CiberCidadãos
Acção Colectiva para a
Cidadania Digital

`A: SUA EXCELÊNCIA MARGARIDA TALAPA, PRESIDENTE DA ASSEMBLEIA DA REPÚBLICA

Assunto: *Posicionamento sobre as Propostas de Leis da Segurança Cibernética e Crimes Cibernéticos*

EXCELÊNCIA,

Permita-nos, respeitosamente, apresentar as nossas cordiais saudações. A sociedade civil acompanha com atenção o processo de apreciação parlamentar das propostas de lei de segurança cibernética e de combate aos crimes cibernéticos, entendendo tratar-se de instrumentos determinantes para a governação do espaço digital em Moçambique. Como em qualquer propocesso desta natureza, e sendo tradição da Assembleia da República, V.Excia não descarta, a inclusão de contributos de todos os interessados nos processos legislativos nacionais. Neste contexto, a CIBERCIDADÃOS - Accção Colectiva para a Cidadania Digital, em parceria com o MISA Moçambique e a Associação Moçambicana de Jovens pela a Igualdade de Gênero e Educação, vem mui respeitosamente apresentar a sua posição como uma contribuição construtiva ao debate parlamentar, visando reforçar a qualidade, a clareza e o equilíbrio das disposições legais, de modo a assegurar a eficácia no combate às ameaças cibernéticas sem comprometer direitos, liberdades e garantias fundamentais dos cidadãos no ambiente digital.

1. **Proposta de Lei de Segurança Cibernética**

A presente proposta de Lei de Segurança Cibernética funda-se em cada vez mais crescente evolução e utilização das Tecnologias de Informação e Comunicação (TIC), que embora represente benefícios, contribui para o aumento de desafios de incidentes e ataques cibernéticos que se sofisticam a cada dia, possibilitando

Cidade de Maputo, Rua Bento Mukhesswane, Nr 98 R/C, Malhangalene B. Email: cibercidadãos@gmail.com

ocorrência de prejuízos incomensuráveis para a economia, a sociedade e a soberania estatal.

A proposta visa prevenir e sancionar a prática de cibercrimes, tal como o Governo alega "diariamente, milhões de ataques são efectuados ao cidadão, às infra-estruturas críticas e às redes a nível global através da Internet, comprometendo os sectores público e privado, academia e a sociedade civil, expondo igualmente informações, dados sensíveis de pessoas e do Estado".

Essencialmente a Proposta de Lei tem em vista a consagração do Conselho Nacional de Segurança Cibernética, da Autoridade Nacional de Segurança Cibernética, da Equipa Nacional de Resposta a Incidentes de Segurança Cibernética, Segurança das Redes e dos Sistemas de Informação, a definição de requisitos de segurança e notificação de incidentes, respostas à ameaças e incidentes de Segurança Cibernética, fiscalização, previsão e estatuição de infracções, bem como a criação de um fundo de Segurança Cibernética com o objectivo de fornecer recursos financeiros para a promoção da segurança Cibernética com vista a garantir um espaço cibernético seguro, resiliente e inclusivo.

2. Proposta de Lei de Crimes Cibernéticos

Relativamente à Proposta de Lei de Crimes Cibernéticos tem por objectivo estabelecer o regime jurídico aplicável aos crimes cibernéticos e neste quadro debruça-se sobre matéria de penal, processual e de cooperação internacional.

O instrumento legal em prelo tem sua génese na crescente utilização das tecnologias de informação e comunicação, bem como do aumento da criminalidade associada ao uso de sistemas informáticos, impondo a necessidade de dotar o ordenamento jurídico nacional de instrumentos adequados à prevenção, investigação e repressão destes fenómenos.

A presente Proposta de Lei procede:

RECEPÇÃO DA AR
AS 15 HORAS 23
DATA 23/04/2026
ASS:

- A colmatação de lacunas relativas à prevenção e combate aos crimes cibernéticos no Código Penal e reforço de mecanismos procedimentais - Código de Processo Penal e na Lei da Cooperação Jurídica e Judiciária em Matéria Penal - Lei b.°21/2019, de 11 de Novembro.
- Condensar todas as normas respeitantes aos crimes cibernéticos num único diploma legal, o que permitirá unificação e melhor utilização pelos aplicadores do Direito desta matéria.

