



A Tipificação Penal dos Cibercrimes Praticados com Recurso à Inteligência Artificial em Moçambique: Uma Hermenêutica do Vazio Normativo e a Urgência Legislativa

Bitone Viage¹

RESUMO

A crescente instrumentalização da inteligência artificial (IA) na prática de crimes cibernéticos tem desafiado os marcos legais tradicionais, exigindo dos ordenamentos jurídicos respostas normativas mais técnicas e atualizadas. Em Moçambique, embora haja dispositivos legais relevantes como a Lei das Telecomunicações, a Lei das Transações Eletrónicas e o Código Penal, bem como propostas legislativas em curso, verifica-se a ausência de previsões específicas voltadas à criminalidade digital potenciadas por IA. O presente artigo tem como objetivo analisar criticamente o quadro normativo vigente e as propostas de lei atualmente em debate, avaliando sua capacidade de resposta aos novos riscos associados à utilização maliciosa da IA. A pesquisa adota uma abordagem qualitativa, de natureza exploratória e descritiva, com base em análise documental, hermenêutica jurídico-sistemática e comparada. Os resultados demonstram que persiste um vazio normativo significativo quanto à tipificação de condutas como *deepfakes*, manipulação algorítmica de dados e ataques automatizados, o que compromete a eficácia do combate à criminalidade digital contemporânea. Conclui-se pela necessidade de uma reforma legal urgente e

¹ Licenciando em Direito pela Universidade Eduardo Mondlane. Mestre em Ciência Política, com especialização em Políticas Públicas e Instituições Públicas, pela Universidade Federal do Pará (UFPA – 2018). Licenciado em Relações Internacionais e Diplomacia pelo Instituto Superior de Relações Internacionais – Moçambique (ISRI – 2016). Licenciado em Ensino de Filosofia, com habilitações em História, pela Universidade Pedagógica – Moçambique (UP – 2016).

Viage, B.; A Tipificação Penal dos Cibercrimes Praticados com Recurso à Inteligência Artificial em Moçambique: Uma Hermenêutica do Vazio Normativo e a Urgência Legislativa. Revista Portuguesa de Ciências Jurídicas V.6, Nº1, p.14-34, Jan./Jul. 2025. Artigo recebido em 05/06/2025. Aprovado em 27/06/2025

estruturada, que contemple tipos penais específicos, mecanismos de supervisão algorítmica, cooperação internacional e proteção reforçada dos direitos fundamentais no ambiente digital.

Palavras-chave: Cibercriminalidade; Inteligência Artificial; Reforma Legislativa; Moçambique; Regulação Algorítmica.

1. Introdução

Nas últimas décadas, a digitalização das estruturas sociais, políticas e económicas alterou profundamente o modo como os Estados concebem, regulam e protegem o espaço jurídico. No centro dessa transformação encontra-se a IA, uma tecnologia disruptiva que, embora prometa eficiência, inovação e modernização, tem sido também instrumentalizada para fins ilícitos.

A cibercriminalidade com recurso à IA representa hoje uma das ameaças mais sofisticadas e assimétricas à soberania digital, à segurança jurídica e à estabilidade institucional dos Estados modernos.

Em Moçambique, o crescimento do uso de Tecnologias de Informação e Comunicação (TIC), aliado à ainda incipiente arquitetura legal, tornou-se um terreno fértil para a emergência de novos riscos. A ausência de um marco jurídico específico sobre a criminalidade digital mediada por sistemas inteligentes expõe lacunas significativas no ordenamento jurídico nacional, tanto no plano penal como institucional.

Esta realidade agrava-se diante da constatação de que, mesmo as propostas legislativas atualmente em discussão, como (i) a Proposta de Lei de Segurança Cibernética e (ii) a Proposta de Lei de Prevenção e Repressão dos Crimes Cibernéticos, ambas submetidas pelo Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC) não contemplam de forma clara, sistemática e técnica os desafios emergentes associados à utilização da IA em contextos criminosos.

Neste contexto, emerge a presente investigação, orientada pela seguinte pergunta-problema: *qual deve ser a resposta legislativa adequada do Estado moçambicano face ao recrudescimento da cibercriminalidade com recurso à inteligência artificial, à luz da realidade normativa vigente e das propostas em curso?*

O objetivo geral deste estudo é analisar criticamente o quadro normativo atual em Moçambique no que respeita à criminalidade cibernética com suporte em IA, com vista à identificação das suas limitações e à formulação de “propostas legislativas” adequadas ao contexto tecnológico contemporâneo. Como objetivos específicos, pretende-se: (i) relacionar e interpretar as principais normas em vigor que tangenciam a cibercriminalidade; (ii) avaliar o conteúdo e alcance das propostas de lei em tramitação; (iii) compreender os riscos concretos da IA enquanto vetor criminógeno; e (iv) sugerir diretrizes jurídicas e institucionais para uma reforma penal orientada à realidade algorítmica.

