RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano V, v.1, n.1, jan/julho 2025. | submissão: 19/06/2025 | aceito: 21/06/2025 | publicação:23/06/2025

Acesso ilegítimo como forma de violação de dados em Moçambique

Illegitimate access as a form of data breach in Mozambique

El acceso ilegítimo como forma de violación de datos en Mozambique

Raúl de Miguel Benjamim Jofrisse Nhamitambo[1]
Álvaro Rui Massingue[2]
Elvis Ernesto Job[3]
Emerson Sérgio Guissiuana[4]
Juvêncio Jonas Miambo[5]

RESUMO

A presente pesquisa tem como objectivo analisar sobre Acesso Ilegítimo como forma de Violação de Dados em Moçambique. No contexto moçambicano, o acesso ilegítimo a dados emerge como um desafio crítico na contemporaneidade digital, caracterizado pela obtenção, uso, modificação ou divulgação de informações digitais sem a devida autorização ou amparo legal. A Lei das Transacções Electrónicas de Moçambique (aprovado pela Lei n.º 3/2017, de 9 de Janeiro) e o Código Penal (aprovado pela Lei n° 24/2019, de 24 de Dezembro), retratam sobre o acesso não autorizado a sistemas informáticos ou bases de dados, sublinhando a seriedade com que o legislador encara esta problemática. A crescente digitalização dos serviços, tanto no sector público quanto no privado, acentua a importância da protecção de dados. A exposição ou uso indevido de informações pessoais e sensíveis pode desencadear uma série de consequências prejudiciais. O avanço das tecnologias da informação em Moçambique trouxe consigo oportunidades, mas também sérios riscos à privacidade e à segurança digital dos cidadãos e instituições. Um dos principais riscos é o acesso ilegítimo a dados pessoais, que

[1] Doutor em Ciências Jurídicas, pela Universidade Para La Cooperación Internacional México (UCIMEXICO) – México (2020); Mestre em Assessoria Jurídica de Empresas, pela Universidad a Distancia de Madrid (UDIMA) - Madrid (2016); Licenciado Ciências Jurídicas e Investigação Criminal, pelo extinto Instituto Superior de Ciências e Tecnologia Alberto Chipande (ISCTAC) – Beira (2011); Advogado e Membro da Ordem dos Advogados de Moçambique (desde Abril de 2018); Professor Auxiliar de Direito das Tecnologias de Informação e Comunicações (Direito das TIC's) – na Universidade Joaquim Chissano (UJC) – Maputo (desde Fevereiro de 2020), no Curso de Licenciatura em Engenharia de Tecnologias e Sistemas de Informação; Professor Auxiliar de Direito Administrativo e Noções de Direito Administraticvo – na Universidade Pedagógica de Maputo (UP - Maputo), nos Cursos de Licenciaturas em Gestão de Recursos Humanos e Gestão Pública e Educacional; Técnico Superior de Assistência Jurídica – Gabinete Jurídico (UP - Maputo); Docente Universitário de Introdução ao Direito, Direito Administrativo I e II e, Direito de Trabalho, nos Cursos de Licenciatura em Direito, Contabilidade e Auditoria e, Administração Pública e Autárquica – no Instituto Superior Maria Mãe de África (ISMMA); Professor Auxiliar no Instituto Superior de Contabilidade e Auditoria de Moçambique (ISCAM), leccionando a disciplina Complementos de Fiscalidade no Curso de Mestrado em Auditoria; Autor, Revisor, Avaliador Externo e Parecista na Revista Científica Multidisciplinar O Saber (desde II Semestre de 2024); Autor, Avaliador e Parecista na Revista Multidisciplinar RECIMA21 (desde I Semestre de 2025) e Avaliador e Parecerista na Revista Internacional Consinter de Direito (Conselho Internacional de Estudos Contemporâneos em Pós-Graduação – CONSINTER), desde II Semestre de 2025 e Organizador da Editora Científica Digital (Desde I Semestre de 2025). Matola – Maputo.

