UNIVERSIDADE
EDUARDO
MONDLANE

FACULDADE DE DIREITO

LICENCIATURA EM DIREITO

Trabalho de Fim de Curso

Tema:

SITUAÇÃO JURÍDICA DO CIBERCRIME EM MOÇAMBIQUE

Licenciando: Júlia José Tembe

Supervisor: Prof. Doutor Manuel Castiano

Maputo, Fevereiro de 2024

JÚLIA JOSÉ TEMBE

SITUAÇÃO JURÍDICA DO CIBERCRIME EM MOÇAMBIQUE

Supervisor

Prof. Doutor Manuel Castiano

Monografia a ser apresentada à Faculdade de Direito da Universidade Eduardo Mondlane, como requisito parcial para a conclusão do Curso de Licenciatura em Direito.

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE DIREITO

Maputo, Fevereiro de 2024

Agradecimentos

Em primeiro lugar agradecer a Deus pela vida, saúde e por sempre me acompanhar nos momentos cruciais da minha vida.

Agradecer, em segundo lugar, à minha família por todo o apoio proporcionado. Um especial agradecimento aos meus irmãos, Beto e Gil, pela paciência buscando-me à paragem incansavelmente, todas as noites, e à minha mãe, Refinalda, que sempre esteve disposta a me apoiar sempre que necessário.

Um obrigada muito especial às minhas amigas Cleyde e Vanessa, o presente que a Faculdade me ofereceu e que carrego com estima e amor por toda a vida. Obrigada amigas pelo apoio durante toda a caminhada.

E, por fim, ao meu supervisor, Prof. Doutor Manuel Castiano, pela orientação prestada e pelos ensinamentos partilhados.

Dedicatória

Dedico a presente Monografia ao meu saudoso pai, José Baptista Tembe (em memória) que sempre me apoiou e incentivou a correr atrás dos meus sonhos.

RESUMO

O presente trabalho surge no âmbito das exigências curriculares de Trabalho de Fim de Curso, para a obtenção do grau de Licenciatura em Direito pela Universidade Eduardo Mondlane, subordinando-se ao tema: **"Situação Jurídica do Cibercrime em Moçambique"**. Este trabalho aborda a situação legal do cibercrime em Moçambique, descrevendo a actual situação legislativa e os desafios enfrentados no combate ao cibercrime, discutindo se as leis existentes bastam para inibir os crimes cibernéticos ou se deve haver uma melhoria legislativa com vista a acompanhar as necessidades actuais das ameaças cibernéticas. Para isso, foi feita uma pesquisa descritiva, usando-se a abordagem qualitativa, utilizando livros que abordam o tema, artigos científicos e análise documental, para a aquisição de maior domínio sobre o tema. O estudo conclui com a insuficiência da legislação actual para responder à grande demanda de cibercrime e à necessidade de melhoramento da eficácia das leis, através da actualização contínua e elaboração de um dispositivo legal que determine o regime geral dos crimes cibernéticos.

Palavras-chave: redes de conexão, cibercrime, segurança cibernética.

ABSTRACT

The present work arises within the scope of the curricular requirements of Final Course Degree in Law from the Eduardo Mondlane University, under the theme: “Legal Situation of Cybercrime in Mozambique”. This work addresses the legal situation of cybercrime in Mozambique, describing the current legislative situation and the challenges faced in combating cybercrime, discussing whether existing laws are sufficient to inhibit cybercrime or whether there should be legislative improvement in order to keep up with current needs of cyber threats. For this, descriptive research was carried out, using a qualitative approach, using books that address the topic, scientific articles and documentary analysis to acquire greater knowledge of the topic. The study concludes with the insufficiency of the current legislation to respond to the great demand for cybercrime and the need to improve the effectiveness of laws, through continuous updating and elaboration of the legal provision that determines the general regime of cybercrimes.

Key words: connection networks, cybercrime, cybersecurity.

ÍNDICE

Principais Abreviaturas e Siglas

Art. – Artigo;

CCE – Convenção do Conselho da Europa;

CP – Código Penal;

CRM – Constituição da República de Moçambique;

IA- Inteligência Artificial;

INTIC – Instituto Nacional de Tecnologias de Informação e Comunicação;

IP – Internet Protocol;

nº - Número;

p. - Página

PGR – Procuradoria Geral da República;

UE – União Europeia;

TIC's – Tecnologias da Informação e da Comunicação.

Introdução

De acordo com o professor Reginaldo César Pinheiro, com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente, se percebe que nem todos a utilizam de maneira sensata e acreditando que a Internet é um espaço livre, acabam por cometer excessos nas suas condutas e criando novas modalidades de delitos: os crimes virtuais.[1]

O estudo dos crimes cibernéticos é importante no mundo contemporâneo, pois estamos em uma era digital onde a tecnologia de informação e a Internet desempenham papéis essenciais em quase todos os aspectos da vida quotidiana. Os crimes cibernéticos não ameaçam somente a segurança e privacidade de pessoas individuais mas também têm potencial de causar danos à economia, segurança nacional e estabilidade social. Os crimes cibernéticos vão desde o roubo de informações confidenciais e financeiras até à disseminação de desinformação, além de ataques a estruturas do Governo. Por estas razões, é importante que as leis acompanhem a essa evolução dos crimes, através da criação de dispositivos que criminalizem as diversas condutas que lesam os bens jurídicos que o Estado protege e da promoção das normas de combate ao cibercrime.

O nosso ordenamento jurídico está empenhado em combater esse fenómeno crescente e encontra-se minimamente preparado para a responder à questões de cibercriminalidade, pois dispõe de leis que contemplam artigos relacionados ao cibercrime, bem como brigadas destinadas somente a receber e tratar situações de cibercriminalidade. A Lei nº 24/2019, de 24 de Dezembro, que aprova o Código Penal, dispõe de artigos que estão em perfeita harmonia com a Convenção de Budapeste.[2] No entanto, Moçambique encontra-se, ainda, no processo de adesão à Convenção.

[1] Apud FIORILLO, Celso Antonio; CONTE, Christiany. Crimes no Meio Ambiente Digital. 2. Ed. São Paulo, 2016, P. 183

[2] Convenção sobre o Cibercrime, assinada no âmbito do Conselho da Europa. É considerado o maior tratado internacional sobre crimes cibernéticos e tem como objectivo principal o estabelecimento de vias de cooperação internacional em matéria penal e processual e ainda a criação de procedimentos uniformes para o combate ao cibercrime.

Para além do preparo legislativo, é de igual modo necessária uma capacitação técnica e processual através de agentes e meios de investigação que lidem exclusivamente com o fenómeno, visto que este carece de especial atenção por estar sempre em evolução.