Quanto a justificativa, este estudo reside na urgência de construir uma resposta jurídica nacional tecnicamente robusta e politicamente consciente, capaz de enfrentar as novas morfologias do crime digital, sobretudo num país que se encontra em transição digital, com um ecossistema jurídico-institucional ainda vulnerável e suscetível a disrupções tecnológicas. Como defendem Floridi & Cowls (2020)², não se trata apenas de regular a tecnologia, mas de proteger os fundamentos do Estado de Direito na era algorítmica.

No que concerne à metodologia, a investigação adota uma abordagem qualitativa e exploratória, com base na análise documental de diplomas legais nacionais (vigentes e propostos), tratados internacionais ratificados ou em fase de adesão (como a Convenção de Malabo e a Convenção de Budapeste), e literatura doutrinária especializada sobre cibercrime, inteligência artificial e Direito Penal. O estudo ancora-se ainda em pressupostos da hermenêutica jurídico-sistemática, permitindo interpretar o “*silêncio normativo*” à luz das exigências contemporâneas de atualização legislativa.

² Floridi, L., & Cowls, J. (2020). *A Unified Framework of Five Principles for AI in Society*. Harvard Data Science Review, 2.

2. Considerações Iniciais

A reflexão que sustenta este estudo tem origem em experiências institucionais e académicas vividas pelo autor em dois espaços distintos, mas profundamente complementares, a primeira decorreu no âmbito do I Seminário sobre Direito e Inteligência Artificial, realizado no segundo semestre de 2024 pela Faculdade de Direito da Universidade Eduardo Mondlane, ocasião em que o autor apresentou a comunicação intitulada *“Desafogando o Poder Judicial por Meio da Inteligência Artificial”*. A participação neste evento despertou, de forma mais aprofundada, a necessidade de compreender não apenas os benefícios da IA para o sistema de justiça, mas também os seus riscos jurídicos, éticos e penais, especialmente quando utilizada como instrumento de criminalidade cibernética sofisticada e difícil de rastrear.

A segunda experiência relevante ocorreu no âmbito do III Seminário sobre Cibercriminalidade, realizado nos dias 4 e 5 de junho de 2025, organizado pelo Ministério Público de Moçambique em parceria com o Escritório das Nações Unidas sobre Drogas e Crime (UNODC), sob o lema *“Combater o Crime Organizado na Era da Inteligência Artificial”*. O evento constituiu uma plataforma interinstitucional para a análise dos desafios impostos pela criminalidade digital com suporte em tecnologias emergentes, com destaque para o uso malicioso da IA em práticas ilícitas transnacionais.

Foi a partir desse duplo contexto que emergiu a inquietação científica central que norteia esta investigação: *qual deve ser a resposta legislativa adequada do Estado moçambicano face ao recrudescimento da cibercriminalidade com recurso à inteligência artificial, à luz da realidade normativa vigente e das propostas em curso?*

A presente pesquisa, portanto, não nasce apenas de uma inquietação teórica, mas também da vivência prática e institucional, num ambiente em que o legislador, o operador judiciário e o académico se confrontam com um novo tipo de ameaça discreta, automatizada, massiva e potencialmente desestabilizadora.

A partir desta interrogação fundacional, construiu-se uma análise crítica do ordenamento jurídico nacional e das propostas legislativas em curso, com o objetivo de identificar as lacunas normativas existentes e propor mecanismos jurídicos eficazes e tecnicamente informados para a prevenção, repressão e responsabilização dos crimes cibernéticos com recurso à IA.

A doutrina tem-se debruçado exaustivamente sobre as intersecções entre cibercriminalidade e inteligência artificial, oferecendo valiosos contributos teóricos e analíticos. Todavia, o foco deste estudo recairá, especificamente, sobre a arquitetura legal vigente em Moçambique no que respeita ao combate ao cibercrime praticado com recurso a tecnologias baseadas em IA, procurando identificar as lacunas normativas, os desafios operacionais e as possíveis vias de reforma legislativa.

Para um melhor enquadramento do problema, impõe-se, antes de mais, identificar o quadro normativo atualmente existente em Moçambique e, subsequentemente, delinear as expectativas normativas no que tange à regulamentação eficaz dos desafios jurídicos suscitados pela cibercriminalidade praticada com recurso à inteligência artificial.

3. Códigos Antigos e Crimes Novos: A (In)capacidade Jurídica de Reagir à IA no Direito Penal Moçambicano

A resposta legislativa em Moçambique aos desafios colocados pela cibercriminalidade, especialmente quando associada ao uso de tecnologias emergentes como a IA, ainda se encontra em fase incipiente.