3. **Direito Internacional**

No âmbito do Direito Internacional destacam-se os seguintes instrumentos:

3.1 **A Convenção da União Africana sobre Cibersegurança e Protecção de dados pessoais (CUACPDP)** - que encoraja os estados partes a adoptar medidas legislativas e/ou regulamentares que julgar adequadas e eficazes, tipificando como infracções criminais os actos que afectem a confidencialidade, a integridade, disponibilidade e a sobrevivência dos sistemas TIC's.

3.2 **Convenção das Nações Unidas contra a Ciber-criminalidade -** defende que o uso dos sistemas tecnológicos de informação e comunicação pode ter impacto considerável em termos de magnitude e formato de actividades criminais, incluindo crimes transnacionais, como é caso do terrorismo violento, tráfico de pessoas, tráfico de órgãos humanos, contrabando, tráfico de drogas, entre outros (Resolução n.° 79/243 de 2024.

3.3 **Convenção sobre o Crime Cibernético do Conselho da Europa (Convenção de Budapeste)** - em matéria de crime cibernético permite obtenção da prova digital e de cooperação internacional e também modelo de estrutura normativa interna que cada Estado deve adoptar -

para poder eficazmente combater este tipo de fenómeno criminal. Esta convenção estabelece mecanismos e ferramentais processuais para investigar estes crimes e proteger evidências ou prova electrónicas relacionadas com os crimes cometidos eletronicamente.

O Procurador Geral da República na sua Informação Anual à Assembleia da República destacou que devido a natureza transnacional da cibercriminalidade que frequentemente impõe a necessidade de obtenção de prova alojada fora do território nacional, o que só é possível com a cooperação internacional.

4. Fragilidades

4.1 Moçambique ainda não ratificou a Convenção de Budapeste.

4.2 As Propostas de Lei não preveem fraudes digitais, ataques à integridade de sistemas associados à Inteligência Artificial e outros crimes praticados com base na Inteligência Artificial e tecnologias Emergentes como *deepfakes (alteração de fotos e vídeos) e ciberterrorismo.*

4.3 A IA está inserida no âmbito da transformação digital utilizada por redes criminosas para sofisticar fraudes, tornar anónimas as transmissões, manipular dados, ludibriar sistemas de vigilância e corromper cadeias de informação dai mostrar-se premente a sua regulamentação - a informação do PGR vai no mesmo sentido.

4.4 Não tipificação das diversas modalidades dos chamados crimes de *phising* e *ciberbullying* - na medida em que estes crimes apresentam técnicas que dificultam a prevenção e investigação.

4.5 A proposta de Lei de crimes cibernéticos não se debruça de forma específica da punição agravada de ataques à infraestruturas críticas como telecomunicações, electricidade, abastecimento de água e outros infraestruturas vulneráveis.

5. Riscos associados

5.1 **Controle das Comunicações e Bloqueios**: Existe o receio de que a nova legislação facilite o controle estatal sobre o espaço digital. Críticos apontam que a lei surge sob o espectro de decretos recentes, como o Decreto n.º 48/2025, que permite ao Governo bloquear redes de telecomunicações em situações de risco iminente para a segurança pública.

5.2 **Vigilância e Privacidade**: Organizações como a Cibercidadãos e o MISA Moçambique destacam a necessidade de a lei clarificar a "fronteira" entre a segurança do Estado e os Direitos individuais, como a privacidade e a liberdade de expressão.

5.3 **Ambiguidade Jurídica**: Especialistas e a sociedade civil alertaram para a importância de alinhar o novo quadro legal a convenções internacionais (como a de Budapeste e a de Malabo), para evitar que termos vagos na lei moçambicana sejam usados para restringir liberdades já garantidas, como a Lei do Direito à Informação.

