



Policy Brief

PROTECÇÃO DE DADOS PÉSSOAIS EM MOÇAMBIQUE

OPORTUNIDADES E DESAFIOS PARA
A GARANTIA DE DIREITOS NO ESPAÇO DIGITAL

Parceiros:



INTRODUÇÃO

A Proposta de Lei de Protecção de Dados Pessoais, submetida à Assembleia da República, constitui uma oportunidade para reforçar os direitos dos cidadãos e estabelecer responsabilidades mais claras na recolha, utilização e partilha de informação pessoal. O seu impacto dependerá da qualidade das garantias jurídicas e da capacidade das instituições para as tornar efectivas. Este *policy brief* sistematiza as oportunidades e os desafios para a protecção de dados dos cidadãos em Moçambique, e apresenta recomendações para o aperfeiçoamento e a implementação da futura lei. A análise parte de uma preocupação central: assegurar que a transformação digital proteja a privacidade, preserve as liberdades fundamentais e amplie a participação dos cidadãos.

PRINCIPAIS CONSTATAÇÕES

i. Uma oportunidade para tornar os direitos efectivos

A protecção de dados pessoais encontra fundamento no artigo 71 da Constituição da República de Moçambique e nos compromissos assumidos por Moçambique no âmbito da Convenção de Malabo (Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais). A adopção de um regime transversal permite, assim, consolidar garantias actualmente dispersas e tornar mais claras as obrigações das entidades públicas e privadas, tanto no tratamento de registos físicos como de informação digital. Os direitos de informação, acesso, rectificação, oposição, eliminação e portabilidade previstos na proposta podem reforçar o controlo dos cidadãos sobre a sua informação. A sua concretização deve permitir conhecer as finalidades do tratamento, corrigir registos incorrectos e reagir ao uso abusivo de dados. Para isso, os procedimentos precisam de ser compreensíveis, acessíveis e acompanhados de meios efectivos de reclamação e reparação.

ii. Independência da fiscalização

A proposta prevê um Conselho Nacional de Protecção de Dados Pessoais presidido pelo Primeiro-Ministro e atribui as funções de Autoridade Nacional de Protecção de Dados Pessoais ao regulador das tecnologias de informação e comunicação que presentemente é o INTIC – Instituto Nacional de Tecnologias de Informação e Comunicação. Embora reconheça autonomia e independência funcional e decisória, mantém a tutela ministerial e remete aspectos da organização da autoridade para regulamentação.

Este modelo exige garantias que permitam fiscalizar o próprio Estado sem interferências, já que o Estado é, também ele, um activo processador de dados pessoais. A independência da Autoridade, em nosso entender, deve, assim, traduzir-se na selecção transparente dos dirigentes, estabilidade dos mandatos, condições restritas de destituição, recursos adequados e liberdade de decisão. A coordena-

ção política do sistema não deve abranger a direcção de investigações, reclamações ou processos sancionatórios que deverão ser levados a cabo de modo completamente independente pela Autoridade.

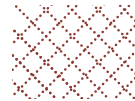
iii. Segurança pública e protecção contra abusos

As excepções à aplicação dos comandos da lei por motivos de segurança pública e defesa nacional colocam um dos principais desafios à efectividade da futura lei. A exigência de fundamentação, necessidade e proporcionalidade constitui uma salvaguarda relevante, mas precisa de ser acompanhada por limites verificáveis e supervisão independente de modo a assegurar que as excepções não criem áreas de tratamento de dados imunes à fiscalização da Autoridade. Neste contexto, importa delimitar as finalidades, a duração da conservação, as condições de acesso e os mecanismos de recurso. Por outro lado, a vigilância intrusiva deve estar sujeita a autorização judicial e controlo efectivo. Do mesmo modo, a interligação de bases de dados públicas deve respeitar finalidades determinadas e permissões de acesso: a capacidade técnica de cruzar informação não legitima qualquer utilização posterior.

iv. Liberdade de imprensa e direito à informação

A protecção de dados deve coexistir com o jornalismo de interesse público, a confidencialidade das fontes e o acesso à informação. A proposta em discussão reconhece um regime específico para fins jornalísticos, mas a sua articulação com as disposições sobre dados sensíveis, dados penais e poderes de fiscalização deve ser suficientemente clara para evitar restrições indevidas que podem colocar em causa a Liberdade de expressão e o direito de informar e ser informado.

A futura lei deve, por conseguinte, assegurar que a investigação jornalística não fica dependente de autorização administrativa prévia. Deve igualmente impedir que pedidos de eliminação ou invocações genéricas de privacidade sejam utilizados para ocultar informação relevante sobre



o exercício de funções públicas. Quando um documento contenha dados cuja divulgação deva ser limitada, a disponibilização parcial deve ser ponderada antes da recusa integral de acesso ao mesmo.

v. Conformidade proporcional e economia digital

A obrigação generalizada de designar encarregado de protecção de dados pode impor encargos desproporcionais a pequenas empresas, associações e órgãos de comunicação social com recursos limitados. As exigências organizativas devem atender à natureza, escala e risco do tratamento, sem reduzir os direitos dos titulares. Uma pequena organização que trate informação altamente sensível pode justificar obrigações reforçadas. A proposta depositada no Parlamento não procede a qualquer distinção entre entidades, partindo de uma obrigação de toda e qualquer entidade designar um encarregado de protecção de dados pessoais. É um ponto a ser revisto com cautela.