O ordenamento jurídico nacional dispõe de alguns instrumentos normativos que tangenciam a matéria, mas carece de uma abordagem integrada, específica e sistemática voltada à prevenção, repressão e responsabilização de atos ilícitos praticados em ambiente digital com recurso à IA. Destacam-se, entre os diplomas atualmente em vigor:

- **A Lei n.º 4/2016, de 6 de junho**, que altera a **Lei das Telecomunicações (Lei n.º 8/2004)**, introduzindo algumas disposições relacionadas à infraestrutura e segurança das redes, com implicações indiretas na cibersegurança;
- **A Lei n.º 3/2017, de 9 de janeiro**, sobre transações eletrónicas, que regula, entre outros aspetos, a proteção de dados pessoais e a segurança da informação, embora sem fazer menção expressa à inteligência artificial; e
- **A Resolução n.º 5/2019**, que aprova a adesão de Moçambique à **Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais** (Convenção de Malabo), cujo potencial normativo ainda carece de internalização plena no plano legislativo nacional.

Ora vejamos, os diplomas legislativos supracitados constituem, sem margem para dúvidas, um esboço jurídico preliminar para a regulação da era digital em Moçambique, no entanto, sob uma análise técnico-jurídica mais apurada, verifica-se que tais instrumentos carecem de disposições específicas que incidam sobre os riscos emergentes decorrentes da utilização da IA na prática de crimes cibernéticos.

Tendo em vista o objetivo central deste estudo, passa-se, de seguida, à análise das principais disposições legais supra e atualmente em vigor no ordenamento jurídico moçambicano que incidem sobre a criminalidade cibernética.

Esta incursão normativa procurará identificar os limites substantivos e processuais das leis existentes, destacando os seus méritos, mas sobretudo as suas insuficiências no tratamento das condutas ilícitas potenciadas por sistemas de inteligência artificial.

3.1. Limites e Potencialidades da Lei das Telecomunicações no Combate à Cibercriminalidade³

³ Assembleia da República de Moçambique. (2016). Lei n.º 4/2016, de 3 de junho, que altera a Lei n.º 8/2004, de 21 de junho, Lei das Telecomunicações. Boletim da República, I série, n.º 66, 3 de junho de 2016.

Se atentarmos para a Lei n.º 4/2016, de 6 de junho, que altera a Lei n.º 8/2004, de 21 de junho, atinente ao regime jurídico das telecomunicações, verifica-se tratar-se de um diploma com escopo predominantemente regulatório, circunscrito à organização, funcionamento e supervisão do setor das telecomunicações.

A sua incidência normativa concentra-se, essencialmente, nos seguintes eixos: (i) a prestação e qualidade dos serviços de telecomunicações; (ii) os mecanismos de fiscalização e regulação técnica do setor; e (iii) a definição dos direitos e deveres dos operadores.

Não obstante a sua relevância para o fortalecimento da infraestrutura digital nacional, esta norma apresenta um alcance claramente limitado no que respeita à prevenção, deteção e responsabilização de condutas criminosas mediadas por tecnologias como a AI, não prevendo dispositivos específicos voltados à cibersegurança ou à criminalidade digital.

Ainda que se admita a possibilidade de uma interpretação extensiva das suas disposições, a Lei n.º 4/2016 não contempla mecanismos jurídicos específicos de combate, prevenção ou investigação de crimes digitais. Do mesmo modo, não estabelece qualquer regime jurídico aplicável à utilização de algoritmos inteligentes, como *deepfakes*, *bots* automatizados ou sistemas de tomada de decisão baseados em IA.

Tal omissão normativa evidencia a insuficiência da legislação vigente para responder, de forma eficaz, aos desafios complexos colocados pela emergência da criminalidade cibernética com suporte em tecnologias disruptivas.

3.2. A Lei das Transações Eletrónicas no Combate à Criminalidade Digital Automatizada⁴

No que respeita à Lei n.º 3/2017, atinente às transações eletrónicas e à proteção de dados pessoais, cumpre reconhecer que, à data da sua aprovação, foi considerada uma norma inovadora

⁴ Assembleia da República de Moçambique. (2017). *Lei n.º 3/2017 de 9 de janeiro: Lei de Transações Eletrónicas*. Moçambique.

no ordenamento jurídico moçambicano, sobretudo por inaugurar um quadro legal aplicável à economia digital emergente.

Contudo, a sua incidência normativa revela-se bastante circunscrita, centrando-se: (i) no reconhecimento da validade jurídica de documentos e assinaturas eletrónicas; (ii) na consagração de princípios orientadores para a proteção de dados pessoais; e (iii) na imposição de deveres específicos aos controladores e operadores de dados.

Apesar da sua importância estruturante, a referida lei não contempla dispositivos específicos voltados à criminalidade cibernética emergente com suporte em tecnologias de IA, não se verifica, por exemplo, qualquer regulamentação ou previsão sancionatória relativamente a ciberameaças como ataques de *phishing* potenciados por IA generativa, manipulação automatizada de perfis digitais ou fraudes eletrónicas cometidas por meio de *bots* inteligentes.

3.3.A Convenção de Malabo e o Vácuo Normativo sobre Crimes com Inteligência Artificial⁵

Por fim, importa referir a Resolução n.º 5/2019, que aprovou a ratificação, por parte do Estado moçambicano, da Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais, instrumento regional fundamental para o reforço do quadro normativo sobre o ciberespaço em África.