ORCID: 0009-0006-4118-1970. rnhamitambo@gmail.com.(+258) 872058783/847417800.

[2] Estudante do 3° ano do Curso de Licenciatura (Graduação) em Engenharia em Tecnologias e Sistemas de Informação na Universidade Joaquim Chissano.

[3] Estudante do 3° ano do Curso de Licenciatura (Graduação) em Engenharia em Tecnologias e Sistemas de Informação na Universidade Joaquim Chissano.

[4] Estudante do 3° ano do Curso de Licenciatura (Graduação) em Engenharia em Tecnologias e Sistemas de Informação na Universidade Joaquim Chissano.

[5] Estudante do 3° ano do Curso de Licenciatura (Graduação) em Engenharia em Tecnologias e Sistemas de Informação na Universidade Joaquim Chissano.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

consiste na obtenção, utilização ou manipulação de informações privadas sem o devido consentimento ou autorização legal.

Palavras-chave: Acesso Ilegítimo; Violação de Dados; Privacidade; Segurança Digital.

ABSTRACT
This research aims to analyze Illegitimate Access as a form of Data Violation in Mozambique. In the Mozambican context, illegitimate access to data emerges as a critical challenge in the digital contemporary world, characterized by the obtaining, use, modification or disclosure of digital information without due authorization or legal support. The Electronic Transactions Law of Mozambique (approved by Law No. 3/2017, of January 9) and the Penal Code (approved by Law No. The increasing digitalization of services, both in the public and private sectors, emphasizes the importance of data protection. The exposure or misuse of personal and confidential information can trigger a series of harmful consequences. The advancement of information technologies in Mozambique has brought with it opportunities, but also serious risks to the privacy and digital security of citizens and institutions. One of the main risks is illegitimate access to personal data, which consists of obtaining, using or manipulating private information without due consent or legal authorization.

Keywords: Illegitimate Access; Data Breach; Privacy; Digital Security.

RESUMEN

Esta investigación tiene como objetivo analizar el acceso ilegítimo como una forma de violación de datos en Mozambique. En el contexto mozambiqueño, el acceso ilegítimo a los datos emerge como un desafío crítico en el mundo digital contemporáneo, caracterizado por la obtención, uso, modificación o divulgación de información digital sin la debida autorización o soporte legal. La Ley de Transacciones Electrónicas de Mozambique (aprobada por la Ley No. 3/2017, de 9 de enero) y el Código Penal (aprobado por la Ley No. La creciente digitalización de los servicios, tanto en el sector público como en el privado, enfatiza la importancia de la protección de datos. La exposición o el uso indebido de información personal y confidencial puede desencadenar una serie de consecuencias perjudiciales. El avance de las tecnologías de la información en Mozambique ha traído consigo oportunidades, pero también graves riesgos para la privacidad y la seguridad digital de los ciudadanos e instituciones. Uno de los principales riesgos es el acceso ilegítimo a datos personales, que consiste en obtener, usar o manipular información privada sin el debido consentimiento o autorización legal.

Palabras - clave: Acceso ilegítimo; Violación de datos; Privacidad; Seguridad digital.

INTRODUÇÃO

No presente trabalho abordaremos sobre Acesso Ilegítimo como forma de Violação de Dados em Moçambique. A crescente digitalização das sociedades contemporâneas tem trazido consigo

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

uma série de desafios, especialmente no que diz respeito à segurança da informação e à proteção de dados pessoais.

Em Moçambique, o acesso ilegítimo a dados tem-se tornado uma preocupação crescente, refletindo não apenas a vulnerabilidade das infraestruturas tecnológicas, mas também a falta de uma legislação robusta que regule a privacidade e a proteção de dados. Este fenómeno não é apenas uma questão técnica, mas também social, uma vez que a violação de dados pode ter consequências devastadoras para indivíduos e organizações, comprometendo a confiança pública e a integridade das instituições. A relevância deste tema é evidente, considerando o contexto actual de Moçambique, onde a digitalização avança rapidamente, mas sem a devida atenção às questões de segurança.

