estabelecimento de programas de certificação de qualidade e segurança das aplicações e infraestruturas, estratégias de proteção da confidencialidade, integridade e disponibilidade da informação, regulamentos de proteção de informação, etc. No seu glossário é definida integridade como a garantia de que os dados permaneçam íntegros e sem qualquer alteração quando disponibilizados. E autenticidade como a propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

5 CONSIDERAÇÕES FINAIS

Neste artigo, nos concentramos no nível nacional da política de informação, observando-a concretamente em Moçambique onde procuramos compreender a gestão de

dados pessoais, buscando elementos na legislação oferecida pela(s) política(s) existente(s) e nas qualidades diplomáticas que esta apresenta. Ora, foi constatado que Moçambique não possui ainda uma política de informação e/ou uma política de arquivo enquanto um documento norteador, traduzido em programas, que poderia melhor avançar diretrizes no que concerne às qualidades diplomáticas que devem ser preservadas em todo o processo de gestão de dados pessoais.

Constatamos ainda que a legislação moçambicana analisada, na sua maioria, aponta apenas as qualidades de autenticidade e integridade de documentos e/ou informação, e, na sua totalidade, não aponta a qualidade diplomática de confiabilidade. Esta mesma legislação não apresenta diretamente estas e/ou outras qualidades diplomáticas para os dados, especificamente dados pessoais. A gestão de dados e/ou informações pessoais aparece no quadro legal moçambicano sem designação explícita. Da análise feita, percebemos a indicação de diferentes momentos da gestão desses dados em diferentes normativas. Do mesmo modo, as qualidades diplomáticas desses dados e sua preservação são muitas vezes indicadas nas entrelinhas ou indiretamente.

Concluímos que existem bases para uma normativa de proteção de dados pessoais específica e que de forma específica possa também sublinhar a gestão de dados pessoais. Entendemos ainda que essa normativa deveria conhecer a sua criação dentro de um quadro de política de informação nos moldes que defendemos acima, de tal modo que as qualidades diplomáticas inerentes à eles sejam melhor salvaguardadas.

A realização deste artigo abre campo para discutirmos, num próximo artigo, a questão da qualidade de dados pessoais na legislação de Moçambique, buscando alicerces na Lei Geral de Proteção de Dados do Brasil e no Regulamento Geral de Proteção de Dados da União Europeia.

REFERÊNCIAS

DANIEL, E. Information Policy. **University of North Carolina at Chapel Hill**. School of Information and Library Science. Disponível em: https://ils.unc.edu/daniel/info-policy.html#policya. Acesso em: 30 jun. 2023.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, v. 12, n. 2, p. 91-108, 2011.

DURANTI, L. Diplomatics: New Uses for an Old Science, Part I. **Archivaria**, p. 7-27, 1989.

DURANTI, L. From Digital Diplomatics to Digital Records Forensics. **Archivaria**, p. 39-66, 2009.

DURANTI, L. Reliability and Authenticity: The Concepts and Their Implications. **Archivaria**, p. 5-10, 1995.

DURANTI, L.; EASTWOOD, T.; MACNEIL, H. **Preservation of the Integrity of Electronic Records**. Dordrecht: Springer Netherlands, 2002.

EFING, A. C.; CATUZO, M. E. A Proteção Jurídica dos Dados Pessoais na Internet. **Revista Internacional Consinter de Direito**, p. 323-342, 2016.

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.

GODINHO, A. M.; NETO, G. R. Q.; TOLÊDO, R. C. M. A responsabilidade civil pela violação a dados pessoais. **Revista IBERC**, v. 3, n. 1, 2020.

JARDIM, J. M.; SILVA, S. C. DE A.; NHARRELUGA, R. S. Public policy analysis: an approach towards public policies on information. **Perspectivas em Ciência da Informação**, v. 14, p. 2-22, 2009.

LAURIAULT, T. P. *et al.* Today's Data are Part of Tomorrow's Research: Archival Issues in the Sciences. **Archivaria**, p. 123-179, 2007.