O presente trabalho tem em vista descrever o actual cenário legislativo face ao cibercrime bem como demonstrar as melhorias que podem ser feitas com vista à protecção do cidadão e da segurança nacional contra a cibercriminalidade. O trabalho está dividido em quatro capítulos, onde o primeiro procura dar uma visão geral do cibercrime, a sua definição, os elementos constitutivos, os tipos de cibercrime e a manifestação do cibercrime em Moçambique. O segundo capítulo trata dos meios processuais do cibercrime em Moçambique, neste procuramos entender como é feita a prossecução penal nos crimes cibernéticos, incluindo todo o processo investigativo e suas dificuldades. O terceiro capítulo designa-se "Regime Jurídico do Cibercrime em Moçambique" e nele procuramos entender o actual cenário legislativo de Moçambique perante o cibercrime. Neste capítulo, revisamos a actual situação jurídica do cibercrime e apontamos as melhorias a serem feitas em prol da segurança cibernética no nosso país. E por último, o capítulo quarto fala da eficácia dos actuais dispositivos jurídicos voltados ao cibercrime, dos desafios enfrentados pela actual legislação e se essa legislação tem feito o seu papel no combate a esse fenómeno mundial.

0.1.PROBLEMA

As redes de conexão têm um papel prepondenrante na sociedade contemporânea. Elas estão presentes em todos os aspectos da vida, inclusive em áreas mais importantes do Governo.

As redes ajudam na rápida interação, no processamento e armazenamento de informação e poupam-nos dos métodos analógicos e demorados. Porém, no em meio de diversas vantagens do seu uso, surgem vários inconvenientes como o crescente aparecimento de novas e sofisticadas formas de crime e de diversos criminosos. O cibercrime surge nesse contexto e ocorre quando se faz uso das redes de conexão para o cometimento de actividades criminosas.

Para se fazer face a esses crimes, é necessário um preparo legislativo eficaz. O aprimoramento das normas de combate ao cibercrime se mostra necessário, para o fortalecimento dos meios de prevenção, investigação e punição dos crimes cibernéticos. O cenário dos crimes cibernéticos está em constante evolução, com novas técnicas e ameaças,

surgindo regularmente e tornando a segurança cibernética uma causa preocupante em todo o mundo.

A renomada Professora, Ivette Ferreira (especialista em Direito Digital e Crimes Cibernéticos) destaca que para lidar com o cibercrime é necessária uma legislação actualizada e abrangente, pois estes crimes geralmente transcendem fronteiras e, por isso, requerem cooperação internacional.

Com o presente trabalho, pretendemos compreender como está a situação legal do cibercrime em Moçambique, abordando a legislação específica existente, as possíveis lacunas e os obstáculos na aplicação das leis para enfrentar as ameaças cibernéticas.

Como forma de guiar este estudo, levanta-se a seguinte pergunta de partida: **Como podemos entender a eficácia e adequação do actual quadro jurídico para lidar com o cibercrime?**

0.2 JUSTIFICATIVA

A escolha do tema foi influenciada pelo aumento significativo da onda de cibercriminalidade que se verifica no nosso país e no mundo. O cibercrime necessita de um tratamento especial, devido às suas características e sua susceptibilidade de tomar proporções gigantescas, podendo facilmente levar a um concurso de crimes. A capacidade que o cibercrime tem de envolver grandes organizações criminosas e terroristas é também factor alarmante e que carece de devida atenção. Para além disso, o cibercrime é ainda caracterizado pelo fácil desaparecimento da prova, por isso é necessário um célere tratamento e investigação dos casos.

Face a esses aspectos caracterizadores, demonstra-se ser crucial o estudo desse fenômeno, pois envolve a segurança nacional. Face ao uso frequente dos meios digitais no nosso quotidiano é naturalmente compreensível o aumento dos casos de crimes cibernéticos, por isso, o ordenamento jurídico deve acompanhar a essa evolução, através da melhoria e aprimoramento das suas normas e das técnicas de combate ao crime cibernético.

Com isso, esperamos que com o presente trabalho, se possa identificar as melhorias a serem feitas no âmbito jurídico moçambicano, para o enfrentamento das ameaças cibernéticas locais, bem como para uma melhor cooperação com outros ordenamentos.

2.Objectivos

2.1 Geral

- Analisar o actual quadro jurídico do cibercrime em Moçambique.

2.2 Específicos

- Identificar o regime jurídico do cibercrime em Moçambique;
- Verificar a actuação das autoridades na investigação do cibercrime em Moçambique;
- Identificar os meios processuais do cibercrime no nosso ordenamento jurídico;
- Analisar a eficácia das actuais normas de combate ao cibercrime.

3. Hipóteses

- A actual legislação é insuficiente para responder às situações de cibercrime.

- O melhoramento da lei reduziria os casos de cibercrime.

4. Metodologia

Para a realização deste trabalho foram utilizados os seguintes métodos:

- Pesquisa bibliográfica recorrendo a manuais de autores, artigos científicos e outros documentos académicos;
- Pesquisa de documentos, analisando documentos jurídicos como o Código Penal, a Convenção de Malabo e a Lei de Cooperação Internacional.

I.CIBERCRIME NO ORDENAMENTO JURÍDICO MOÇAMBICANO

O cibercrime ou crime cibernético refere-se aos crimes cometidos por via das redes de conexão ou das TIC's no geral.

Para Gustavo Testa Correa (que usa a terminologia **crimes digitais)**, crimes digitais são todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática, é indispensável a utilização de um meio electrónico[3]

Este tipo de crime tem diversas designações, tais como crime informático, crime digital, crime electrónico, crime cibernético, entre outras que se referem à mesma actividade. Para os propósitos deste trabalho, adoptaremos o termo **crime cibernético.** Em geral, o crime cibernético ocorre quando um indivíduo usa uma rede de conexão para praticar um acto ilícito ou tirar vantagem de terceiros. Mas, também pode referir-se ao uso de computador como instrumento de ataque ou ainda quando o alvo de ataque é outro computador ou tecnologia.

O cibercrime ocorre no meio virtual, para que o seu tipo legal esteja preenchido é necessário que o infractor esteja conectado a uma rede e que use ela como meio para a consumação do crime. No cibercrime, o usuário comum é o mais vulnerável, por desconhecimento, ou por não acreditar na gravidade da situação e sucumbe aos golpes.

Fernando e Guilherme de Souza Nucci, na intenção de elucidar a interpretação do tema, dispõem que o **bem jurídico tutelado** que a lei procura proteger, será a liberdade individual da pessoa como forma directa, já indiretamente abrange tanto a intimidade quanto a privacidade e a inviolabilidade de se comunicar e de se corresponder. A **acção central** da conduta, a **tipificação do crime,** é o acto de invadir sem permissão a segurança de algum dispositivo electrónico de alguém, **sendo esse o crime**. Portanto, o crime constitui-se no acto ilegal de invadir o dispositivo de alguém, sendo esta uma violação indevida do mecanismo de segurança com finalidade de obter, adulterar ou destruir as informações do dispositivo.