A falta de conscientização sobre a importância da protecção de dados e a escassez de recursos para a implementação de medidas de segurança eficazes agravam ainda mais a situação. Além disso, a interconexão crescente entre sistemas e plataformas digitais torna o País um alvo atractivo para cibercriminosos, que exploram as fragilidades existentes.

Na era digital contemporânea, a protecção de dados pessoais e corporativos tornou-se uma preocupação fundamental para indivíduos, organizações e governos em todo o mundo. Em Moçambique, País que experimenta um crescimento significativo no uso de tecnologias de informação e comunicação, o acesso ilegítimo a dados emerge como uma ameaça cada vez mais preocupante à privacidade, segurança e estabilidade econômica.

O acesso ilegítimo pode ser definido como a entrada não autorizada em sistemas informáticos ou bases de dados, com o intuito de visualizar, copiar, modificar ou destruir informações confidenciais. Essa prática constitui uma violação grave dos direitos fundamentais à privacidade e à proteção de dados pessoais, além de representar uma ameaça à segurança nacional e à integridade das instituições. A Constituição da República de Moçambique, promulgada em 2004, estabelece no seu artigo 71 o direito à privacidade, incluindo a inviolabilidade das comunicações. No entanto, a legislação específica sobre protecção de dados e segurança da informação ainda apresenta lacunas significativas que dificultam o combate eficaz ao acesso ilegítimo e a outras formas de violação de dados.

A pesquisa é qualitativa e com método bibliográfico e documental.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

EMBASSAMENTO TEÓRICO

Acesso Ilegítimo e Violação de Dados

O acesso ilegítimo a sistemas de informação constitui uma das principais ameaças à segurança digital na atualidade. Segundo Sêmola (2014), o acesso ilegítimo pode ser definido como "qualquer tentativa de entrada ou utilização de recursos computacionais sem a devida autorização, visando comprometer a confidencialidade, integridade ou disponibilidade das informações". Esta definição abrange tanto ataques externos quanto internos, realizados por indivíduos não autorizados ou por pessoas que excedem as permissões que lhes foram concedidas. Já a violação de dados, de acordo com Pinheiro (2018), refere-se ao "comprometimento da confidencialidade, integridade ou disponibilidade de dados pessoais ou sensíveis, resultando em acesso não autorizado, destruição, perda, alteração ou divulgação". Na perspectiva moçambicana, essa definição ganha contornos específicos devido às particularidades sociais, econômicas e tecnológicas do país.

Evolução Histórica da Proteção de Dados

A proteção de dados pessoais emergiu como preocupação global a partir da década de 1970, com o advento das primeiras legislações específicas na Europa. Segundo Doneda (2019), a proteção de dados evoluiu de uma abordagem centrada na privacidade para um conceito mais abrangente de autodeterminação informativa, reconhecendo o direito dos indivíduos de controlar suas informações pessoais.

No contexto africano, a proteção de dados ganhou relevância mais recentemente. A União Africana adotou em 2014 a Convenção sobre Cibersegurança e Proteção de Dados Pessoais, também conhecida como Convenção de Malabo, estabelecendo um marco regional para a proteção de dados no continente (União Africana, 2014). Em Moçambique, o debate sobre proteção de dados ganhou impulso somente na última década, impulsionado pelo crescimento do uso de tecnologias digitais e pela maior conscientização sobre os riscos associados ao tratamento inadequado de informações pessoais.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Quadro Jurídico Internacional e Regional

A proteção de dados pessoais é reconhecida internacionalmente como um direito fundamental. Documentos como a Declaração Universal dos Direitos Humanos (1948) e o Pacto Internacional Pág. 2 sobre Direitos Civis e Políticos (1966) estabelecem o direito à privacidade como um direito humano fundamental.