MACNEIL, H. **Trusting Records**. Dordrecht: Springer Netherlands, 2000.

MADSEN, W. **Handbook of Personal Data Protection**. London: Palgrave Macmillan UK, 1992.

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.

MOÇAMBIQUE. Constituição da República de Moçambique. **Boletim da República**. I SERIE, n.° 51, 2004.

MOÇAMBIQUE. Decreto n.° 84/2018, 26 de Dezembro de 2018. Aprova a revisão do Sistema Nacional de Arquivos do Estado abreviadamente designado SNAE e revoga o Decreto n.° 36/2007, de 27 de Agosto. **Boletim da República.** I SERIE, n.° 252, 2018.

MOÇAMBIQUE. Decreto n.º 44/2019, 22 de Maio de 2019. Aprova o Regulamento de Protecção do Consumidor do Serviço de Telecomunicações. **Boletim da República.** I SÉRIE, n.° 98, 2019.

MOÇAMBIQUE. Decreto n.º 59/2019, 3 de Julho de 2019. Cria o Sistema de Certificação Digital de Moçambique e aprova o Regulamento do Sistema de Certificação Digital de Moçambique. **Boletim da República.** I SÉRIE, n.° 127, 2019.

MOÇAMBIQUE. Decreto n.º 66/2019, 1 de Agosto de 2019, Aprova o Regulamento de Segurança de Redes de Telecomunicações. **Boletim da República.** I SÉRIE, n.° 148, 2019.

MOÇAMBIQUE. Lei n.º 3/2017, 9 de janeiro de 2017, Lei de Transacções Electrónicas. **Boletim da República.** I SÉRIE, n.° 5, 2017.

MOÇAMBIQUE. Lei n.º 34/2014, 31 de Dezembro de 2014. Lei do Direito à Informação. **Boletim da República.**, I SÉRIE, n.° 105, 2014.

MOÇAMBIQUE. Resolução n.º 17/2018, 21 de Junho de 2018. Aprova a Política para a Sociedade da Informação de Moçambique. **Boletim da República.** I SÉRIE, n.°122, 2018.

MOÇAMBIQUE. Resolução n.º 46/2006, 26 de Dezembro de 2006. Aprova a Estratégia para a Gestão de Documentos e Arquivos do Estado. **Boletim da República.** I SERIE, n.° 51, 2006.

MOÇAMBIQUE. Resolução n.º 69/2021, 31 de Dezembro de 2021. Aprova a Política de Segurança Cibernética e Estratégia da sua Implementação. **Boletim da República.** I SÉRIE, n.° 253, 2021.

MOÇAMBIQUE. Resolução nº 3/97, 18 de Fevereiro de 1997. Política e Estratégia de Informação. **Boletim da República.** I SÉRIE, n.° 7, 1997.

MONTVILOFF, V. **Políticas nacionales de información**: manual sobre la formulación, aprobación, aplicación y funcionamiento de una política nacional sobre la información - UNESCO Bibliothèque Numérique. Paris, 1990.

NOLASCO, L. G.; SILVA, B. D. M. Crimes cibernéticos, privacidade e cibersegurança. **Revista Quaestio Iuris**, v. 15, n. 4, p. 2353-2389, 2022.

ROBERTS, D. Defining electronic records, documents and data. **ARCHIVES AND MANUSCRIPTS**, v. 22, n. 1, p. 14-26, 1994.

ROJE, R. Data Practices and Management. *In*: MARUSIC, A. (Ed.). **A Guide to Responsible Research**. Collaborative Bioethics. Cham: Springer International Publishing, 2023. p. 65-81.

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.

SILVA, E. P.; CARDOSO, C. As relações entre arquivologia e a Lei Geral de Proteção de Dados: uma análise dos cursos da Enap sobre LGPD. **P2P E INOVAÇÃO**, v. 8, n. 2, p. 141-159, 2022.

SILVEIRA, C. R.; KARPINSKI, C. A diplomática contemporânea no atendimento aos princípios da Lei Geral de Proteção de Dados. **Brazilian Journal of Information Science**, v. 17, p. 7, 2023.