MISA MOÇAMBIQUE

Policy Brief

Protecção de Dados em Moçambique: Da Necessidade à Urgência

Introdução e Contexto

Nos últimos anos, a protecção de dados pessoais tem emergido como uma preocupação central em diversas jurisdições ao redor do mundo, impulsionada pelo crescimento exponencial da tecnologia digital e da Internet.[1] Em Moçambique, este tema ganha particular relevância à medida que o país avança na sua agenda de modernização e digitalização, abrindo portas para novas oportunidades, mas também se expondo a riscos significativos relacionados à privacidade e segurança dos dados.[2]

A ausência de uma legislação robusta e a falta de uma cultura de protecção de dados têm deixado os cidadãos vulneráveis a violações de privacidade, uso indevido de informações pessoais e cibercrimes.[3] Esta situação exige uma resposta urgente para garantir que o direito à privacidade seja respeitado e que os dados pessoais sejam devidamente protegidos, alinhando-se com as melhores práticas internacionais.[4]

Neste contexto, a implementação de políticas de protecção de dados, em Moçambique, não é apenas uma necessidade, mas uma urgência. A introdução de uma legislação específica, a criação de mecanismos de fiscalização e a promoção de uma cultura de segurança da informação são passos essenciais para proteger os cidadãos e fomentar um ambiente digital seguro e confiável.[5]

Este *Policy Brief* analisa a situação actual da protecção de dados em Moçambique, destacando a urgência de medidas eficazes e propondo recomendações concretas para a formulação e implementação de políticas adequadas.

Situação Actual

Moçambique é um recente signatário da Convenção da União Africana sobre Ciber-segurança e Protecção de Dados Pessoais[6] ("Convenção da UA"), tendo assinado a 26 de Junho de 2018. Embora Moçambique ainda não tenha ratificado a Convenção da UA, isto pode indicar uma direcção geral para a forma como um quadro de protecção de dados se pode desenvolver na jurisdição.[7] Tal pressupõe dizer que em Moçambique não existe legislação específica sobre protecção de dados ou privacidade. No entanto, existem outras fontes de direito que impõem algumas obrigações em matéria de privacidade, como ilustra o quadro abaixo.

1 Kari Karppinen, Outi Puukko, Four Discourses of Digital Rights: Promises and Problems of Rights-Based Politics. Journal of Information Policy 1 May 2020; 10 304–328.

2 MISA Moçambique, Policy Brief 3 – Práticas e Experiências Internacionais de Legislação sobre Cibersegurança e dos Direitos Digitais https://misa.org.mz/index.php/quem-somos/planos-e-relatorios/relatorios/130-policy-brief-3-praticas-e-experiencias-internacionais-de-legislacao-sobre-ciberseguranca-e-dos-direitos-digitais?format=html, acesso em 15 de Julho de 2024.

3 MISA Moçambique, Policy Brief 3 – Práticas e Experiências Internacionais de Legislação sobre Cibersegurança e dos Direitos Digitais https://misa.org.mz/index.php/publicacoes/relatorios/130-policy-brief-3-praticas-e-experiencias-internacionais-de-legislacao-sobre-ciberseguranca-e-dos-direitos-digitais, acesso em 15 de Julho de 2024.

4 Tsandzana, D. (2022), Direitos digitais em Moçambique: abordagem, contexto e desafios, UP Maputo https://www.academia.edu/85773034/Direitos_digitais_em_Mo%C3%A7ambique_abordagem_contexto_e_desafios, acesso em 15 de Julho de 2024.

5 Op cit. 1.

6 Convenção da União Africana sobre Ciber-segurança e Protecção de Dados Pessoais https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection, acesso em 12 de Julho de 2024.

7 INOVA Legal, Direito Digital na Ordem Jurídica Moçambicana – algumas manifestações https://inovalegal.org/direito-digital-na-ordem-juridica-mocambicana-algumas-manifestacoes/, acesso em 12 de Julho de 2024.

Código Civil (Decreto-Lei n.º 47344, de 25 de Novembro de 1966, em vigor em Moçambique através do Edital n.º 22869, de 4 de Setembro de 1967)
Código Penal (Lei n.º 24/2019, de 24 de Dezembro, na redacção dada pela Lei n.º 17/2020, de 23 de Dezembro)
Lei do Trabalho (Lei n.º 23/2007, de 1 de Agosto) e a nova Lei do Trabalho (Lei n.º 13/2023, de 25 de Agosto)
A Lei das Transacções Electrónicas (Lei n.º 3/2017, de 9 de Janeiro)
Regulamento de Registo e Licenciamento dos Prestadores de Serviços Electrónicos Intermediários e dos Operadores de Plataformas Digitais (Decreto n.º 59/2023, de 27 de Outubro)
Resolução n.º 5/2019, de 20 de Junho, ratifica a Convenção da União Africana sobre Ciber-segurança e Protecção de Dados Pessoais ("Convenção da UA")

Tabela 1: quadro regulador sobre privacidade de dados

Existe uma especial atenção que deve ser dada ao Decreto 59/2023, que exige o registo dos prestadores intermediários de serviços electrónicos e dos operadores de plataformas digitais. Refira-se que a Lei das Transacções Electrónicas define o prestador de serviços intermediário como qualquer pessoa que, em representação de outra, envie, receba e armazene mensagens de dados, e também que preste serviços de acesso à rede ou preste serviços através de uma rede. A exigência de registo é aplicável aos Prestadores de Serviços Electrónicos Intermédios e Operadores de Plataformas Digitais que ofereçam serviços a receptores sediados ou localizados em Moçambique, independentemente do local onde os prestadores estejam sediados.

