Policy Brief - 2

O que aprender das experiências legislativas no âmbito da cibersegurança e direitos digitais à luz das práticas internacionais?

- **Apesar de Moçambique ter dado passos importantes na ratificação de instrumentos internacionais sobre cibersegurança e protecção de dados, o Governo e a Assembleia da República devem priorizar, no país, a harmonização do quadro legal em vigor, e aquele que for aprovado, às convenções e acordos internacionais assinados pelo governo no âmbito da SADC, União Africana e ITU.**
- **Baseando-se nos instrumentos internacionais e regionais de cibersegurança, a futura Lei sobre esta matéria deverá clarificar a fronteira entre as questões de segurança do Estado, a privacidade e as liberdades fundamentais dos cidadãos.**

Breve contextualização

Moçambique participa da União Internacional de Telecomunicações (ITU) e da Comunidade de Desenvolvimento da África Austral (SADC). O país é, também, signatário de parte dos instrumentos internacionais sobre cibersegurança e protecção de dados (Convenção de Malabo). Ao nível doméstico, possui um quadro legal não especificamente voltado à cibersegurança e direitos digitais, entre os quais a Lei de Transações Electrónicas Lei n. 03/2017 de 09 de Janeiro), a nova Lei das Telecomunicações (A Lei n. 04/2016 de 03 de Junho), a Lei da Revisão do Código Penal (Lei 24/2019 de 24 de Dezembro), que cobre os crimes informáticos e fraudes eletrônicas, o Decreto do Registo de Cartões SIM (Decreto n. 18/2015 de 28 de Agosto), e o Decreto sobre a Interoperabilidade do Governo Eletrónico (Decreto n. 67/2017 de 1 de Dezembro). Igualmente dispõe de uma Política para a Sociedade da Informação (Resolução 17/2018 de 21 de Junho) e do Plano Estratégico (2019-2028) desdobrado em Plano Operacional (2019-2023) para a construção da Sociedade da Informação em Moçambique[1].

Não obstante à relevância do quadro legal, das políticas e iniciativas de cibersegurança e protecção de dados em vigor no país, persistem desafios de regulação que, sendo transpostos, permitiriam que as matérias de cibersegurança e protecção de dados pessoais se traduzissem num compromisso do Estado (INITC, 2022). Trata-se de uma consciência assumida pelo Governo, através das instituições dedicadas à gestão das Tecnologias de Informação e Comunicação (TIC's)[2]. Este reconhecimento governamental representa um importante passo, ao transmitir não apenas a consciência da gravidade do problema no geral, mas a urgência de uma acção de aprimoramento do quadro legal sobre a segurança cibernética.

A referida consciência, todavia, contrasta com o aparente cepticismo quanto à adesão aos instrumentos internacionais que inspiram os processos legislativos dos países, tal é o caso da Convenção de Budapeste sobre o cibercrime (CBC), ainda não ratificada pelo Estado moçambicano. Trata-se de um instrumento que, entre várias disposições, insta aos Estados signatários a produzirem leis e políticas que punem os criminosos e protegem os cidadãos de potenciais crimes cibernéticos cometidos pelas instituições e seus servidores, em prejuízo do cidadão[3]. A não ratificação desta convenção ocorre num contexto de insuficiência do regime jurídico de recolha da prova electrónica; de incapacidade institucional para investigação, prossecução penal e judiciária; e de fraca cooperação dos provedores de serviços da Internet para o combate ao cibercrime, de acordo com a Procuradoria-Geral da República (PGR)[4]. Destaque-se, porém, que a não ratificação da CB não impede que o país dê passos nos processos legislativos progressistas nesta matéria, dado que a Convenção de Malabo (especialmente o artigo 8), já subscrita pelo Estado, consubstancia as recomendações da CB. É neste quadro que é produzido o presente documento, que reflecte as questões-chave levantadas no debate inserido nas celebrações do Dia Mundial da Liberdade de Imprensa (2022) que dedicou parte do tempo para uma reflexão sobre as experiências legislativas no âmbito da cibersegurança e direitos digitais à luz das práticas internacionais. O debate insere-se nas acções de advocacia para a produção de um quadro legal específico sobre cibersegurança e protecção de dados.

1 file:///C:/Users/User/Downloads/1130-Texto%20do%20artigo-4756-5474-10-20210929.pdf

2 Desafios assumidos pelo Presidente do Conselho de Administração do INTIC, Lourino Chemane, durante a sua intervenção na Conferência Nacional alusivo ao Dia Mundial da Liberdade de Imprensa.

3 Artigo 12º da Convenção de Budapest sobre Cibercrime.

4 Governante moçambicano, pela ratificação da Convenção de Budapeste sobre Crimes Cibernéticos – Instituto Nacional de Tecnologias de Informação e Comunicação (intic.gov.mz).

Dos instrumentos internacionais e regionais de cibersegurança e protecção de dados

O instrumento de referência africana sobre a matéria de cibersegurança e Protecção de Dados Pessoais é Convenção de Malabo (CM). Aprovada pela União Africana, em 2014, a convenção orienta os países a adoptarem uma série de medidas legislativas para lidar com o comércio eletrónico, com a proteção de dados e com o cibercrime. Entre as principais questões, o documento determina que os países adoptem políticas nacionais de cibersegurança, definam uma autoridade regulatória e infraestruturas críticas de cibersegurança. Obriga, igualmente, a aprovação de leis sobre cibersegurança que respeitem os Direitos Humanos e garantam a participação da sociedade civil nas consultas, por parte dos signatários. A CM recomenda que as leis prevejam a criação de Centros de Reposta de Incidentes Cibernéticos, *Computer Security Incident Response Team* (CSIRT), com recursos humanos qualificados, para prevenir e proteger as infraestruturas e os cidadãos de incidentes cibernéticos.

A Convenção de Budapeste sobre cibersegurança, outro instrumento importante, ainda não ratificado por Moçambique, assume-se como padrão dos processos legislativos sobre cibercrime a nível global. Se por um lado a convenção prevê, em larga escala, a salvaguarda de direitos e liberdades fundamentais no combate ao cibercrime, por outro clarifica as circunstâncias de actuação dos Estados para a salvaguarda da segurança colectiva (artigo 108).

Outro instrumento internacional é o Regulamento Geral de Proteção de Dados (RGPD), um diploma Europeu (EU 2016/679) que, apesar de não vincular directamente ao Estado moçambicano, determina as regras relativas à proteção, ao tratamento e à livre circulação dos dados pessoais das pessoas nos países da União Europeia. A relevância deste instrumento reside no facto de obrigar à prestação de informações aos titulares dos dados (a base legal para o tratamento de dados, o prazo de conservação e ainda informações mais detalhadas sobre as transferências internacionais e a possibilidade de apresentar queixa junto da Comissão Nacional de Proteção de Dados). A recolha e processamento de dados pessoais, à luz deste instrumento, fundamenta-se nos seguintes princípios: O consentimento do sujeito (o cidadão); A participação do sujeito de dados; Obrigação legal da qual o controlador é sujeito; A protecção de um interesse vital do sujeito de dados; o interesse público ou no interesse de uma autoridade oficial**;** interesses legítimos da entidade, exceto quando esses interesses forem anulados pelos interesses ou direitos e liberdades fundamentais do sujeito de dados, que requerem uma proteção de dados pessoais[5]. Os dados colectados, neste quadro, são unicamente utilizados para a finalidade a que se destinam[6], ao meso tempo em que o titular pode consultar os seus dados, em posse da empresa ou entidade pública, assim como aceder informa-se sobre o tratamento desses dados.

O regulamento de dados de cibercriminalidade é o outro instrumento da União Europeia. Este instrumento lida com aspectos relacionados à vigilância das telecomunicações. Todavia, é por muitos considerado bastante generalista, carecendo de pormenorização, para minimizar interpretações díspares, sobretudo no que às formas de garantia e respeito pelos Direitos Humanas diz respeito. Além disso, a aplicação prática da vigilância, à luz deste instrumento, fica ao critério dos tribunais. Os "13 Princípios Internacionais sobre a aplicação do Direito Humano à vigilância das comunicações", uma iniciativa da Sociedade Civil, é outro instrumento importante. O documento destaca a importância de um processo participativo e baseado no conhecimento dos procedimentos, a finalidade e nas possibilidades de supervisão desse processo. Finalmente, no quadro europeu, está a Carta de Direitos Humanos e Princípios para a Internet (CDHPI), uma iniciativa da Coalizão "Dinâmica para Direitos e Princípios da Internet[7] (IRPC), baseada no Fórum de Governação da Internet das Nações Unidas. Tal como a designação refere, o instrumento dedica especial enfoque na transformação de políticas de governação da internet numa forte perspectiva dos Direitos Humanos.

No contexto da SADC[8], a Lei-Modelo sobre a Proteção de Dados e Cibersegurança constitui o instrumento de referência mais próximo à realidade dos países membro, inspirado nas convenções internacionais. A Lei estabelece uma série de infrações nos casos de acesso ilegal à computadores, de interseção das comunicações, de violação de dados, de produção e reprodução da pornografia infantil. No capítulo dos conteúdos, o documento sanciona crimes a xenofobia, racismo, homofobia, o assédio online, entre outros. A aplicabilidade das disposições legais parecem bem pormenorizadas, ao levar igualmente em conta a necessidade de autorização judiaria para a intercepção e recolha de dados pessoais.

Das possibilidades de um quadro legal de cibersegurança e proteção de dados em Moçambique

Embora Moçambique tenha as suas especificidades, os processos de produção legislativa de questões complexas como a temática da cibersegurança e protecção de dados, parecem de certa forma encaminhados. A existência de instrumentos internacionais, maior parte dos quais já ratificados e de literatura aparentemente abundante sobre esta matéria, permitem que o país adopte uma via não muito distante das abordagens internacionais e regionais. Confere algum conforto ao país, também, o facto de já dispor de uma considerável legislação avulsa e de políticas que, não sendo explicitamente dedicada a regulação da cibersegurança e protecção de dados, permitem responder, com algum mérito, os desafios associados ao cibercrime.

O já referido conforto resultante dos instrumentos internacionais, que podem inspirar a produção interna de uma legislação específica em cibersegurança, releva-se, ainda, inconclusivo, dado que o país regista um assinalável atraso na ratificação da Convenção de Budapest. Este atraso concorre para possíveis limitações na adaptação da legislação à evolução das tecnologias e da geopolítica global (Cepik e Marcelino, 2021).

A adopção deste instrumento transmitiria um compromisso "político' de legislar para a protecção de direitos e liberdades fundamentais, tendo em conta também que, no ordenamento jurídico moçambicano, as normas do direito internacional possuem o mesmo valor das normas infraconstitucionais, emana-

5 https://stripe.com/pt-br-de/guides/general-data-protection-regulation

6 Na altura da submissão dos dados, esta finalidade tem de ser bem explícita, tal como o tempo durante o qual estes serão mantidos.

7 https://itsrio.org/wp-content/uploads/2017/01/IRPC_booklet_brazilian-portuguese_final_v2.pdf

8 Comunidade para o Desenvolvimento da África Austral.

das da Assembleia da Republica e do Governo (Art. 18 da CRM).

Duas principais notas se podem extrair da Convenção de Budapest e de Malabo: A primeira convecção destaca, não apenas a dimensão dos Direitos Humanos no ecossistema digital, mas também institui a cultura de responsabilização das partes faltosas, especialmente as instituições e os respectivos servidores ou colaboradores. A segunda convenção, de Malabo, resolve o problema do cepticismo quanto a transparência da gestão da informação dos sujeitos, ao propor a criação de uma autoridade independente de proteção de dados para fornecer supervisão e controlo. Os princípios desta convenção parecem convergir com o Regulamento Geral (europeu) de Proteção de Dados (RGPD). Não vinculando os países africanos, da SADC em particular, o documento pode constituir uma fonte de aprendizagem no exercício legislativo nacional. A combinação dos instrumentos em referência com a lei-modelo da Região Austral, considerada progressista, constitui uma das vias para o processo legislativo em cibersegurança e Direitos Digitais em Moçambique.

Desafios e recomendações

- À luz do direito comparado, o Estado deve assumir a ratificação das convenções e protocolos internacionais como prioridade, sem prejuízo da necessária adaptabilidade dessas normas às especificidades do país e das mutações permanentes do ecossistema digital.
- Em todos os actos legislativos sobre cibersegurança e direitos digitais, a Assembleia da República deve agir com base no princípio de ampliação do acesso aos serviços de telecomunicações, o respeito pelas liberdades fundamentais, incluindo o direito à privacidade dos sujeitos e a salvaguarda do interesse público e nacional.
- No quadro das suas intervenções para a protecção do ecossistema digital em Moçambique, o Governo, a Assembleia da República e as Organizações da Sociedade Civil devem primar pelos princípios da transparência, da participação e da responsabilização, por formas a eliminar potenciais arbitrariedades e ampliar os direitos e liberdades já adquiridos.
- Para uma melhor articulação entre a futura Lei de cibersegurança e protecção de dados e os instrumentos internacionais sobre esta matéria, o Governo e a Assembleia da República deverão garantir que, no processo legislativo, garanta-se a a extracção daquele conteúdo, nessas normas, que melhor respondem às necessidades de protecção da vida privada e de outros direitos dos cidadãos.

Parceiros:

USAID FROM THE AMERICAN PEOPLE

ADVANCING RIGHTS IN SOUTHERN AFRICA ARISA