[3] CORREA, Gustavo Testa. Aspectos Jurídicos da Internet. São Paulo. Saraiva, 2000. P. 43

O **sujeito activo** do acto é qualquer pessoa que invade sem autorização os equipamentos electrónicos. O **sujeito passivo**, a pessoa que sofra a consequência do sujeito activo.[4]

Este tipo de crime surgiu com a eclosão da Internet. Embora a Internet tenha surgido como parte da globalização e com o objetivo de tornar a vida mais fácil, reduzindo o tempo, encurtando distâncias e revolucionando a maneira de fazer negócio, o surgimento das novas tecnologias trouxe consigo novas formas de crime, assim como novos meios de cometimento de crimes que já existiam. O cibercrime não é necessariamente um novo tipo legal de crime. A maior parte dos crimes que fazem parte do cibercrime são crimes que já existiam, já eram cometidos de outras formas, o que acontece é que com o surgimento das redes de Internet, surgiram novos meios para o alcance de um fim, são crimes velhos com um novo *modus operandi*, é o caso de crimes como difamação, injúria e ameaça. De acordo com Jesus e Milagre, facto é que a maior parte dos crimes electrónicos está relacionada a delitos em que o meio para a realização da conduta é virtual, mas o crime em si não. (Jesus e Milagre, 2016, p. 50)

Uma das grandes diferenças do cibercrime e dos crimes tradicionais (ou comuns), é o uso das tecnologias, que ocorre no cibercrime. Os crimes tradicionais são cometidos sem qualquer auxílio das novas tecnologias, já o cibercrime envolve diretamente o uso das novas formas de conexão.

Alburquerque, avança a seguinte classificação dos crimes cibernéticos:

Crimes Informáticos Puros: os que corresponderiam aos crimes em que dados e sistemas informáticos constituem o objecto do crime[5] e os **crimes informáticos impuros** diriam respeito aos crimes em que os recursos informáticos constituem o meio de execução, tendo como objecto, bens jurídicos que já são protegidos por tipos penais existentes.[6]

José de Castro Meira distingue crimes informáticos puros e impuros da seguinte forma: os **puros**, são aqueles praticados contra o sistema de computadores em si mesmos. Já os **impuros**, já se encontram devidamente tipificados no ordenamento jurídico pátrio, uma vez

[4] Apud, BEZERRA, Clara Augusta, 2020, p. 15
[5] ALBURQUERQUE, Roberto Chacon de. A Criminalidade Informática. São Paulo, Editora Juarez de Oliveira, 2006, p. 40 e 41.
[6] IDEM.

que o manuseio do computador e da Internet é mero meio, simples codificação no modus operandi do delito, não implicando no delito.[7]

Do acima exposto, verifica-se que, para a classificação do cibercrime, importa o bem jurídico lesionado, neste caso, os sistemas informáticos para o cibercrime puro e também o meio usado para o cometimento do crime, os recursos informáticos são simplesmente meios de execução de crimes já existentes no cibercrime impuro.

O cibercrime é um ataque direcionado não à pessoa física, mas à informação, património, reputação das pessoas, organizações ou então governos.

Estes crimes podem ser cometidos em locais diferentes do nosso espaço jurídico. Isto quer dizer que alguém, em determinado ordenamento **X**, pode efectuar um ataque contra o património de uma determinada empresa **Y**, com sede em Moçambique, por exemplo. Daí a necessidade de cooperação entre os países para a resolução desse tipo de crime.

Existem teorias que tentam explicar a motivação dos criminosos ao cometer esses crimes. Das várias teorias, destacam-se a Teoria da Escolha Racional e a Teoria da Desorganização Social. A Teoria da Escolha Racional advoga que os criminosos cometem crimes cibernéticos, depois de pesar os benefícios e os custos potenciais. Isto é, por um lado, eles consideram a probabilidade de serem detidos e punidos, em comparação com os ganhos que vão adquirir com essas acções, por outro lado.

Já a Teoria da Desorganização Social, argumenta que a falta de controlo social online, a ausência de regulamentação eficaz e a falta de supervisão podem levar ao aumento do cibercrime. Com isso, constata-se uma grande necessidade de regular de forma eficaz o mundo digital, para tentar travar esse aumento do cibercrime e garantir uma maior segurança cibernética.

Em Moçambique, não seria diferente. O cibercrime tem ganhado mais espaço, devido ao crescente uso das redes de conexão por meio da população.

[7] MEIRA, José de Castro. A tutela penal dos cybercrimes e o projecto de Lei contra os crimes de informática. Revista da Fundação Escola Superior do Ministério Público do Distrito Federal e Territórios. Brasília, 2007, p. 156 e 157.

Para salvaguardar os interesses da sociedade, é necessário um maior investimento em leis que vão de alguma forma garantir a segurança cibernética. É verdade que dificilmente nos iremos sentir completamente seguros, pois o mundo virtual é um mundo em constante evolução, porém, o nosso ordenamento deve buscar formas de acompanhar a essa evolução. O nosso governo reconhece a necessidade do reforço das leis de combate ao cibercrime.[8]

Nos últimos anos, temos verificado uma maior predominância de crimes como a fraude relativa aos meios de pagamento electrónico, o roubo de identidade, a burla informática, roubo de dados pessoais e financeiros, bem como chantagens online. A quantidade de informações disponibilizadas online permite que qualquer pessoa acesse e isso torna-nos extremamente vulneráveis à acção de criminosos, isso aliado à facilidade que estes têm de ocultar a sua identidade.

A facilidade de ocultar a identidade, o anonimato e a dificuldade de localizar os criminosos e de avançar com a prossecução penal podem gerar uma sensação de impunidade.

De acordo com Ferreira:

“por isso, temos a sensação de impunidade, sendo um atrativo muito forte para o crescimentodesse tipode delito. As ameaças podem ser tanto por meio de monitoramentos não autorizados do sistema com a (DEEP WEB), como através de ataques mais sofisticados por hackers.” (Ferreira, 2015, p.32)

O INTIC tem tomado medidas que visam assegurar a protecção do cidadão no espaço cibernético nacional. Nesse âmbito, o INTIC operacionalizou uma equipa nacional de resposta a Incidentes Cibernéticos, que é uma iniciativa do governo em coordenação com o sector privado e comunidades académicas e científicas, com o objectivo de atenuar/amenizar os efeitos dos ataques cibernéticos no país. Estas iniciativas são avançadas no âmbito da Política Nacional de Segurança Cibernética, aprovada em 2021.