Para além da tabela 1 acima, a Constituição da República de Moçambique estabelece que todos os cidadãos têm direito à protecção da sua vida privada e têm direito à honra, ao bom nome, à reputação, à protecção da imagem pública e à reserva da intimidade da vida privada. Além disso, o artigo 71.º da Constituição identifica a necessidade de legislar sobre o acesso, a geração, a protecção e a utilização de dados pessoais informatizados (por entidades públicas ou privadas); no entanto, a legislação de implementação ainda não foi aprovada.

Lacunas e Ausências: Por uma Advocacia Urgente

Moçambique, ao assinar a Convenção da União Africana sobre Ciber-segurança e Protecção de Dados Pessoais[8] em 26 de Junho de 2018, demonstrou uma intenção clara de se alinhar com as normas internacionais de protecção de dados e segurança cibernética. No entanto, a falta de ratificação desta convenção e a ausência de uma legislação específica sobre protecção de dados no país revelam uma lacuna crítica que precisa ser preenchida com urgência.

Adicionalmente, o facto de Moçambique não possuir um quadro legal robusto para a protecção de dados pessoais deixa os cidadãos expostos a riscos significativos de violações de privacidade e ciber-crimes, tal e qual se viveu em 2022 diante da invasão de páginas virtuais do Governo de Moçambique[9] e os recorrentes ataques que atingem até 1,5 milhão de cidadãos mensalmente.[10] Ou seja, a inexistência de uma autoridade responsável pela supervisão das questões de protecção de dados agrava, ainda mais, a situação, resultando em uma aplicação mínima das práticas de segurança da informação. Sem requisitos obrigatórios de notificação de violações, há ausência de transparência e de resposta eficaz a incidentes de segurança que podem comprometer dados sensíveis.

Por conseguinte, a necessidade de uma advocacia urgente neste campo é evidente, sendo que a criação de uma legislação específica para a protecção de dados, acompanhada da implementação de mecanismos de fiscalização e controle, é imperativa. Além disso, é crucial fomentar uma cultura de segurança da informação entre os cidadãos e as instituições, públicas e privadas, promovendo a consciencialização sobre a importância da protecção de dados pessoais.

Enquanto MISA Moçambique, é nosso entendimento que a advocacia deve desempenhar um papel central na mobilização de recursos e na sensibilização da sociedade para a importância desta causa. Tal inclui a pressão sobre os legisladores para a criação de uma lei abrangente de protecção de dados, a capacitação de profissionais na área de segurança cibernética, e a promoção de práticas seguras entre as empresas e organizações que lidam com dados pessoais.

Defendemos que a protecção de dados, em Moçambique, não pode ser adiada. Ou seja, a segurança e a privacidade dos cidadãos dependem de acções rápidas e eficazes para estabelecer um ambiente digital seguro e confiável – a urgência de uma advocacia proactiva e determinada é a chave para assegurar que Moçambique possa enfrentar os desafios do mundo digital moderno e proteger os direitos dos seus cidadãos.

Legislação sim, mas não apenas!

Actualmente, não existe qualquer requisito de notificação de violações em Moçambique. Está a ser discutida uma Lei de Ciber-segurança que pretende estabelecer, entre outros aspectos, o regime jurídico aplicável à protecção das redes de comunicação de dados, dos dados, dos sistemas de informação e das infra-estruturas críticas no ciberespaço. Dado que Moçambique não tem leis específicas de protecção de dados nem uma autoridade específica responsável pela supervisão das questões de protecção de dados, a aplicação das questões relacionadas com a protecção de dados é mínima.

- A criação de uma legislação específica para a protecção de dados pessoais em Moçambique é uma medida essencial, mas, por si só, não é suficiente para garantir

8 Op cit. 4.

9 Rádio Moçambique, Vários sites governamentais moçambicanos invadidos por ataque cibernético https://www.rm.co.mz/varios-sites-governamentais-mocambicanos-invadidos-pelo-ataque-cibernetico/, acesso em 12 de Julho de 2024.