No contexto europeu, o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, implementado em 2018, tornou-se uma referência global em termos de proteção de dados pessoais, influenciando legislações em todo o mundo (Carvalho, 2020).

No âmbito africano, além da Convenção de Malabo, a Carta Africana dos Direitos Humanos e dos Povos também oferece proteção à privacidade, embora não mencione explicitamente a proteção de dados (Makulilo, 2016).

Formas de Acesso Ilegítimo a Dados

De acordo com Cert.br (2022), as principais formas de acesso ilegítimo a dados incluem:

▪ Ataques de Phishing: Envolve a obtenção fraudulenta de informações sensíveis (senhas, números de cartão de crédito) através de falsificação de identidade, geralmente via e-mail ou websites falsos.

▪ Malware: Softwares maliciosos como vírus, trojans, ransomware e spyware, que são projetados para infiltrar sistemas, extrair dados ou causar danos.

▪ Ataques de Engenharia Social: Manipulação psicológica de pessoas para induzi-las a realizar acções ou divulgar informações confidenciais.

▪ Exploração de Vulnerabilidades: Aproveitamento de falhas em sistemas operacionais, aplicativos ou hardware para obter acesso não autorizado.

▪ Ataques de Força Bruta: Tentativas repetidas de descobrir senhas ou chaves de criptografia através de múltiplas combinações.

Impactos do Acesso Ilegítimo

Os impactos do acesso ilegítimo a dados são multidimensionais. Segundo estudo da IBM Security (2023), as violações de dados têm custos financeiros significativos para as

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

organizações, incluindo despesas com investigação, notificação, resposta técnica, perda de clientes e danos à reputação.

Para os indivíduos, as consequências incluem roubo de identidade, fraudes financeiras, danos à reputação e violação da privacidade. Em nível nacional, o acesso ilegítimo a dados governamentais ou de infraestruturas críticas pode representar ameaças à segurança nacional e à estabilidade social (Ponemon Institute, 2022).

Particularidades do Contexto Moçambicano

O contexto moçambicano apresenta particularidades que influenciam tanto a ocorrência quanto o combate ao acesso ilegítimo a dados. De acordo com Machava (2021), o rápido crescimento no uso de tecnologias digitais, combinado com baixos níveis de literacia digital e infraestrutura de segurança deficiente, cria um ambiente propício para violações de dados. Mussá (2020), identifica alguns desafios específicos do contexto moçambicano:

- Desigualdade Digital: O acesso desigual à internet e a tecnologias digitais cria disparidades na compreensão e capacidade de protecção contra ameaças digitais.
- Limitações Institucionais: A falta de recursos e capacidade técnica das instituições responsáveis pela aplicação da lei e regulação do ambiente digital.
- Conscientização Limitada: Baixos níveis de conscientização sobre segurança digital entre a população geral e mesmo entre profissionais de TI.
- Quadro Legal Incompleto: Lacunas na legislação específica sobre proteção de dados e cibersegurança.

RESULTADOS E DISCUSSÃO

Acesso Ilegítimo

O acesso ilegítimo constitui uma das principais formas de violação de dados, caracterizando-se pela obtenção, manipulação ou utilização de informações sem a devida autorização dos titulares ou responsáveis legais. Este fenómeno assume particular relevância no contexto das infraestruturas digitais, onde a crescente digitalização de processos e a massificação do

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

armazenamento de dados em sistemas informatizados ampliam as possibilidades de ocorrência de acessos não autorizados.