Através deste canal, os cidadãos reportam casos que têm a ver com incidentes cibernéticos. O INTIC pretende com esta equipa, fortificar a capacidade das equipas moçambicanas na detenção de incidentes cibernéticos no país, incluindo a investigação, a contenção e a recuperação de dados, para os casos em que os incidentes são bem sucedidos. “Queremos também que haja mitigação das ameaças e isso envolve o desenvolvimento de medidas para

[8] https://opais.co.mz/pgr-quer-reforco-de-leis-de-combate-a-crimes-ciberneticos

poder lidar com os ataques e análises forenses, quando necessário", disse Lourino Chemane, Presidente do Conselho de Administração do INTIC.

O cibercrime está presente nos países desenvolvidos e não só. Moçambique tem sofrido ataques cibernéticos e a prova disso é o ataque que paralisou os principais sites do Governo em Fevereiro de 2022. O Governo moçambicano foi alvo de um ataque cibernético que deixou vários portais oficiais das instituições públicas temporariamente inoperacionais e onde só se via a imagem de um homem com lenço na cabeça e segurando uma metralhadora e com os dizeres "atacado por 'hackers' iemenitas" escritos em inglês.[9] Este evento demonstrou fragilidades na segurança nacional e afectou a economia da administração pública e privacidade dos cidadãos. Passou a questionar-se se o país está realmente preparado para responder à ataques cibernéticos. Este evento fez com que as autoridades e entidades do Governo tomassem mais atenção aos possíveis ataques cibernéticos e apostasse no reforço dos meios de proteção dos sistemas informáticos e dados pessoais.

[9] https://www.dw.com/pt-002/ataque-de-hackers-deixa-inoperacionais-portais-mo%C3%A7ambicanos/a-60854704

II. MEIOS PROCESSUAIS DO CIBERCRIME NO NOSSO ORDENAMENTO

O cibercrime tem um tratamento diferente dos crimes comuns.

Quanto ao "locus delicti" levanta-se as seguintes questões:

Haverá de se submeter ao direito nacional apenas os factos criminosos praticados por cidadãos ou por estrangeiros no território nacional? Ou serão abrangidos factos praticados no exterior?

Nos termos do art. 4 do Código Penal de 2019, a lei penal moçambicana é aplicável a factos praticados em Moçambique, seja qual for a nacionalidade do agente ou ainda a bordo de navio ou aeronave matriculado em Moçambique[10] e o art. 6 do mesmo dispositivo estabelece que, o lugar da prática do facto será aquele em que, total ou parcialmente, o agente tenha atuado, bem como aquele lugar em que o resultado típico se tiver produzido.

Entretanto, falando de cibercrime, o ciberespaço (*que em informática quer dizer o espaço virtual constituído por informação que circula nas redes de computadores e telecomunicações)*[11] de alguma forma dificulta a localização dos actos criminais no mundo real, devido à complexidade e vastidão do seu limite. A falta de restricções territoriais torna ainda mais complicada a atuação das autoridades nacionais. O cibercrime tem um carácter transnacional, visto que não necessita de uma proximidade física entre a vítima e o criminoso, podendo estes estar em diferentes países. Esse carácter transnacional torna impossível assegurar a segurança cibernética de forma individual, obrigando, assim, as nações a adoptar abordagens conjuntas com outros ordenamentos. Outro factor que dificulta a localização dos criminosos é o anonimato predominante no ciberespaço. Os criminosos têm maior probabilidade de se manter anónimos no mundo virtual, e isso torna o processo de recolha de provas e apreensão de suspeitos extremamente difíceis, chegando a recorrer-se a cooperação do país em que foi praticado o acto criminoso.

Nos casos em que o autor do crime e vítima estão em países diferentes, as autoridades não podem simplesmente recorrer aos procedimentos normais de investigação e apreensão.

[10] Moçambique. Lei nº 24/2019, de 24 de Dezembro. Aprova a lei de revisão do Código Penal.
[11] https://www.Infopedia-pt/dicionários/língua-portuguesa/ciberespaço

Apesar de que para os criminosos a Internet não ter fronteiras, os agentes têm o dever de respeitar a soberania de outras nações.

A soberania estatal no ciberespaço é necessária e essencial para o estabelecimento de uma ordem internacional virtual (o que chamaríamos “ciberordem”).

Outro facto que dificulta a aplicação da lei aos criminosos do ciberespaço é o facto de estes poderem operar a partir de uma localização onde a sua actividade não é criminalidazada ou não é tida como motivo para extradição. A Rússia, por exemplo, é conhecida por, relactivamente ao cibercrime, perseguir criminosos que atacam alvos domésticos e ignorar aqueles aque atacam alvos no estrangeiro. Isso permite que os criminosos actuem com total impunidade.

A apreensão dos suspeitos é também dificultada ou quase impossível pelo facto de alguns criminosos praticarem os crimes através da Deep Web. A Deep Web é uma Internet paralela que quase nunca deixa rastros, nela os hackers conseguem acessar a dados sigilosos sem deixar o seu IP e assim não serem identificados. Esses espaços são tão ocultos que até mesmo um hacker não consegue identificar outro.

1.Investigação

Como dito anteriormente, o processo de recolha de prova é extremamente difícil nesse tipo de crime. A maior parte das provas que as autoridades têm de recolher são provas digitais intangíveis. Essas provas são facilmente manipuladas no ciberespaço. Elas podem ser alteradas ou até mesmo apagadas, tornando-se um grande empecilho para o processo forense.

Outro factor crucial é o volume de provas, o material digital que pode ser encontrado que vai levar dos investigadores um dispendioso tempo e recursos de computação na identificação de elementos relevantes para o processo.

Nos casos em que os sujeitos processuais se encontram em jurisdições diferentes as investigações só podem avançar com a cooperação das autoridades de ambos os Estados, uma vez que a soberania nacional não permite investigações no interior de um território de um país estrangeiro sem a autorização expressa desse mesmo país. Em Moçambique os tramites legais desse processo de troca e ajuda mútua são regulados pela Lei nº 21/2019 de 11 de Novembro que estabelece os Princípios e Procedimentos da Cooperação Jurídica e Judiciária Internacional em Matéria Penal.

Os métodos tradicionais de cooperação internacional podem mostrar-se ineficazes no cibercrime pois os vestígios da acção criminosa podem desaparecer rapidamente enquanto decorre a tramitação legal necessária para a cooperação.

Existe a necessidade de se treinar os investigadores para a localização, preservação e análise de provas digitais e estes têm que ter a sua disposição todas as ferramentas necessárias para desempenhar as tarefas. A tecnologia está em constante evolução e os investigadores devem estar a par dos criminosos.

III.REGIME JURÍDICO DO CIBERCRIME EM MOCAMBIQUE

O nosso ordenamento jurídico tem se mostrado preocupado e engajado com a segurança cibernética, por via disso, têm sido aprovadas leis e ratificadas convenções como forma de amenizar o impacto da cibercriminalidade que se tem verificado.