10 INTIC, Ataques Cibernéticos atingem 1,5 Milhão por mês em Moçambique https://www.intic.gov.mz/ataques-ciberneticos-atingem-15-milhao-por-mes-em-mocambique/, acesso em 12 de Julho de 2024.

a segurança e a privacidade dos cidadãos. A experiência de outras jurisdições demonstra que, além de um quadro legal robusto, é necessário um conjunto de acções complementares que assegurem a implementação eficaz e sustentável dessas normas, com destaque para:

i. A legislação deve ser acompanhada pela criação de uma autoridade independente de protecção de dados. Esta entidade será responsável por monitorar o cumprimento da lei, lidar com reclamações, aplicar sanções em caso de violações e promover a consciencialização sobre os direitos de privacidade. Sem uma autoridade dedicada, a aplicação das leis de protecção de dados corre o risco de ser ineficaz e fragmentada.
ii. É crucial investir em capacitação e formação contínua. Profissionais de todas as áreas, especialmente aqueles que lidam com grandes volumes de dados pessoais, precisam ser treinados nas melhores práticas de segurança da informação. A educação e a formação não devem se limitar ao setor tecnológico, mas devem incluir também áreas como o direito, a gestão e a saúde, onde a protecção de dados é igualmente crucial.
iii. A consciencialização pública também desempenha um papel vital. Os cidadãos devem ser informados sobre os seus direitos em relação à protecção de dados pessoais e sobre como podem se proteger contra possíveis violações. Campanhas de sensibilização, workshops e materiais educativos são ferramentas importantes para construir uma cultura de privacidade e segurança no país.
iv. Parcerias entre o governo, o sector privado e organizações da sociedade civil são igualmente importantes. O desenvolvimento de políticas e práticas eficazes de protecção de dados exige a colaboração de todos os setores. Empresas que operam em Moçambique, especialmente aquelas que lidam com dados sensíveis, devem adotar políticas rigorosas de protecção de dados e trabalhar em conjunto com o governo para garantir a conformidade com a legislação.
v. Finalmente, a infra-estrutura tecnológica deve ser fortalecida para suportar as exigências de protecção de dados. Tal inclui a implementação de sistemas seguros de armazenamento e transmissão de dados, bem como a adopção de tecnologias avançadas de segurança cibernética para prevenir e responder a incidentes de violação.

Em suma, enquanto a legislação é um passo crucial, a protecção de dados em Moçambique requer uma abordagem multifacetada que inclua supervisão independente, capacitação, consciencialização pública, parcerias estratégicas e infra-estrutura tecnológica robusta. Embora esteja em discussão em diferentes fóruns como se viu em Fevereiro de 2024[11], apenas com uma estratégia abrangente será possível assegurar a protecção eficaz dos dados pessoais e a privacidade dos cidadãos.

Recomendações

1. **Estabelecimento de uma Autoridade Independente de Protecção de Dados** é fundamental para garantir a implementação e a fiscalização eficaz da legislação de protecção de dados. Esta entidade deve ter poderes claros para monitorar o cumprimento das leis, investigar violações, aplicar sanções e promover a consciencialização pública sobre os direitos de privacidade. A independência desta autoridade é crucial para assegurar que ela possa operar sem influências externas e focar na protecção dos direitos dos cidadãos.

2. **Desenvolvimento e Implementação de Programas de Capacitação** é essencial para a construção de uma cultura de segurança da informação. Estes programas devem abranger diversas áreas, incluindo tecnologia da informação, direito, saúde e gestão. A capacitação deve focar nas melhores práticas de segurança, conformidade com a legislação e resposta a incidentes de violação de dados, garantindo que os profissionais estejam preparados para proteger eficazmente os dados pessoais sob sua responsabilidade.

3. **Campanhas de Consciencialização Pública** é crucial para informar os cidadãos sobre seus direitos de privacidade e como proteger seus dados pessoais. Estas campanhas podem incluir workshops, seminários, materiais educativos e uso de *media* sociais para alcançar um público amplo. A consciencialização pública ajuda a criar uma cultura de privacidade e segurança, capacitando os cidadãos a tomar medidas proativas para proteger suas informações pessoais e a exigir que organizações e instituições respeitem seus direitos de privacidade.

4. **Fortalecimento da Infra-estrutura Tecnológica** é necessário para suportar as exigências de protecção de dados em um ambiente digital. Isso inclui a implementação de sistemas seguros de armazenamento e transmissão de dados, a adopção de tecnologias avançadas de segurança cibernética e a realização de auditorias regulares de segurança. Além disso, é importante desenvolver uma estratégia nacional de ciber-segurança que inclua medidas de prevenção e resposta a incidentes, garantindo que o país esteja preparado para enfrentar ameaças cibernéticas e proteger dados sensíveis de maneira eficaz.

Maputo, Agosto de 2024

11 INTIC, Na vanguarda da Segurança Digital: INTIC avança rumo à conclusão da Proposta de Lei de Crimes Cibernéticos https://www.intic.gov.mz/na-vanguarda-da-seguranca-digital-intic-avanca-rumo-a-conclusao-da-proposta-de-lei-de-crimes-ciberneticos/, acesso em 12 de Julho de 2024.