Ao ser cossignatário e, subsequentemente, proceder à sua ratificação, Moçambique vinculou-se juridicamente às obrigações decorrentes da Convenção, passando a integrar o conjunto de Estados que podem invocar e aplicar os seus preceitos na regulação interna e na resolução de litígios transnacionais relacionados com infrações cibernéticas e violações de dados pessoais.

Todavia, cumpre assinalar que, não obstante o valor normativo internacional do referido instrumento, a sua implementação prática em Moçambique depende da adoção de legislação interna de adequação e regulamentação, neste sentido, a simples ratificação, embora politicamente

⁵ União Africana. (2014). *Convenção da União Africana sobre a Cibersegurança e a Proteção de Dados Pessoais* [Convenção de Malabo]. Malabo, Guiné Equatorial.
RPCJ, Portugal-PT, V.6, N.º1, p. 14-34, Jan./Jul. 2025 www.revistas.editoraenterprising.net

relevante, não garante *per se* uma resposta normativa eficaz aos desafios emergentes da cibercriminalidade baseada em IA, nomeadamente os crimes transfronteiriços com uso de *malware*, *ransomware* e manipulação algorítmica de dados sensíveis.

3.4. A Arquitetura Normativa em Curso: Propostas de Lei e a Falta de Resposta aos Crimes Digitais com IA

A crescente sofisticação da criminalidade cibernética, especialmente quando combinada com a utilização de tecnologias de IA, exige do Estado moçambicano não apenas uma atualização normativa, mas uma verdadeira reformulação do seu paradigma legal em matéria de segurança digital. Deste modo, a resposta institucional deve evoluir para além do reconhecimento genérico do fenómeno e assumir um compromisso concreto com o desenvolvimento de um quadro legislativo robusto, coerente e tecnologicamente informado.

Presentemente, não se encontra em tramitação pública na Assembleia da Republica um projeto de lei específico sobre cibercriminalidade com recurso à IA.

Todavia, em 2021, o Conselho de Ministros, no uso das competências que lhe são conferidas pela Constituição da Republica, aprovou a Resolução n.º 69/2021, que adota a Política de Segurança Cibernética e a respetiva Estratégia de Implementação. Este instrumento normativo surge como resposta institucional aos desafios impostos pelo acelerado progresso das TIC, assumindo-se como um marco orientador da ação do Estado moçambicano no domínio da cibersegurança.

Entre os seis (6) pilares estratégicos definidos para a operacionalização da Política de Segurança Cibernética, destaca-se nessa análise, aquele que prevê a criação de um quadro legal específico para a segurança cibernética, o qual se revela crucial para consolidar a capacidade normativa e institucional do Estado nesta matéria. Este pilar está orientado para:

- i.* Reforçar o quadro legal nacional sobre segurança cibernética, mediante a aprovação de legislação específica que regule a prevenção, deteção, repressão e responsabilização dos crimes informáticos;

- ii.** Ratificar convenções internacionais relevantes no domínio da segurança cibernética e da cibercriminalidade, visando o alinhamento com os instrumentos jurídicos multilaterais e o reforço da cooperação internacional;
- iii.** Celebrar acordos de cooperação judiciária internacional em matéria de cibercriminalidade, de modo a permitir a assistência mútua eficaz na investigação e repressão de delitos transnacionais praticados no ciberespaço;
- iv.** Assinar tratados internacionais sobre segurança cibernética, com enfoque na harmonização normativa e no intercâmbio de boas práticas entre Estados; e
- v.** Promover e divulgar o quadro legal existente sobre segurança cibernética, com vista à sensibilização dos diversos atores públicos, privados e cidadãos quanto aos seus direitos, deveres e responsabilidades no uso do ciberespaço.

No âmbito deste pilar, importa destacar, de forma analítica, dois subdomínios estratégicos: em primeiro lugar, a necessidade de reforçar o quadro legal sobre a segurança cibernética e, em segundo, a imperatividade de ratificar convenções internacionais relevantes nesta matéria.

Com vista à concretização do primeiro subpilar, o reforço do quadro legal sobre a segurança cibernética, o Estado moçambicano, por intermédio do INTIC, submeteu, em 2024, à Assembleia da República, duas propostas legislativas que aguardam ainda apreciação, debate e aprovação pelo parlamento. São elas:

- A Proposta de Lei de Segurança Cibernética; e
- A Proposta de Lei de Prevenção e Repressão dos Crimes Cibernéticos.

3.4.1. Proposta de Lei de Segurança Cibernética⁶

⁶ República de Moçambique. (2024). *Proposta de Lei n.º/2023 de Segurança Cibernética* (versão 7.0, 15 de março de 2024). Assembleia da República.

A Proposta de Lei de Segurança Cibernética, disponível no portal oficial do INTIC, visa, em termos gerais, estabelecer um quadro jurídico abrangente para a segurança cibernética em Moçambique. O seu principal objetivo é assegurar a proteção dos cidadãos, das instituições públicas e privadas, do Estado e das infraestruturas críticas, no contexto do espaço digital..