A nossa jurisdição dispõe de instrumentos que regulam os crimes cibernéticos, porém, sendo estes um fenômeno em constante evolução é preciso que as leis estejam em pé de igualdade com esse crescimento por forma a garantir uma maior segurança jurídica no âmbito cibernético.

O nosso actual quadro jurídico, em relação ao cibercrime, comporta:

- Resolução nº 69/2021, de 31 de Dezembro, Política de Segurança Cibernética e Estratégia da sua Implementação;
- Resolução nº 5/2019, de 20 de Junho, Convenção da União Africana sobre Segurança e Protecção de Dados Pessoais;
- Lei nº 3/2017, de 9 de Janeiro, Lei das Transacções Electrónicas;
- Lei nº 24/2019, de 24 de Dezembro, Código Penal;
- Lei nº4/2016, de 3 de Junho, Lei das Telecomunicações;
- Regulamento de Registo de Cartões SIM, decreto nº 18/2015, de 9 de Julho;
- Decreto nº 44/2019, de 22 de Maio, que aprova o Regulamento de Protecção do Consumidor do Serviço de Telecomunicações;
- Decreto nº 67/2017, de 1 de Dezembro, Regulamento do Quadro de Interoperabilidade de Governo Electrónico;
- Resolução nº 17/2018, de 21 de Junho, Política para a Sociedade da Informação;
- Decreto nº 59/2019, de 3 de Julho, Regulamento do Sistema de Certificação Digital de Moçambique.

A existência dessa legislação específica não elimina a vulnerabilidade da nossa jurisdição para com o cibercrime. Muitas dessas leis têm lacunas que resultam na difícil aplicação das leis e também prejudicam a eficácia das mesmas.

1.A Convenção de Budapeste (Convenção do Conselho da Europa)

Um dos maiores instrumentos jurídicos de combate ao cibercrime é a Convenção do Conselho da Europa (CCE), comumente designada Convenção de Budapeste. Ela tem como principal objectivo facilitar a cooperação internacional, detecção, investigação e penalização da cibercriminalidade e apela ao estabelecimento de uma base comum de actuação legal e judicial. A princípio a Convenção de Budapeste tinha como objectivo a criação de uma legislação comum que permitisse uma maior cooperaçaão entre os Estados da União Europeia (UE) mas hoje em dia ela está aberta à assinatura por todos os países. Ela é, para os seus Estados parte, um mecanismo rápido e eficaz de cooperação internacional. Hoje ela tem como principal objetivo estabelecer regras claras e coordenadas entre os Estados para lidar com a luta contra a cibercriminalidade.

A Convenção de Budapeste é o primeiro tratado internacional que aborda as lacunas de lei relacionadas com as redes de comunicação e requer que os países actualizem e harmonizem suas leis criminais contra os tipos de cibercriminalidade nela tipificados. Ela é usada como padrão por vários países em matéria de segurança cibernética. Embora Moçambique não tenha ainda ratificado à Convenção de Budapeste, já iniciou o processou de harmonização das normas penais em conformidade com o estabelecido na Convenção, a título de exemplo temos o art. 4 do Código Penal de 2019 que contempla o princípio da territorialidade, bem como o art. 5 que prevê os factos praticados fora do território nacional, ambos consentâneos com o art. 22 da Convenção. No art. 22, a Convenção estabelece os seus critérios jurídicos que são baseados no princípio da territorialidade. Neste artigo ela determina que cada parte adoptará medidas legislativas e de outro tipo, necessárias para estabelecer jurisprudência sobre qualquer violação da lei, quando esta for cometida no seu território, embora sejam também identificadas situações em que este princípio da territorialidade pode ser ultrapassado.

1.1Limitações

A ideia base da Convenção é a harmonização das leis nacionais e definição da matéria processual interna em relação ao cibercrime, com vista melhorar a capacidade de actuação das autoridades a nível transnacional. Esta concepção é de difícil implementação, pois a maioria dos artigos da Convenção implicam a adopção de medidas legislativas ou outro tipo de implementação. E esta tarefa é dificultada pelas diferenças nas leis locais e na cultura de cada país. O nosso ordenamento jurídico já demonstrou interesse na ratificação desta convenção e actualizou as suas normais penais para que estejam em conformidade com as exigências da convenção e com ela harmonizadas, preparando assim o espaço para receber este dispositivo no nosso leque legislativo. É o caso dos artigos 4, 5 do Código Penal de 2019 e artigos 222 e 225 do Código do Processo Penal.

Portanto, nos termos da Convenção, são dois pontos essenciais a se ter em conta com vista a implantação de um regime de cooperação internacional entre os países signatários. O primeiro ponto é a lista de condutas criminosas previstas na Convenção e que devem estar presente no ordenamento jurídico do país que pretenda tornar-se signatário. E o segundo, é um conjunto de mecanismos legais e institucionais para a cooperação internacional.

2. Convenção da União Africana sobre Cibersegurança e Protecção de Dados (de Malabo)

A nível regional, Moçambique ratificou a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais (também chamada Convenção de Malabo), através da Resolução 5/2019, de 20 de Junho. Tem como objectivo definir os regulamentos críticos para o estabelecimento de um ambiente digital seguro e abordar as lacunas na legislação e no reconhecimento jurídico de comunicação e assinaturas electrónicas e ainda harmonizar as leis dos estados africanos sobre o comércio electrónico, protecção de dados, a promoção de cibersegurança e controle de crimes cibernéticos. Visa, ainda, lidar com a ausência de regulamentos específicos que protegem os consumidores, os direitos de propriedade intelectual, sistemas de dados e de informação pessoal, assim como a privacidade online.

A convenção determina no nº1 do art. 25 que cada Estado membro deve adoptar as medidas legislativas e ou regulamentares que julgar eficazes, considerando como infracções criminais substantivas os actos que afectam a confidencialidade, integridade e disponibilidade e a sobrevivência dos sistemas das TIC's, os dados que eles processam e as infraestruturas de redes subjacentes, assim como as medidas consideradas eficazes para a busca e julgamento dos criminosos.

Algumas das matérias relactivas à cibersegurança, previstas na Convenção já se encontram plasmadas no nosso ordenamento jurídico

3.Código Penal (lei nº 24/2019, de 24 de Dezembro)

Aprovado pela lei nº24/2019, de 24 de Dezembro, o Código Penal contém disposições normativas alinhadas aos preceitos das Convenções de Budapeste e de Malabo.

No âmbito da revisão do Código Penal, procurou-se harmonizar a nova lei penal às directrizes da Convenção de Budapeste, uma vez que o nosso oredenamento está no processo de adesão a esse instrumento.