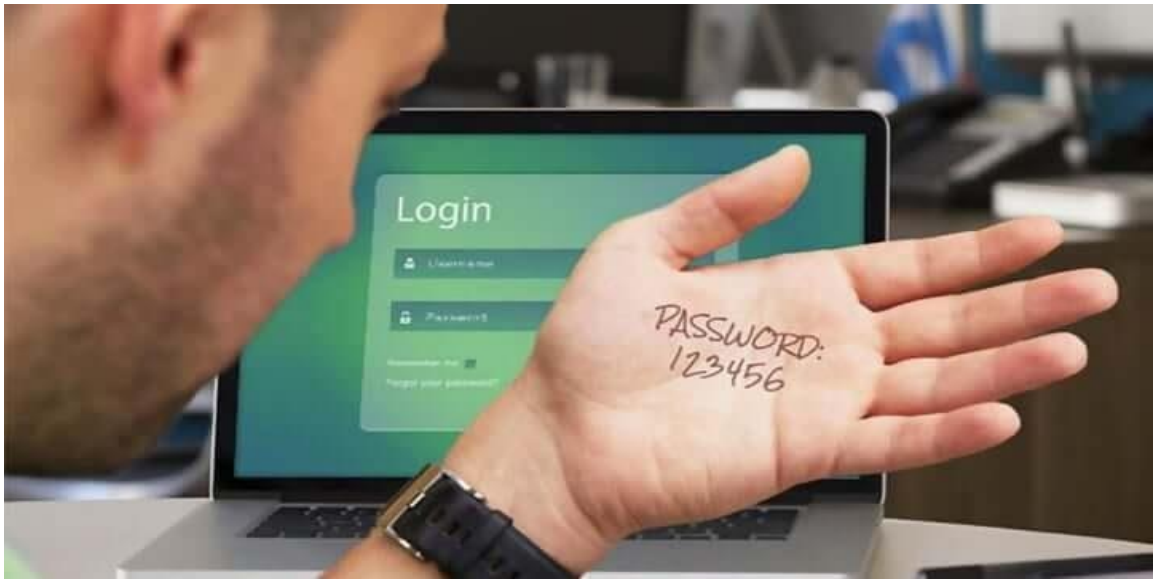
Segundo o artigo 256 da Lei 24/2019, de 24 de Dezembro, que aprova o Código Penal de Moçambique, o Acesso ilegítimo diz que quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, invadir um dispositivo alheio, fixo ou móvel, ligado ou não à rede de computadores, com o fim de obter informação não pública de correio ou comunicações electrónicas privadas, acesso a dados privados, segredos comerciais ou industriais, informações sigilosas ou o acesso remoto não autorizado do dispositivo, é punido com prisão de 1 a 2 anos e multa até 1 ano.

Causas do Acesso Ilegítimo

O acesso ilegítimo a sistemas e dados pode ocorrer por diversas razões, e no contexto moçambicano, esses desafios são particularmente relevantes. Vamos explorar cada uma dessas causas com exemplos específicos. Falta de medidas de segurança adequadas. Muitas instituições em Moçambique ainda não implementam protocolos robustos de protecção de dados.

Por exemplo, algumas entidades governamentais e empresas privadas não utilizam criptografia para proteger informações sensíveis, tornando-as vulneráveis a ataques. Em 2022, houve relatos de vazamento de dados em algumas instituições financeiras devido à falta de medidas de segurança eficazes.

Uso de credenciais fracas



Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Senhas fáceis de adivinhar continuam sendo um problema significativo. Em Moçambique, muitos usuários (pessoas físicas e pessoas colectivas públicas)ainda utilizam senhas simples como "123456" ou 5 "password", facilitando ataques de força bruta. Em 2023, um estudo indicou que diversas contas de serviços públicos foram comprometidas devido à reutilização de senhas fracas.

Ataques de engenharia social

Hackers exploram vulnerabilidades humanas para obter acesso a informações sensíveis. Um exemplo comum em Moçambique são os golpes via WhatsApp, onde criminosos se passam por funcionários de bancos ou empresas de telecomunicações para enganar usuários e obter credenciais de acesso. Casos de phishing também são frequentes, onde e-mails falsos solicitam informações bancárias.