Por outro lado, a previsibilidade das regras também é essencial para serviços de computação em nuvem, contratação tecnológica e transferências internacionais. A proposta já contempla adequação, garantias contratuais e regras internas de grupos empresariais. A sua operacionalização deve, porém, evitar autorizações repetitivas e estabelecer critérios e prazos claros. O investimento em capacidade nacional de armazenamento deve combinar segurança, qualidade e custos acessíveis; a localização dos servidores, isoladamente, não garante a protecção dos cidadãos.

vi. Clareza das normas e capacidade de implementação

A articulação entre a comunicação imediata de incidentes e a notificação à autoridade em 72 horas exige clarificação dos destinatários da comunicação, condições e início da contagem dos prazos. As regras sobre crianças devem distinguir a definição de criança da idade para consentir autonomamente em determinados serviços digitais. O regime sancionatório deve também conter elementos essenciais suficientemente determinados na lei, assegurando previsibilidade e garantias de defesa.

A aplicação a tratamentos automatizados permite abranger sistemas de inteligência artificial, mas deve ser acompanhada por garantias específicas para decisões com efeitos relevantes no crédito, emprego ou acesso a serviços. Informação compreensível, possibilidade de contestação e intervenção humana efectiva são necessárias para prevenir discriminação e decisões que o cidadão não consegue questionar.

A proposta prevê regulamentação em 90 dias e entrada em vigor 180 dias após publicação. Este período exige preparação institucional, financiamento e formação. A falta de profissionais especializados, procedimentos internos e meios técnicos pode vir a limitar a aplicação da lei, sobretudo fora dos grandes centros urbanos.

vii. Literacia e inclusão

O reconhecimento de direitos produz resultados limitados quando os cidadãos não sabem como exercê-los. É, por isso, nosso entender que a informação sobre privacidade deve ser transmitida em linguagem simples, línguas locais e formato acessível. Crianças, pessoas com deficiência e cidadãos com menor literacia ou conectividade necessitam de meios adequados de compreensão e apoio. O exercício de direitos não deve depender exclusivamente de plataformas digitais.

viii. Recomendações

- **Aperfeiçoamento das garantias antes da aprovação** - Assembleia da República deve assegurar uma apreciação participativa da proposta e consolidar as garantias de independência da Autoridade, os limites às excepções de segurança e a protecção do jornalismo de interesse público. Deve também harmonizar as disposições sobre incidentes, crianças, decisões automatizadas e sanções. As garantias essenciais dos direitos fundamentais devem constar da própria lei.
- **Preparação de um programa nacional de implementação** - O Governo deve estabelecer um plano com orçamento, responsabilidades e metas verificáveis para o período de preparação e o primeiro ano de aplicação. O plano deve abranger a capacidade de fiscalização, a formação de profissionais e a adaptação dos serviços públicos. A articulação entre protecção de dados, cibersegurança, reguladores sectoriais e gestão documental deve evitar lacunas e sobreposição de competências, preservando a independência da fiscalização por parte da Autoridade.
- **Facilitação do cumprimento de acordo com o risco** - A autoridade deve disponibilizar orientações sectoriais, modelos de informação aos titulares, procedimentos de incidentes e instrumentos para transferências internacionais. A lei deve admitir soluções proporcionais, incluindo encarregados externos ou partilhados, com autonomia e disponibilidade asseguradas. A simplificação para actividades de baixo risco deve coexistir com fiscalização efectiva das operações mais sensíveis.

- **Preparação das organizações** - As instituições públicas e privadas devem identificar os dados que tratam, as finalidades, os fundamentos jurídicos e os destinatários. Devem rever contratos, acessos, conservação e segurança, e organizar procedimentos de resposta a incidentes e pedidos dos titulares. Saúde, identificação civil, serviços financeiros e telecomunicações devem merecer atenção prioritária, em função dos riscos envolvidos.
- **Reforço da participação e a monitoria pública** - A sociedade civil, os media e a academia devem contribuir para a divulgação de direitos, a formação e o acompanhamento da aplicação da lei. Importa promover jornalismo informado sobre protecção de dados e apoiar cidadãos perante violações. A monitoria deve considerar os tempos de resposta às reclamações, o cumprimento das medidas correctivas e a acessibilidade dos mecanismos de protecção, incluindo nas províncias.

CONCLUSÃO

A aprovação da Lei de Protecção de Dados Pessoais pode fortalecer a confiança nos serviços digitais e a capacidade dos cidadãos para defender os seus direitos. Esse resultado exige fiscalização independente, regras claras e instituições preparadas. O sucesso da regulação deve ser medido pela protecção efectiva das pessoas, pela preservação das liberdades e pela possibilidade de participar no espaço digital com segurança e autonomia.