A referida proposta de lei define as responsabilidades das diversas entidades públicas e privadas no domínio da segurança cibernética, regulando a implementação de medidas técnicas e organizacionais de proteção. Adicionalmente, estabelece mecanismos de coordenação interinstitucional, cooperação e resposta célere a incidentes cibernéticos, com o propósito de promover um ambiente digital mais seguro, resiliente e confiável no uso das tecnologias de informação e comunicação.

Ademais, a proposta de lei consagra disposições atinentes à gestão de riscos cibernéticos, à obrigatoriedade de notificação de incidentes de segurança, à proteção dos dados de tráfego e das bases de dados, bem como à divulgação responsável de vulnerabilidades identificadas nos sistemas informáticos.

A proposta estabelece ainda a criação de um Fundo de Segurança Cibernética, destinado ao financiamento de ações estratégicas para o reforço da resiliência digital nacional. Esta previsão normativa evidencia o comprometimento do legislador moçambicano com uma abordagem integrada, colaborativa e orientada por princípios de transparência e responsabilidade partilhada no enfrentamento dos desafios emergentes do ciberespaço.

Não obstante o mérito da iniciativa legislativa, importa assinalar que, face à crescente utilização de ferramentas de IA por agentes ciberdelinquentes para a realização de ataques automatizados, disseminação de conteúdos manipulados (*deepfakes*), adulteração de dados e exploração ampliada de vulnerabilidades sistémicas, a proposta de lei revela uma orientação predominantemente voltada ao combate de infrações tradicionais e incidentes cibernéticos já conhecidos. Deste modo, a proposta carece de mecanismos específicos e adequados para responder aos riscos emergentes associados à cibercriminalidade potenciados por tecnologias avançadas de IA.

3.4.2. Proposta de Lei de Prevenção e Repressão dos Crimes Cibernéticos⁷

A proposta de Lei de Prevenção e Repressão dos Crimes Cibernéticos também disponível no portal do INTIC, numa rápida leitura, foi possível verificar que, mesma visa estabelecer um quadro jurídico para regular os crimes cibernéticos, abrangendo tanto as condutas ilícitas relacionadas ao uso de tecnologia de informação e comunicação quanto os processos de investigação e cooperação internacional nesses delitos.

A proposta define um conjunto de infrações cibernéticas, incluindo o acesso ilícito a sistemas informáticos, a interceção não autorizada de comunicações, a interferência indevida em sistemas e dados, bem como a falsificação digital. Para além disso, estabelece as bases para a responsabilização penal de pessoas singulares e coletivas, prevendo igualmente os procedimentos aplicáveis à preservação, apreensão e obtenção de provas em suporte eletrónico, em conformidade com os princípios do processo penal digital.

Adicionalmente, a proposta de lei procura facilitar a cooperação internacional entre as autoridades nacionais e estrangeiras na investigação e repressão de crimes cibernéticos, instituindo mecanismos formais de troca de informações, salvaguardando a confidencialidade dos dados partilhados e promovendo a assistência mútua em matéria penal.

Em termos gerais, a proposta visa estabelecer um quadro legal que proteja eficazmente os sistemas informáticos, assegure a recolha célere e tecnicamente válida de provas digitais, e responsabilize criminalmente os agentes infratores, sejam pessoas singulares ou coletivas

Contudo, mais uma vez, a eficácia da proposta legislativa em responder, de forma específica, aos crimes praticados com recurso à IA revela-se questionável. A título exemplificativo, o artigo 1.º, relativo ao âmbito de aplicação, e o artigo 2.º, referente ao objeto da lei, referem-se

⁷ República de Moçambique. (2024). *Proposta de Lei n.º /2023 de Prevenção e Repressão dos Crimes Cibernéticos*. Assembleia da República.

genericamente aos crimes cometidos através do uso das tecnologias de informação e comunicação, incluindo os sistemas informáticos e os suportes eletrónicos.

No entanto, não se verifica qualquer menção explícita aos modos específicos pelos quais a IA pode ser instrumentalizada na prática de cibercrimes como é o caso da produção e disseminação de *deepfakes*, da automação de ciberataques, da manipulação massiva de dados ou da utilização de algoritmos de *machine learning* para fins maliciosos.

Esta omissão legislativa, ao deixar de prever dispositivos normativos específicos para tratar dos riscos e condutas ilícitas associadas ao uso avançado de IA, pode comprometer a efetividade da proposta no combate as novas tipologias criminais digitais.

No que concerne à operacionalização do segundo subpilar, relativo à ratificação de convenções internacionais em matéria de segurança cibernética, importa destacar que Moçambique registou um avanço significativo ao ratificar a Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais, este passo revela um compromisso claro com os princípios orientadores da Estratégia de Transformação Digital para África (2020–2030), bem como com a harmonização normativa no espaço continental africano.