A parte especial do Código Penal, dispõe nos artigos 211 a 213 o crime de pornografia de menores, que é um crime que tem atingido proporções mundiais, como afirma Malaquias. A Pornografia Infantil transformou-se em uma verdadeira calamidade social[12] (2015, p. 82). A situação piora quando os criminosos pensam que podem propagar as imagens e sair impunes. Por isso, é importante a criminalização e punição severa de todos os actos relacionados a este crime, desde a produção, divulgação e até mesmo posse de material com conteúdo pornográfico infantil. A criminalização destas condutas tem em vista proteger a formação moral da criança, proporcionando uma convivência saudável em sociedade e é dever do Estado zelar pelo desenvolvimento íntegro da criança, a integridade física, a liberdade sexual, a dignidade e a honra da criança ou adolescente são objectos jurídicos a serem tutelados pelos tipos penais[13] (Malaquias, 2015, p. 82). Nesse âmbito, a lei pune com prisão até 2 anos quem distribuir, importar, importar, exportar, divulgar, exibir ou ceder profissionalmente ou com finalidade de lucro, a qualquer título ou por qualquer meio, materiais de fotografia, filme ou gravação pornográfica de menores de dezoito anos[14]

Ainda no âmbito da harmonização da lei penal, na Convenção de Budapeste o "acesso ilegítimo", previsto e punido no art. 256 do CP, é um dos exemplos de infracções criminais que estão em conformidade com as directrizes da Convenção. Como orienta o art. 2 da Convenção, cada parte deverá adoptar medidas legislativas e outras que se mostrem necessárias para estabelecer o acesso intencional e ilegítimo a um sistema informático como infracção penal.[15] O mesmo ocorre com o crime de intercepção ilegítima (art. 3 da Convenção), previsto no nº 2, do art. 256 CP.

Portanto, é notável o empenho do legislador em acomodar as normas nacionais em harmonia com aquele dispositivo que, dentro em breve, será parte do nosso leque legislativo.

[12] MALAQUIAS, Roberto António. Crime Cibernético e Prova: a investigação criminal em busca da verdade. 2ed. Curitiba: Juruá. 2015.
[13] IDEM
[14] Moçambique. Lei nº 24/2019, de 24 de Dezembro. Lei de revisão do Código Penal.
[15] Art. 2. Convenção de Budapeste

4.Código do Processo Penal (lei nº 25/2019, de 26 de Dezembro)

O novo Código do Processo Penal, aprovado pela lei nº25/2016 de 26 de Dezembro, contém inovações como o recurso a escutas telefónicas (artigos 222 e 225) como meio de obtenção de prova no cibercrime, em conformidade com o art. 21 da Convenção de Budapeste.

A Convenção contém mais disposições relactivas ao processo penal nos crimes cibernéticos e que permitem uma maior cooperação entre os países, como é caso do art. 16, que prevê a conservação expedicta de dados informáticos armazenados o que permite a interceptação e execução de informações por parte das autoridades nos processos ligados ao cibercrime.

5.Lei das Transacções Electrónicas (lei nº 3/2017, de 9 de Janeiro)

Aprovada pela lei 3/2017, tem como objectivo regular as transacções electrónicas no geral e garantir a segurança dos provedores e utilizadores das tecnologias de informação e comunicação e aplica-se a todas as pessoas (singulares e colectivas) e entidades que apliquem as TIC's nas suas actividades.

A entidade reguladora no âmbito da Lei das Transações Electrónicas é o Instituto Nacional de Tecnologias da Informação e Comunicação (INTIC) e este é responsável por regular, supervisionar e fiscalizar o sector das TIC's no nosso país.

A lei visa garantir que as transacções electrónicas se processem de forma célere e com maior segurança jurídica, permitindo assim que o cidadão esteja mais confiante no uso das plataformas de transacção electrónica. A lei permite, por exemplo, que, no âmbito das suas negociações, o cidadão possa realizar assinaturas electrónicas[16]. O reconhecimento da validade legal das assinaturas electrónicas ajuda na gestão do tempo, elimina a necessidade de se levar documentos físicos de um lugar para o outro e facilita a realização de negócios à distância.

[16] Cfr. Artigo 22, Lei das Transacções Electrónicas.

As suas disposições conferem previsão legal à protecção de dados pessoais, porém, com isso não se dispensa a necessidade de uma lei específica que se dedique inteiramente à matéria de cibercriminalidade como um todo e não de forma sectorial.

A Lei de Transações Electrónicas desempenha um papel importante na persecução penal dos cibercrimes, na medida em que ela confere forca probatória as mensagens de dados, conforme estabelece o artigo 24 da mesma "as mensagens de dados fazem prova em juízo (...)"[17] e ainda "toda a informação apresentada sob forma de mensagem electrónica goza de forca probatória."[18]

No âmbito desta lei, serão dados pessoais qualquer informação relativa a uma pessoa singular que possa ser identificada directa ou através da referência a um número de identificação ou a um ou mais factores específicos à mesma. Nesse contexto, esses dados têm proteção legal devidamente prevista na CRM que, proíbe o acesso a arquivos, ficheiros e registos informáticos ou de bancos de dados para conhecimento de dados pessoais relativos a terceiros.[19] Porém, segundo Mara Lopes "a Lei das Transacções Electrónicas apresenta diversos conceitos indeterminados que não permitem materializar, com certeza, o alcance das obrigações dos processadores de dados e dos controladores de dados – sendo que quanto a estes últimos nem sequer define quem são. Até que seja regulamentada, a Lei não oferece, por si só, garantias concretas que se traduzam em maior segurança aos dados pessoais electrónicos."[20] Explica ainda que esta lei de transacções electrónicas aprova um regime especial, sendo que não temos um regime geral de protecção de dados sobre o qual este regime assenta, este facto aliado à falta de regulamentação específica tornam extremamente difíceis a aplicabilidade e eficácia desta lei.

[17] Cfr. nº 1, artigo 24, Lei das Transações Electrónicas.
[18] Cfr. nº 2, artigo 24, Lei das Transações Electrónicas.
[19] Cfr. nº 3, artigo 71, Constituição da República de Moçambique.
[20] https://www.mdradvogados.com/pt/conteudo/publicacoes/ja-temos-lei-das-transaccoes-electronicas-e-agora/149/

6.Estratégia Nacional de Segurança Cibernética de Moçambique

No âmbito do combate ao cibercrime, o Governo lançou a Estratégia Nacional de Segurança Cibernética, um conjunto de políticas e procedimentos que visam a protecção dos sistemas contra as ameaças. Nesta estratégia, o Governo tem como finalidade a promoção de um espaço cibernético seguro e resiliente.

A política de segurança cibernética estabelece, em seis pilares, princípios e objetivos que orientam para uma segurança cibernética duradoura.

Os princípios e objetivos que estruturam a Política de Segurança Cibernética são:

1. Liderança e coordenação;
2. Protecção de infra-estruturas críticas de informação;
3. Protecção de activos de informação;
4. Legal e regulatório;
5. Desenvolvimento da capacidade de pesquisa e inovação;
6. Cultura de segurança cibernética, treinamento e conscientização.