Ausência de legislação específica e desafios na aplicação

Embora Moçambique tenha leis relacionadas à protecção de dados, como o Código Penal aprovado em 2019, a fiscalização ainda enfrenta desafios. A falta de regulamentação clara sobre crimes cibernéticos dificulta a punição de invasores. Em 2024, houve debates sobre a necessidade de uma lei específica de protecção de dados para fortalecer a segurança digital no país.

Consequências do acesso ilegítimo a violação de dados em Moçambique

As consequências do acesso ilegítimo a dados pessoais incluem: Violação da Privacidade, o acesso não autorizado a dados pessoais compromete a privacidade dos indivíduos, expondo informações sensíveis como convicções políticas, religiosas, filosóficas, origem étnica ou filiação partidária. O Código Penal, no artigo 316, tipifica como crime a criação, manutenção ou utilização ilícita de ficheiros automatizados contendo tais dados, impondo penas de prisão maior de dois a oito anos e multa até um ano.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Prejuízos Financeiros

O acesso ilegítimo a dados pode resultar em fraudes financeiras, como o uso indevido de informações bancárias ou pessoais para obtenção de benefícios ilícitos. O artigo 319 do Código Penal trata da burla por meios informáticos, punindo quem, com intenção de enriquecimento ilícito, causar prejuízo patrimonial a outrem mediante interferência no tratamento de dados ou uso não autorizado de programas informáticos.

Danos à Reputação

A divulgação não autorizada de dados pessoais pode prejudicar a imagem pública de indivíduos ou organizações, afetando sua credibilidade e confiança perante a sociedade. Embora o Código Penal não trate especificamente de danos à reputação, a violação de dados pode ser considerada uma forma de difamação ou calúnia, sujeitando o infrator às penas previstas para tais crimes.

Práticas de Segurança como Pilar da Protecção de Dados

Além da legislação, a implementação de práticas de segurança eficazes é crucial para proteger os dados pessoais. O Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC), destaca a importância de medidas como a autenticação multifatorial, criptografia de dados e a realização de auditorias regulares para garantir a integridade e a confidencialidade das informações. A criação de um Sistema de Certificação Digital fundamentado em criptografia de chave pública, conforme previsto no artigo 11 da Lei de Transacções Eletronicas (LTE), é uma das iniciativas para assegurar a autenticidade e validade jurídica dos documentos eletrônicos. A formação contínua de profissionais de tecnologia da informação e a conscientização dos cidadãos sobre a importância da protecção de dados também são essenciais. O INTIC promove acções para o desenvolvimento de um quadro de governança de dados, visando garantir o acesso, proteger os direitos individuais e impulsionar o desenvolvimento socioeconômico do país.

Importância da Protecção de Dados na Era Digital

Na era digital em que vivemos, a protecção de dados transcendeu a mera conveniência, tornando se um pilar fundamental para assegurar a privacidade, a segurança e a confiança nas interações eletrónicas que permeiam o nosso quotidiano. O avanço célere e a onipresença das

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

tecnologias de informação, das redes sociais, dos serviços financeiros digitais e dos sistemas governamentais online impulsionaram a colecta, o armazenamento e o processamento diário de quantidades massivas de dados, tanto pessoais quanto sensíveis. Este cenário, embora traga consigo inúmeras vantagens em termos de eficiência, conectividade e acesso à informação, também acarreta riscos significativos. A exposição ou o uso inadequado desses dados pode desencadear uma série de prejuízos graves, com impactos que se estendem desde a esfera individual até ao tecido social e institucional.

Tipos de Violação de Dados em Moçambique

Em Moçambique, o acesso ilegítimo a dados configura um desafio crescente na era digital, caracterizado pela obtenção, uso, modificação ou divulgação de informações digitais sem a devida autorização ou respaldo legal, o que constitui uma violação da privacidade e da segurança da informação.