Todavia, importa sublinhar que, apesar do seu valor simbólico e normativo, a referida convenção não oferece respostas suficientemente robustas face aos novos desafios impostos pela criminalidade cibernética potenciados pela inteligência artificial., tal como referido anteriormente.

A nível sistémico, importa referir que Moçambique ainda não ratificou a Convenção de Budapeste sobre o Cibercrime⁸, principal instrumento internacional de natureza vinculativa no domínio da prevenção, repressão e cooperação internacional no combate aos crimes cibernéticos.

No entanto, o país tem demonstrado avanços no processo de adesão a este tratado, o qual estabelece padrões mínimos e harmonizados para a tipificação de condutas ilícitas no ciberespaço,

⁸ Conselho da Europa. (2001). *Convenção sobre o Cibercrime* (Convenção de Budapeste). Budapeste, 23 de novembro de 2001.

RPCJ, Portugal-PT, V.6, Nº1, p. 14-34, Jan./Jul. 2025 www.revistas.editoraenterprising.net

mecanismos de obtenção e preservação de provas eletrónicas, bem como procedimentos de cooperação judiciária e policial transfronteiriça

Desde fevereiro de 2024, Moçambique participa, na qualidade de Estado Observador, nas sessões do Comité da Convenção de Budapeste. Mais recentemente, uma delegação moçambicana marcou presença na 32.^a Sessão do referido Comité, realizada nos dias 2 e 3 de junho de 2025, no âmbito do Conselho da Europa, em Estrasburgo.

A adesão à Convenção de Budapeste implicará que Moçambique proceda a reformas legislativas substanciais, bem como ao fortalecimento institucional das suas estruturas de segurança cibernética, de modo a conformar-se com os padrões internacionais exigidos pelo tratado.

No entanto, permanece uma lacuna crítica no que respeita à incorporação de medidas específicas para o combate dos crimes cibernéticos praticados com recurso à IA.

Para que a resposta normativa seja efetiva, as reformas legislativas devem ser acompanhadas de regulamentações técnicas especializadas e programas de capacitação institucional que contemplem, de forma direta e atualizada, os riscos, os métodos e as dinâmicas operacionais associados ao uso malicioso da IA.

Não obstante o crescimento exponencial dos crimes cibernéticos perpetrados com recurso à IA, observa-se, em Moçambique, uma relativa inércia legislativa face a esse fenómeno emergente, o legislador tem conferido primazia à repressão de delitos tradicionais e à regulação de incidentes tecnológicos já conhecidos, em detrimento de uma abordagem normativa proativa e especializada voltada para as ameaças sofisticadas introduzidas pela IA como já exposto nos pontos anteriores.

4. Da Urgência Legislativa face à Cibercriminalidade com Recurso à IA

A crescente interconexão global, impulsionada pela revolução digital e pela massificação da IA, tem gerado profundas transformações na estrutura dos delitos informáticos, introduzindo uma nova geração de ameaças que desafia a arquitetura tradicional dos sistemas jurídicos.

A IA, ao mesmo tempo que oferece oportunidades significativas de desenvolvimento tecnológico e inovação, está a ser instrumentalizada por agentes mal-intencionados para perpetração de crimes altamente sofisticados, automatizados e de difícil rastreamento.

Segundo o relatório *Cybersecurity Threat Trends 2023*, da INTERPOL, "o uso de IA para fins ilícitos já não é uma previsão teórica, mas uma realidade concreta com impactos reais sobre instituições financeiras, sistemas eleitorais e infraestruturas críticas" (INTERPOL, 2023, p. 6)⁹.

Técnicas como *deepfakes*, *machine learning* para engenharia social e automação de ataques por *bots* autoadaptativos estão a ser empregues em fraudes digitais, ataques à honra de autoridades públicas, manipulação de processos eleitorais e desinformação em larga escala (FLORIDI & COWLS, 2020¹⁰; BRUNDAGE ET AL., 2018¹¹).

Em África, onde os quadros normativos sobre cibersegurança e tecnologias emergentes ainda se encontram em construção, o desafio torna-se ainda mais agudo. Moçambique, em particular, tem registado um crescimento do uso da tecnologia no setor público e privado, mas sem o correspondente fortalecimento institucional e legislativo para mitigar os riscos associados. A ausência de uma legislação especializada que regule a criminalidade cibernética com recurso a IA representa um vácuo normativo estratégico, sobretudo num contexto em que as fragilidades institucionais e a instabilidade política tornam o país suscetível à infiltração digital e à manipulação algorítmica.

Como alerta Chertoff & Simon (2021)¹², “as democracias em desenvolvimento estão na linha de frente da nova guerra digital, onde algoritmos podem ser mais perigosos do que armas convencionais”. Esta constatação reforça a necessidade de uma resposta urgente e coordenada,

⁹ INTERPOL. (2023). *Cybersecurity Threat Trends 2023: Preparing for Artificial Intelligence-Driven Threats*. INTERPOL Global Cybercrime Programme.