5.4 **Militarização da Cibersegurança**: Uma das preocupações mencionadas é que, embora o INTIC (Instituto Nacional de Tecnologias de Informação e Comunicação) seja o coordenador técnico, em determinados contextos as competências podem ser assumidas por autoridades paramilitares.

5.5 **Capacidade de Implementação**: Críticos questionam a eficácia da lei devido à falta de meios humanos especializados e infraestruturas tecnológicas no país para identificar e responsabilizar autores de crimes, o que poderia tornar a lei um instrumento mais focado em punir utilizadores locais do que em travar ameaças globais.

6. Recomendações

6.1 ***Moçambique deve ratificar a Convenção de Budapeste*** *por configurar* um instrumento útil e eficiente na formação do corpo de delito de crimes

cibernéticos transnacionais. - O PGR também foi no mesmo sentido na sua informação prestada no dia 22 de Abril de 2026.

6.2 **Punição da tentativa**: o crime pode não se consumar pela desistência do agente ou frustrar-se pela destreza da vítima ou outros factores a desfavor a consumação do crime. É por estas razões que o legislador deveria ponderar a punição da tentativa e não unicamente remeter ao regime geral previsto artigo 18 do CP. Segundo este artigo a tentativa será punida se ao crime consumado corresponder a pena de 2 anos. Assim, seria consentâneo que nos casos de desistência do agente do crime, a tentativa fosse irrelevante ao critério da moldura penal aplicável ao crime consumado.

6.3 Revisão do n.° 2 do artigo 18 da Lei de Crimes Cibernéticos, que permite que a polícia criminal (SERNIC) efecute apreensões sem que haja mandato de busca e apreensão, salvo em situações excepcionais claramente definidas na lei. Adicionalmente, devem ser estabelecidos critérios rigorosos de necessidade e proporcionalidade, mecanismos de controlo e responsabilização, bem como salvaguardas específicas para a protecção da privacidade, dos dados pessoais e do sigilo profissional, de modo a equilibrar eficazmente a investigação criminal com a garantia dos direitos fundamentais.

6.4 Como se isso não bastasse, a polícia criminal tem 72 horas para requerer a validação dessa apreensão pelo juiz de instrução criminal.

6.5 O mais grave de tudo é que a apreensão de dados informativos pode revestir "eliminação não reversível ou bloqueio do acesso aos dados" - o processo crime comporta a fase de audiência preliminar em o arguido constituído pode requerer diligências de provas. Tendo sido eliminados os dados como será possível reproduzir esta prova?. Razão por que se propõe eliminação da alínea d) do n.°5 do artigo 18.

6.6 A intercepção de comunicações prevista no artigo 19 deve ser precedida de autorização judicial sobre pena de aceder-se informações de índole pessoal, o que pode resvalar na violação dos direitos de personalidade.

pessoal, o que pode resvalar na violação dos direitos de personalidade.

Cidade de Maputo, Rua Bento Mukhesswane, Nr 98 R/C, Malhangalene B. Email: cibercidadãos@gmail.com
Cidade de Maputo, Rua Bento Mukhesswane, Nr 98 R/C, Malhangalene B. Email: cibercidadãos@gmail.com

6.7 Em relação ao artigo 22 atinente à informação espontânea há que se garantir o direito constitucional de plena defesa, isto é, que essa informação seja facultada ao arguido e seus mandatários para exercer o direito do contraditório. Também, há que se assegurar que o arguido não será julgado duas vezes sobre os mesmos factos em homenagem ao "*principio ne bis in idem*".

Maputo, 23 de Abril de 2026.

Ernesto Saúl

CiberCidadãos
Acção Colectiva para a
Cidadania Digital

(Director Executivo da Cibercidadãos)

Organizações subscritoras

MISA MOÇAMBIQUE

AMJUGE
ASSOCIAÇÃO MOÇABICANA DE JOVENS PELA IGUALDADE DE GÉNERO E EDUCAÇÃO