Dos diversos projectos de segurança cibernética traçados alguns já foram materializados, como é o caso da operacionalização de equipas de resposta a incidentes de segurança cibernética, porém ainda existem alguns objetivos por alcançar desde a revisão do quadro legal ao estabelecimento de sistemas de alerta sobre incidentes cibernéticos.

Portanto, a Estratégia Nacional de Segurança Cibernética é potencialmente eficaz e essencial para a protecção da sociedade e do Governo contra as crescentes ameaças no ambiente digital.

7.Lei de Cooperação Internacional (lei nº 21/2019, de 11 de Novembro)

A lei de cooperação internacional, aprovada pela lei nº 21/2019, de 11 de Novembro, veio estabelecer proncípios e procedimentos da cooperação jurídica internacional da República de Moçambique com outros Estados, assim como com entidades internacionais estabelecidas no âmbito dos tratados e acordos internacionais que vinculem o Estado Moçambicano, em matéria penal.[21]

A cooperação internacional é um aspecto muito importante no combate ao cibercrime pois este atravessa fronteiras terrestres. Os cibercriminosos operam a nível global e a colaboração mútua entre os países é um meio para se potencializar a eficácia do combate ao cibercrime, através da facilidade de extradição de criminosos cibernéticos e da troca de informações. Considerando que as investigações de cibercrime envolvem actividades que geralmente ocorrem em países diferentes, a cooperação facilita o trabalho conjunto entre agências de aplicação da lei dos diferentes países, permitindo a recolha de provas, a extradição dos criminosos e a coordenação dos esforços para prende-los.

A lei em questão prevê como formas de cooperação internacional:

- A extradição, respeitando os limites estipulados no regime jurídico;
- A transmissão de processos penais, onde pode ser instaurado ou continuar no Estado Moçambicano procedimento penal por facto practicado fora do território moçambica a pedido de um Estado estrangeiro;
- A execução de sentenças penais, onde se pode executar as sentanças penais estrangeiras transitadas em julgado nas condições previstas na lei. Também é possível a execução no estrangeiro de sentenças penais moçambicanas, desde que estejam verificadas as condições previstas no art. 94 da lei de cooperação internacional;
- A transferência de pessoas condenadas a penas e medidas privativas de liberdade, a transferência é feita mediante consentimento ou pedido da pessoa condenada;
- A vigilância de pessoas condenadas ou em liberdade condicional, o pedido de vigilância é feito com o objectivo de favorecer a reinserção social do condenado através da adopção de medidas adequadas e para vigiar o seu comportamento com vista a evenctual aplicação de uma reacção criminal ou à sua execução;

[21] Cfr. Art. 1 da Lei de Cooperação Internacional

- O auxílio judiciário mútuo em matéria penal, é feito através da comunicação de actos processuais e outros actos públicos que admitidos pelo Direito moçambicano, quando se demonstrem necessários à realização das finalidades do processo, bem como os actos necessários à apreensão ou recuperação de intrumentos, objectos ou productos da infração.

A Procuradoria Geral da República (PGR) é o órgão central competente para tramitar os pedidos de cooperação de qualquer natureza, para tramitar as medidas compulsatórias, as cartas rogatórias e também para solicitar ao Tribunal Supremo a revisão e reconhecimento das sentenças estrangeiras.[22]

A cooperação internacional é eficaz no combate ao cibercrime porque permite esta troca entre os países, tornando possível uma abordagem mais coordenada para enfrentar as ameaças cibernéticas.

[22] Cfr. nº1, Artigo 5, Lei de Cooperação Internacional.

IV.EFICÁCIA DAS NORMAS DE COMBATE AO CIBERCRIME

As normas de combate ao cibercrime desempenham um papel crucial na protecção digital contra as ameaças cibernéticas. A eficácia da norma é capacidade que ela tem de produzir os efeitos práticos esperados na realidade. A eficácia das normas de combate ao cibercrime depende da implementação, colaboração internacional e adaptação constante às evoluções tecnológicas. Como sabemos, a área digital verifica um crescimento exponencial diário e da mesma forma os crimes nesse ambiente têm a mesma evolução.

Sobre a eficácia da norma penal, o professor Eduardo Correia dispõe que, a aplicação da sanção penal ou a sua ameaça são simplesmente um modo de prevenir as violações futuras (teoria utilitárias) e isto quer na medida em que a ameaça ou execução desse agem sobre a generalidade das pessoas, intimidando-as e desviando-as da prática do crime (prevenção geral), quer na medida em que actuam sobre o agente num sentido segregador, afastando-o ou eliminando-o da sociedade- reeducativo ou correctivo, adaptando-o à vida social- ou intimidativo- dando-lhe consciência da seriedade da ameaça penal (prevenção especial)[23].

Sobre a eficácia da norma penal, o autor dispõe ainda que ″a tranquilidade pública só deverá considerar-se convenientemente reestabelecida quando a pena for um justo castigo, um adequado meio de intimidação e um conveniente processo de regeneração moral do denlinquente.″[24]

No entanto, no caso do cibercrime, as normas por si só não são o único meio de combate ao cibercrime. Este requer uma abordagem mais abrangente, que combine uma estrutura legal sólida, tecnologias mais avançadas, educação contínua e cooperação internacional (esta facilita a extradição de criminosos e a troca de informações entre países).

As normas precisam de estar padronizadas e implementadas de forma adequada, promovendo a consistência nas práticas de segurança cibernética. A inclusão de directrizes para respostas a incidentes é uma forma perfeita de fazer com que estas sejam mais eficazes, através da pronta resposta aos incidentes cibernéticos, minimizando danos.

As ameaças cibernéticas estão sempre em evolução, e isso requer que as normas também acompanhem essa evolução para que elas possam alcançar os objetivos pretendidos. Elas devem evoluir para que sejam capazes de enfrentar as novas ameaças que surgem. Atualmente, temos assistido ao crescimento das IA's. Elas vieram revolucionar ainda mais o

[23] CORREIA, Eduardo. Direito Criminal. P. 41
[24] CORREIA, Eduardo. Direito Criminal. P. 69

mundo digital, alguns acreditam que elas, em dado momento, tomam o lugar do ser humano até em actividades profissionais, gerando assim o desemprego. No mundo jurídico, existem IA's, sendo usadas para auxiliar advogados em tarefas como busca de informações em bancos de dados e até mesmo na previsão de resultados de casos. Isto serve para demonstrar o quanto o mundo virtual evolui e o quanto estamos cada vez menos preparados para responder às novas situações que surgem diariamente.

Normas específicas e claras e que estabeleçam penas e sanções significativas podem sim dissuadir os criminosos cibernéticos e causar impacto positivo na prevenção do cibercrime, mas este trabalho terá um resultado mais satisfatório com a combinação dos diferentes esforços, a colaboração do sector público e privado, as regulamentações específicas, a cooperação internacional bem como a educação e conscientização da sociedade no geral.