Essa prática ilícita abrange diversas condutas, como a invasão de sistemas informáticos, o uso de credenciais alheias e a exploração de falhas técnicas para aceder a dados confidenciais. A Lei das Transacções Electrónicas de Moçambique (Lei n.º 3/2017, de 9 de janeiro) estabelece que, constitui infracção o acesso não autorizado a sistemas informáticos ou bases de dados, bem como a interceção, modificação ou uso de informação digital sem consentimento (Arts. 46.º e 47.º). Neste contexto, os tipos de violação de dados incluem:

Acesso não autorizado

O acesso não autorizado consiste na obtenção ilícita de dados por parte de indivíduos ou entidades que não possuem permissão para tal. Segundo Tipton e Krause (2014), esse tipo de violação representa uma das formas mais frequentes de ataques à segurança da informação, pois permite que o invasor visualize, copie ou manipule informações sensíveis sem deixar vestígios evidentes.

Em Moçambique, a Lei das Transacções Electrónicas (que aprova a Lei n.º 3/2017, de 9 de Janeiro), criminaliza explicitamente o acesso indevido a sistemas e dados eletrónicos, nos seus Artigos 46.º e 47.º. Tais actos são comuns em fraudes bancárias, invasões de contas em plataformas digitais e sistemas governamentais. Exemplo: Invasão de contas bancárias via apps móveis, acesso a registos de saúde ou educacionais sem permissão.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Relevância da Protecção de Dados

Com o crescimento do uso de serviços digitais no sector público (como o e-SISTAFE, e-SNIS, e-SNGRHE, plataformas de ensino online, entre outros), a violação de dados tornou-se um risco real para a privacidade dos cidadãos e a integridade das instituições. No entanto, o País ainda enfrenta desafios técnicos e legais, como:

• Fraca aplicação da legislação existente: As leis em vigor podem não ser aplicadas de forma consistente ou eficaz, seja por falta de recursos, capacidade institucional ou conscientização sobre a importância da protecção de dados.

• Baixo nível de literacia digital: A falta de conhecimento e habilidades digitais por parte dos cidadãos e até mesmo de algumas instituições pode torná-los mais vulneráveis a ataques cibernéticos e violações de dados, além de dificultar a adopção de práticas seguras de protecção de informações.

• Ausência de uma autoridade nacional específica para protecção de dados pessoais: Moçambique ainda não possui um órgão regulador independente e especializado em protecção de dados, o que limita a capacidade de fiscalização, supervisão e aplicação das leis, bem como a resposta a incidentes de violação de dados.

CONCLUSÃO

De concluir que, o acesso ilegítimo a dados pessoais é uma realidade preocupante em Moçambique. Embora o país tenha marcos constitucionais e legais relevantes, ainda há lacunas na aplicação prática e na fiscalização. A protecção eficaz dos dados depende da criação de um quadro regulatório mais completo, da capacitação das instituições e da consciência colectiva da sociedade. Investir na protecção de dados é, acima de tudo, investir na dignidade, na liberdade e na segurança dos cidadãos moçambicanos.

Em Moçambique, revela - se a urgente necessidade de reforçar a segurança digital no país. Apesar da existência de instrumentos legais, como o Código Penal e a Lei das Transações Eletrónicas, ainda persistem lacunas normativas e estruturais que comprometem a eficácia na prevenção e repressão de crimes informáticos. A crescente digitalização das instituições públicas

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

e privadas, aliada à falta de mecanismos de fiscalização eficazes, expõe os cidadãos a riscos crescentes de perda de privacidade, danos financeiros e reputacionais.

Para enfrentar esse cenário, torna-se essencial a aprovação de uma legislação específica de protecção de dados pessoais, alinhada com os padrões nacionais e internacionais, bem como a criação de uma autoridade independente que fiscalize seu cumprimento. Da mesma forma, o fortalecimento da infraestrutura de cibersegurança, a formação de profissionais qualificados e a promoção da educação digital junto à população são medidas indispensáveis.

A protecção de dados deve ser entendida não apenas como uma questão técnica, mas como um direito fundamental, diretamente ligado à dignidade, liberdade e segurança dos cidadãos. Moçambique precisa, portanto, investir numa abordagem integrada, preventiva e colaborativa, que una esforços legais, tecnológicos e sociais para garantir a integridade das informações e a confiança no ambiente digital.

REFERÊNCIAS

DIÁRIO ECONÓMICO. INTIC aponta ausência de regulamentação para protecção de dados 6 jun. 2024. Disponível em: https://www.diarioeconomico.co.mz/2024/06/06/economia/banca/intic-aponta-ausencia de-regulamentacao-para-proteccao-de-dados-financeiros, acessado aos 07 de Maio de 2025.

INSTITUTO NACIONAL DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO (INTIC). Actual quadro legal e regulamentar garante a protecção de dados pessoais em Moçambique. Disponível em: https://intic.gov.mz/actual-quadro legal-e-regulamentar-garante-a-proteccao-de-dados-pessoais-em-mocambique. , acessado aos 04 de Maio de 2025.

INTIC. INTIC dissemina mecanismos de proteção de dados pessoais. Disponível em: https://intic.gov.mz/intic-dissemina-mecanismos-de-protecao-de-dados-pessoais, acessado aos 06 de Maio de 2025.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Sommerville, I. (2011). Software engineering. Pearson Education. Fernanda farinelli, conceitos básicos de programação Orientada a objetos, (2007).

Solove, D. J. (2006). The digital person: Technology and privacy in the information age. NYU Press.

Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.

Tavares, José. Direito Digital e a Proteção de Dados em África. Maputo: Editora Acadêmica Moçambicana, 2022.

Tipton, H. F., & Krause, M. (Eds.). (2014). Information security management handbook (6th ed.). Auerbach Publications.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

LEGISLAÇÃO

MOÇAMBIQUE, Lei nº 24/2019, de 24 de Dezembro. Aprova a Lei de Revisão do Código Penal. Imprensa Nacional, Moçambique, MPT, 24 de Dezembro.

MOÇAMBIQUE, Lei n.º 11/**2023**: Altera o número 3, do artigo 311 da Constituição da República de **2004**, alterada pela Lei n.º 1/**2018**, de 12 de Junho. Imprensa Nacional, Moçambique, MPT, 12 de Junho.

MOÇAMBIQUE, Lei nº 3/2017, de 9 de Janeiro. Estabelece os princípios, normas gerais e o regime jurídico das Transacções Electrónicas e do governo electrónico. Imprensa Nacional, Moçambique, MPT, 9 de Janeiro.

MOÇAMBIQUE, Lei nº 8/2004 de 21 de Julho. Aprova a Lei das Telecomunicações. Imprensa Nacional, Moçambique, MPT, 21 de Julho.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

MOÇAMBIQUE, Decreto nº 75/2014 de, 12 de Dezembro. Aprova o Regulamento de Controlo de Trafego de Telecomunicações. Imprensa Nacional, Moçambique, MPT, 12 de Dezembro.

MOÇAMBIQUE, Lei nº 25/2019, de 26 de Dezembro. Aprova a Lei de revisão do Código de Processo Penal. Imprensa Nacional, Moçambique, MPT, 26 de Dezembro.

MOÇAMBIQUE, Decreto-Lei n2 1/2005, de 27 de Dezembro. Introduz alterações ao Código de Processo Civil. Imprensa Nacional, Moçambique, MPT, 27 de Dezembro.

CARTA INTERNACIONAL. Moçambique e a Convenção da União Africana sobre Cibersegurança Proteção de Dados Pessoais. https://www.cartainternacional.abri.org.br/Carta/article/view/1130, acessado em 08 de Maio de 2025.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.