¹⁰ Floridi, L., & Cowls, J. (2020). *A Unified Framework of Five Principles for AI in Society*. Harvard Data Science Review, 2.

¹¹ Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute.

¹² Chertoff, M., & Simon, T. (2021). *The impact of artificial intelligence on democracy and the rule of law*. European Commission for Democracy through Law (Venice Commission).

RPCJ, Portugal-PT, V.6, N°1, p. 14-34, Jan./Jul. 2025 www.revistas.editoraenterprising.net

especialmente legislativa, que alinhe Moçambique com os princípios da ciberdefesa contemporânea, da proteção da soberania digital e da integridade institucional.

A criminalidade digital está a atravessar uma fase de mutação profunda, e a introdução da IA marca a transição para um novo paradigma criminal, esta nova realidade não apenas amplia o leque de ameaças digitais, como também desafia diretamente os pressupostos clássicos do Direito Penal e Processual Penal.

A IA, enquanto tecnologia dual com potencial tanto para o bem quanto para o mal permite o surgimento de modalidades sofisticadas de crimes, com difícil rastreamento, elevada escala e impacto geopolítico sensível.

Os crimes com recurso à IA não se limitam ao uso de computadores, trata-se de condutas ilícitas assistidas ou potenciadas por sistemas inteligentes, que podem agir com autonomia parcial ou total.

Entre as manifestações mais relevantes estão: (i) *deepfakes*, considerado como sendo a manipulação audiovisual que forja rostos, vozes e contextos para fins de extorsão, chantagem, fraude ou desinformação política; (ii) ataques automatizados por *bots* com *machine learning*, capazes de contornar sistemas de segurança e adaptar-se em tempo real; (iii) manipulação de mercados financeiros e algoritmos bancários, explorando brechas regulatórias e lógicas de *scoring* digital; e (iv) sabotagem de infraestruturas críticas por IA militar ou ciberferramentas autônomas.

Como bem observa Brundage et al. (2018), o uso malicioso da IA inaugura uma nova era de crimes transfronteiriços, assimétricos, e com enorme capacidade de causar disrupção em sistemas democráticos, económicos e institucionais.

Em termos práticos, já se registam internacionalmente, como é o caso de tentativas de golpes de Estado digitais por manipulação de redes sociais com IA (uso massivo de *bots* para criar revoltas, deslegitimar líderes ou incitar violência), as ciberextorsões baseadas em IA que analisam o comportamento da vítima e enviam ameaças personalizadas, o *phishing* com IA que imita padrões linguísticos da vítima, tornando o engano mais verosímil e ataques a sistemas eleitorais, por alteração ou manipulação dos sistemas de contagem automatizada.

Em Moçambique, apesar da baixa incidência notificada, o risco é iminente, principalmente em contextos como o recenseamento eleitoral digital, o uso de plataformas públicas online e a desinformação em períodos sensíveis.

Como já demonstrado em análises anteriores, nem a proposta de Lei de Segurança Cibernética, de Crime Cibernético (em consulta pelo INTIC), nem a adesão parcial às convenções internacionais, abordam de forma técnica e explícita os crimes com recurso a IA.

A ausência de tipificações próprias e de dispositivos de previsão e repressão limita, atuação célere do Ministério Público, a capacidade de obtenção de prova digital admissível em juízo e a articulação entre agências nacionais e internacionais de combate ao cibercrime.

É urgente que Moçambique adote uma agenda de reforma penal tecnológica, que inclua: (i) novas tipificações penais específicas para crimes com IA (*deepfakes*, ataques algorítmicos, sabotagem automatizada, manipulação de *big data*); (ii) princípios constitucionais sobre supervisão algorítmica e não discriminação automatizada; (iii) capacitação técnica de magistrados, investigadores e peritos digitais; e (iv) criação de uma Autoridade Nacional para a Ética e Regulação da Inteligência Artificial, com poderes sancionatórios e preventivos.

Como afirma Chertoff e Simon (2021), “os Estados precisam legislar não apenas contra o uso da IA como arma, mas também contra a sua instrumentalização para corroer os próprios fundamentos da democracia, como a verdade, a justiça e o Estado de Direito”.

5. Conclusão

A presente análise permitiu demonstrar, com base no quadro normativo vigente e nas propostas legislativas em curso, que Moçambique se encontra diante de um desafio jurídico de elevada complexidade, a crescente sofisticação da criminalidade cibernética mediada por IA está a ultrapassar, em velocidade e impacto, a capacidade de resposta do sistema legal nacional.

O estudo evidenciou que, apesar de existirem normas relevantes como a Lei das Telecomunicações, a Lei de Transações Eletrónicas e a adesão à Convenção de Malabo, tais

instrumentos carecem de dispositivos específicos, técnicos e atualizados capazes de responder eficazmente aos crimes cibernéticos potenciados por IA.