De acordo com David Wall, políticas e acordos internacionais são mais eficazes no combate ao cibercrime, dada a natureza transnacional destes crimes. O contacto e assistência entre os países é fundamental para o fornecimento de dados, para que seja possível seguir as pistas do crime antes que elas desapareçam. A harmonização das leis entre os países é também crucial, pois desencoraja os criminosos, visto que independentemente do país que eles cometam o crime ou sobre o qual recai a acção, a lei é a mesma, assim como a sentença.

Conclusão

O cibercrime é um desafio para os sistemas jurídicos do mundo todo, à medida que com a evolução das tecnologias, os criminosos também tendem a tornar-se mais especializados nos seus actos. A situação jurídica do cibercrime reflecte uma interação entre leis nacionais e internacionais, convenções, regulamentos, estratégias e desafios práticos da aplicação da lei.

O mundo contemporâneo está cada vez mais imerso nas tecnologias, nelas assentam-se diversas actividades no âmbito empresarial, pessoal e até ao nível do Governo e sem percebermos o cibercrime está cada vez mais presente no nosso quotidiano.

Este estudo é orientado para a procura de respostas legais que permitam melhorar a actuação das autoridades, focando a sua atenção sobre as limitações do actual quadro jurídico do cibercrime e propondo alternativas.

O actual cenário legislativo do cibercrime é composto por dispositivos que preveem e punem infracções criminais cometidas por via das redes de conexão, porém, esse cenário precisa de ser melhorado, através da criação de legislação específica para crimes cibernéticos. É necessária a elaboração de um código legal sobre segurança cibernética, este determinará o regime geral de segurança cibernética e irá complementar o regime específico disposto nas diversas leis avulsas existentes.

O governo está ciente das ameaças e efeitos do cibercrime e por isso tem maximizado os seus esforços para garantir que hajam instrumentos que possam proteger o cidadão e penalizar os que cometem estes crimes. O novo Código Penal e o Código do Processo Penal, a Lei de Transações Electrónicas e a Lei das Telecomunicações são exemplos dos esforços do Governo no combate ao cibercrime. Como foi mencionado, as normas por si só não serão suficientes para colmatar os crescentes casos de cibercrime, este fenómeno exige uma abordagem holística, combinando esforços entre o Estado e o sector privado, promovendo a cooperação internacional, o uso de tecnologias avançadas e treinamento dos profissionais, para lidar com o cibercrime, actualizando continuamente as normas por forma a abordar as mudanças constantes nas ameças e ainda a conscientização das pessoas e organizações por forma a entender e se protegerem contra as ameaças.

O reforço do quadro legal para a prevenção e combate ao cibercrime será possível através da ratificação das convenções internacionais, a Convenção do Conselho da Europa, especificamente, a divulgação do quadro legal sobre segurança cibernética e harmonização da nossa legislação com a de outros países.

A natureza transnacional do cibercrime é um desafio para a eficácia do combate, pois exige a cooperação internacional e traz à superfície a questão da jurisdição extraterritorial. É igualmente importante compreender as ameaças e desenvolver estratégias eficazes para enfrentá-las e, desse modo, proteger os dados e segurança no nosso ciberespaço.

Em suma, a situação jurídica do cibercrime em Moçambique é satisfatória mas existe espaço para melhorias.

Há necessidade de melhorar a eficácia das leis, através da sua actualização contínua, acompanhando as mudanças das ameaças do sector tecnológico, a melhoria da cooperação internacional, com a ratificação de dispositivos que vão permitir uma maior troca com os restantes países e, por último, é extremamente importante e necessário o investimento nas capacidades de investigação das autoridades de aplicação da lei.

Referências Bibliográficas

Manuais

- ALBURQUERQUE, Roberto Chacon de, *A Criminalidade Informática*, São Paulo, Editora Juarez de Oliveira, 2006.
- BEZERRA, Clara Augusta, *A Ineficácia da Prestação Jurisdicional no combate aos crimes virtuais: a dificuldade da persecução penal*, Goiânia, 2020.
- CORREA, Gustavo Testa, *Aspectos Jurídicos da Internet*, São Paulo, 2000.
- CORREIA, Eduardo, *Direito Criminal*, Coimbra, 1993.
- FERREIRA, Ivette Senise, *A Criminalidade Informática. Direito e Internet: Aspectos Jurídicos Relevantes*, Bauru, ed. Edipro, 2000.
- FIORILLO, Celso António; CONTE, Christian, *Crimes no Meio Ambiente Digital*, 2ª ed., São Paulo, 2012.
- JESUS, Damásio de; MILAGRE, José António, *Manual de Crimes Informáticos*, São Paulo, Saraiva, 2016.
- MACIE, Albano, *Direito Penal I (Textos de Apoio)*, Maputo, 2018.
- MALAQUIAS, Roberto António, *Crime Cibernético e Prova: a investigação criminal em busca da verdade*, 2ª ed., Curitiba: Juruá, 2015.
- PIZZARO, Teresa Beleza, *Direito Penal*, Lisboa.
- ROSSINI, Augusto Eduardo de Souza, *Informática, Telemática e Direito Penal*, São Paulo, Memória Jurídica, 2004.
- WENDT, Emerson; JORGE, Higor Nogueira, *Crimes Cibernéticos: ameaças e procedimentos de investigação*, Rio de Janeiro, Brasport Livros e Multimídia, 2012.

Consultas na Internet

- https://www.infopedia-pt/dicionários/língua-portuguesa/ciberespaço
- https://www.dw.com/pt-002/ataque-de-hackers-deixa-inoperacionais-portais-mo%C3A7ambicanos/a60854704
- https://opais.co.mz/pgr-quer-reforço-de-leis-combate-a-crimes-cibernéticos
- https://www.mdradvogados.com/pt/conteudo/publicacoes/Ja-temos-Lei-das-Transaccoes-Electronicas-E-agora/149/

Legislação

- Constituição da República de Moçambique (2004), publicada no BR, Série nº 51, quarta-feira, 22 de Dezembro, actualizada pela Lei nº 1/2018, de 12 de Junho, I série, Número 115 – Lei da Revisão Pontual da Constituição da República de Moçambique.
- Lei nº 24/2019, de 24 de Dezembro – Código Penal
- Lei nº 25/2019, de 25 de Dezembro – Código do Processo Penal
- Lei nº 3/2017, de 19 de Janeiro – Lei das Transações Electrónicas
- Lei nº 21/2019, de 11 de Novembro – Lei de Cooperação Internacional
- Lei nº 4/2016, de 3 de Janeiro - Lei das Telecomunicações
- Resolução nº 5/2019, de 20 de Junho – ratifica a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais.