Policy Brief - 3

Práticas e Experiências Internacionais de Legislação sobre Cibersegurança e dos Direitos Digitais

- **Ao poder Executivo, recomenda-se o desencadeamento, com todas as partes interessadas, a abertura do debate público para o aprimoramento do quadro legal e a criação de leis julgadas pertinentes, por formas a instituir uma cultura cibernética baseada em direitos fundamentais;**
- **Ao poder legislativo, que promova reflecções, por iniciativa parlamentar, para a revisão do quadro legal em vigor, aprimorando-o e conformando-o com as boas práticas universais sobre cibersegurança e protecção de dados;**
- **Ao poder judicial, que, mais do que entidade implementadora, defina-se como uma instância de consulta que aclare a viabilidade dos instrumentos legais propostos pelo Executivo, com a participação de Organizações da Sociedade Civil e Empresas das Tecnologias de Informação e Comunicação;**
- **Ao poder Executivo, que promova a protecção uma melhor protecção, no âmbito dessas normas, os interesses da criança, das pessoas portadoras de deficiência, da mulher e outras pessoas em vulnerabilidade (os espaços cibernéticos podem ser usados de forma ofensiva contra os direitos fundamentais destas pessoas).**

Breve contextualização

O debate em torno da cibersegurança no mundo gira em torno de três principais eixos. O primeiro refere-se à dimensão económica; o segundo aponta para a capacidade das infraestruturas e, finalmente, a questão do quadro legal. No caso moçambicano e, não descurando da relevância das duas primeiras dimensões, o quadro legal é apontado como aquele que maior atenção deve merecer neste debate (CEPIK e MARCELINO, 2021). Isto não significa o desmerecimento dos esforços do Estado para a criação de leis e instrumentos favoráveis à repressão de incidentes de cibersegurança e protecção de dados. Significa, sim, o convite `permanente reflexão para que estes instrumentos respondam às demandas decorrentes das dinâmicas actuais do ecossistema digital moçambicano.

Em Moçambique, as questões de cibersegurança e protecção de dados encontram são tratadas na Lei das Transações Comerciais (**Lei** nº 3/2017 de 9 de Janeiro) e outra legislação avulsa. Decorre, daqui o entendimento dos intervenientes do ecossistema digital moçambicano da pertinência de um quadro legal específico que verse exclusivamente esta temática.

A necessidade do tratamento legal específico e a respectiva regulamentação é justificada, fundamentalmente, pela protecção dos direitos fundamentais dos indivíduos. Esta necessidade insere-se no mandato do Governo moçambicano que, através do Instituto Nacional das Tecnologias de Informação e Comunicação, arroga-se a responsabilidade de propor políticas, padrões e regulamentos de cibersegurança (artigo 6 do Decreto nº 60/2017 de 6 de Novembro). Isto inclui, fundamentalmente, a produção de propostas de lei de proteção de dados pessoais e de combate a crimes cibernéticos. O debate nesse sentido iniciou em 2020, numa parceria entre o Governo e as Organizações, através do Ministério da Ciência, Tecnologia e Ensino Superior e a Sociedade Civil. Todavia, prevalece o desafio de transformação da mera vontade de criação de uma legislação específica que assegure a existência de leis no ordenamento jurídico moçambicano, que, por um lado, responda ao dever do Estado de assegurar que cada cidadão esteja seguro no ciberespaço e que, por outro lado, o direito à privacidade desses mesmos cidadãos seja respeitado.

A condução deste processo, além da indispensável consulta aos intervenientes-chave, implica a compreensão de como a legislação de outras geográficas lida com questões de cibersegurança e protecção de dados, numa perspectiva do direito comparado. É dentro desta necessidade que é produzido o presente documento, que sintetiza as principais ideias sobre os processos legislativos e o quadro legal de cibersegurança, tendo como base as experiências internacionais, na sequência do debate virtual realizado adia 02 de Junho de 2022, pelo MISA.

Das experiências africanas

O acesso à internet é um importante indicador em qualquer abordagem sobre direitos e liberdades no ciberespaço, dado

que do acesso deriva o exercício de direitos digitais. De acordo com a União Internacional das Telecomunicações (UIT), nos últimos dez anos, o nível de acesso à Internet na África subsariana triplicou. Do ponto de vista legislativo, nesta região, destaca-se a Lei-Modelo da SADC sobre Cibersegurança e Protecção de Dados em 2014. A este instrumento juntam-se outras duas leis-modelo (a Lei-Modelo sobre Protecção de Dados e a Lei-Modelo sobre Comércio Electrónico e Transações Electrónicas), a legislação e as políticas em matéria de Tecnologias de Informação e Comunicação (TIC Trata-se de um instrumento de referência para os processos legislativos de cada Estado-membro da SADC.

Portanto, a Lei-Modelo da SADC é um guia para os Estados membros da região sobre o significado e implicações no contexto do cibercrimeque criminaliza o acesso ilegal; a interceptação; a interferência de dados; a espionagem; a falsificação; a fraude; a pornografia; material xenófobo e a divulgação de detalhes de uma investigação de crimes cibernéticos. As questões de Direitos Humanos nesta lei, são abordadas nas dimensões do direito à liberdade de expressão, do direito à privacidade, do direito à protecção igual da lei e do direito à liberdade de reunião.

Alguns países da região já possuem legislação de cibersegurança inspirada na lei-modelo da SADC, como são os casos da Zâmbia (s*Zambia Cyber Security and Cyber Crimes Act)*; Maurícias (Lei das TIC das Maurícias),; África do Sul(Lei sobre o Cibercrime); Eswatini (Lei de Crimes Informáticos e Cibercrimes); Zimbabwe (Lei de Protecção de Dados do Zimbabwe);e Tanzânia, (Lei sobre o Cibercrime).

Zimbabwe

OZimbabwe conta com uma Lei de Protecção de Dados, inicialmente considerada Lei de Segurança Cibernética e Protecção de Dados (em 2020). Após consultas públicas, o instrumento foi aprovado, em Dezembro de 2021, com a designação de Lei de Protecção de Dados. Esta lei prevê as figuras de controladores de dados e processadores de dados. Um dos aspectos progressistas deste instrumento legal prende-se com a criação de uma entidade independente, a Autoridade Reguladora de Correios e Telecomunicações do Zimbábue (POTRAZ) como Autoridade de Proteção de Dados,[1] com poderes de execução legal necessários para garantir que os direitos dos cidadãos são respeitados na gestão de dados pessoais. Outro órgão criado por esta lei, é o Centro de Cibersegurança e Monitoramento de Intercepção de Comunicações, dotado apenas de funções de Cibersegurança[2]. A entidade está baseada na Presidência da República, o que representa um potencial foco de vigilância excessiva e/ou abusiva.[3]

Lesotho

O Lesotho Dispõe de uma lei de cibersegurança e protecção de dados, fruto de um processo de consulta pública desencadeada pelo respectivo Governo, em 2020, o projecto de lei que foi adoptado em Março de 2021. A participação de Organizações da Sociedade Civil, como o MISA Lesotho, foi determinante nesse processo legislativo.

A questão mais saliente nesta lei, é o excessivo poder de monitoramento do ciberespaço, atribuído ao Estado, uma vez que inexiste nessa norma, uma definição do que é o acesso ilegal aos dados, apesar de ser criminalizado. Na mesma senda, há também questões-chave relacionadas às sanções penais injustificadas.

Zâmbia

Em Janeiro de 2021 foi aprovada a Política Nacional de Segurança Cibernética, e , em Fevereiro do mesmo ano, elaborado um projecto de lei, sem um rigoroso processo de consultas públicas. A lei define o regulador de telecomunicações como regulador de cibersegurança que, no quadro do seu mandato, deve colaborar com os ministros responsáveis pela segurança, defesa e outros agentes relevantes. O poder excessivo atribuído aos ministros e, que podem permitir interferências do executivo no exercício das liberdades fundamentais constitui uma das principais questões deste instrumento. A clarificação dos limites na intercepção de comunicações, restrições do anonimato, limitação da Liberdade de Expressão, ambiguidades na definição do discurso de ódio[4], entre outras, são consideradas as principais zonas de penumbra da lei.