A análise revelou igualmente que as duas propostas de lei submetidas pelo INTIC em 2024, ainda que representem um avanço no fortalecimento institucional da cibersegurança, não contemplam, de forma expressa e sistematizada, a criminalidade algorítmica, como *deepfakes*, sabotagens automatizadas ou ataques baseados em *machine learning*.

Esta omissão normativa compromete não apenas a repressão, mas também a prevenção e a cooperação judiciária internacional, sobretudo face à transversalidade e ao carácter transfronteiriço desses novos ilícitos.

Do ponto de vista doutrinário e comparado, confirma-se que a IA tem sido instrumentalizada para fins ilícitos com grande potencial disruptivo, podendo inclusive financiar ou catalisar formas não convencionais de golpes de Estado digitais, manipulação de processos eleitorais, engenharia social avançada e erosão da confiança nas instituições públicas.

Esta constatação eleva a cibercriminalidade com IA a uma questão de segurança nacional e de estabilidade democrática.

Face a este cenário, impõe-se uma agenda de urgência legislativa, centrada em três eixos fundamentais: (I) reforma penal tecnológica, com a introdução de tipos penais específicos para crimes praticados com IA, bem como normas procedimentais para preservação e validação de provas digitais complexas; (ii) reforço constitucional e institucional, com a previsão de princípios de não discriminação algorítmica, supervisão judicial dos sistemas automatizados, e criação de uma autoridade nacional independente para a ética e regulação da IA; e (iii) alinhamento internacional estratégico, com a ratificação da Convenção de Budapeste, a internalização plena da Convenção de Malabo e o estabelecimento de canais robustos de cooperação transfronteiriça.

Conclui-se, pois, que a resposta do Estado moçambicano à cibercriminalidade com recurso à IA não pode continuar a ser genérica, fragmentada ou reativa, é necessário transitar para um paradigma normativo proactivo, especializado e integrado, que proteja os direitos fundamentais,

preserve a soberania digital e assegure a continuidade do Estado de Direito perante os desafios emergentes da era algorítmica.

6. Referencia Bibliográfica

Livros:

BRUNDAGE, M., AVIN, S., CLARK, J., TONER, H., ECKERSLEY, P., GARFINKEL, B., ... & AMODEI, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute.

CHERTOFF, M., & SIMON, T. (2021). *The impact of artificial intelligence on democracy and the rule of law*. European Commission for Democracy through Law (Venice Commission).

FLORIDI, L., & COWLS, J. (2020). *A Unified Framework of Five Principles for AI in Society*. Harvard Data Science Review, 2.

INTERPOL. (2023). *Cybersecurity Threat Trends 2023: Preparing for Artificial Intelligence-Driven Threats*. INTERPOL Global Cybercrime Programme.

Legislação:

Assembleia da República de Moçambique. (2016). Lei n.º 4/2016, de 3 de junho, que altera a Lei n.º 8/2004, de 21 de junho, Lei das Telecomunicações. Boletim da República, I série, n.º 66, 3 de junho de 2016.

Assembleia da República de Moçambique. (2017). Lei n.º 3/2017 de 9 de janeiro: Lei de Transações Eletrônicas. Moçambique.

República de Moçambique. (2024). Proposta de Lei n.º /2023 de Segurança Cibernética (versão 7.0, 15 de março de 2024). Assembleia da República.

República de Moçambique. (2024). Proposta de Lei n.º /2023 de Prevenção e Repressão dos Crimes Cibernéticos. Assembleia da República.

Convenções:

União Africana. (2014). *Convenção da União Africana sobre a Cibersegurança e a Proteção de Dados Pessoais* [Convenção de Malabo]. Malabo, Guiné Equatorial.

Conselho da Europa. (2001). *Convenção sobre o Cibercrime* (Convenção de Budapeste). Budapeste, 23 de novembro de 2001.

ABSTRACT

The growing use of artificial intelligence (AI) as a tool for committing cybercrimes has posed significant challenges to traditional legal frameworks, requiring more technical and up-to-date regulatory responses from national legal systems. In Mozambique, although there are relevant legal instruments such as the Telecommunications Law, the Electronic Transactions Law, and the Penal Code as well as legislative proposals under discussion, there remains a lack of specific provisions addressing AI-driven cybercrime. This article aims to critically examine the current legal framework and the legislative proposals in progress, assessing their adequacy in responding to the emerging risks associated with the malicious use of AI. The study adopts a qualitative, exploratory, and descriptive approach, based on documentary analysis, legal hermeneutics, and comparative methods. The findings reveal a significant normative gap concerning the criminalization of practices such as deepfakes, algorithmic data manipulation, and automated cyberattacks, which undermines the effectiveness of the fight against contemporary digital crime. The article concludes that there is an urgent need for comprehensive legal reform that includes specific criminal provisions, algorithmic oversight mechanisms, international cooperation instruments, and the enhanced protection of fundamental rights in the digital environment.

Keywords: Cybercrime; Artificial Intelligence; Legal Reform; Mozambique; Algorithmic Regulation.