Uganda

O Uganda enfrenta uma série de problemas relacionados com os direitos digitais e a segurança cibernética[5]. Estes problemas vão desde a utilização tributada da internet - o que torna os dados muito caros; o assédio *online*; a detenção de utilizadores da internet, etc. Por outro lado, o país dispõe de uma lei contra osos cibercrimes, virada especialmente para penalizar o acesso indevido à computadores. Dispõe, igualmente, de uma outra lei sobre intercepção de comunicações, que permite aos serviços de segurança acederem a informações e dados dos cidadãos em caso de suposto perigo para a segurança nacional. Apesar de dispor de uma ampla legislação em cibersegurança e de ter ratificado a Convenção de Malabo (possui cerca de 12 leis relativas à segurança digital e cibersegurança, incluindo a Lei de Privacidade e Protecção de Dados), Uganda é exemplo concreto de que não basta haver um ambiente legal favorável. A Autoridade Nacional de Tecnologia, que é responsável pelas disposições gerais de tecnologia da informação no Uganda, gere a base de dados do Uganda, regula as normas de outras organizações e é também responsável pelo sistema de gestão da informação. Igualmente, é responsável pela elaboração de uma Lei Nacional de Dados Pessoais que parece vir a ser a lei ugandesa mais problemática, pois prevê a criação de centros de vigilância no país, onde a polícia e as forças militares poderão aceder às informações contidas nestas bases de dados, transformando-se assim em interceptores.

A Lei sobre o Cibercrime, para além de punir crimes cometidos no espço *online*, é utilizada para prender cidadãos pelo

1 https://securiti.ai/zimbabwe-new-data-protection-act/
2 https://zimbabwe.misa.org/2021/12/06/analysis-of-the-data-protection-act/
3 O mesmo órgão passou a ser responsável pela emissão de mandados de interceção de comunicações.
4 https://cipesa.org/?wpfb_dl=447
5 https://www.unwantedwitness.org/download/uploads/Report_How-Undemocratic-Practices-Sway-Digital-Rights-Enjoyment-Governance-In-Uganda.pdf

que possam publicar nesse espaço. A lei apresenta disposições ambíguas e pouco claras, sendo em muitos casos usada de forma abusiva pelo governo, como instrumento de chantagem , através do abuso do poder de vigilância. Por outro lado, está em marcha o processo de aprovação do novo sistema de identidade civil que poderá entrar em vigor em 2023. Trata-se de um instrumento que irá incorporar dados forenses de imigrantes e nacionais.

Desafios e propostas para legislação local

Entre os principais desafios do processo legislativo em matéria de cibersegurança e protecção de dados em Moçambique, destacam-se:

- Apesar do cometimento do Estado e do Governo sobre a urgência de reformas legislativas para a protecção do ecossistema digital em Moçambique, observa-se a uma aparente apatia quanto à tomada de uma posição firme que resulte em acções concretas para a criação de um quadro legal específico em cibersegurança e protecção de dados;

- A aparente inércia em ampliar o debate sobre a segurança cibernética e a proteção de dados no cotexto dos direitos fundamentais, perpetua as incertezas quanto ao futuro do espaço cívico nacional através do ciberespaço;

- Persistem deficiências na percepção dos direitos digitais como direitos fundamentais e essenciais para a realização da dignidade da pessoa humana.

Recomendações

- Ao poder executivo, recomenda-se o desencadeamento, com todas as partes interessadas, a abertura do debate público para o aprimoramento do quadro legal e a criação de leis julgadas pertinentes, por formas a instituir uma cultura cibernética baseada em direitos fundamentais;

- Ao poder legislativo, que promova reflecções, por iniciativa parlamentar, para a revisão do quadro legal em vigor, aprimorando-o e conformando-o com as boas práticas universais sobre cibersegurança e protecção de dados;

- Ao poder judicial, que, mais do que entidade implementadora, defina-se como uma instância de consulta que aclare a viabilidade dos instrumentos legais propostos pelo Executivo, com a participação de Organizações da Sociedade Civil e Empresas das Tecnologias de Informação e Comunicação;

- Reforçar a capacidade de comunicar os direitos digitais à sociedade, esclarecendo por que razão devem estes direitos digitais ser respeitados, promovidos ou protegidos, e como estes direitos digitais podem ser contidos;

- A sociedade civil precisa ampliar as suas Acções de educação cívica sobre o conceito e a importância da internet;

- Ao poder Executivo, que promova a protecção uma melhor protecção, no âmbito dessas normas, os interesses da criança, das pessoas portadoras de deficiência, da mulher e outras pessoas em vulnerabilidade (os espaços cibernéticos podem ser usados de forma ofensiva contra os direitos fundamentais destas pessoas).

Parceiros:

USAID FROM THE AMERICAN PEOPLE

ADVANCING RIGHTS IN SOUTHERN AFRICA ARISA