UNIVERSIDADE CATÓLICA DE MOÇAMBIQUE
FACULDADE DE DIREITO

GABRIEL DESEJADO GABRIEL MEPINA

REPERCUSSÃO DOS CRIMES CIBERNÉTICOS NO DIREITO PENAL MOÇAMBICANO

NAMPULA

2025

UNIVERSIDADE CATÓLICA DE MOÇAMBIQUE
FACULDADE DE DIREITO

GABRIEL DESEJADO GABRIEL MEPINA

REPERCUSSÃO DOS CRIMES CIBERNÉTICOS NO DIREITO PENAL MOÇAMBICANO

Tese a ser apresentada ao Departamento de Doutoramento, na Faculdade de Direito da Universidade Católica de Moçambique, como condição para adquirir o grau de Doutor em Direito Público.

Orientador: Prof. Doutor Barbosa MORAIS

NAMPULA

2025

DECLARAÇÃO ANTI-PLÁGIO

Eu, Gabriel Desejado Gabriel Mepina, declaro, por minha honra, que o texto apresentado é da minha exclusiva autoria e que toda a utilização de contribuições ou textos alheios está devidamente referenciada.

O declarante

_____

(Gabriel Desejado Gabriel Mepina)

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, pelo dom da vida! E forma especial, ao meu supervisor, Prof. Doutor Barbosa Alberto Morais, pelos subsídios no processo da concepção do trabalho, desde o projecto até a realização da pesquisa que culminou com a presente tese.

DEDICATÓRIA

Às minhas filhas:

- Alana Érica Salvador Mepina;
- Ciane Gabriela Salvador Mepina.

Esposa:

- Zainabo José Salvador.

Aos meus Pais:

- Gabriel Mepina;
- Maria Catarina Mirasse.

E a todos os meus sobrinhos, de forma especial – a Fáusia José Nticama, para que sirva de exemplo.

LISTAS DE ABREVIATURAS/SIGLAS/SÍMBOLOS

Abr.	Abreviaturas
Apud	"citado por.."
Art.	artigo
Arts.	Artigos
At.al	"e outros'
B. O.	Boletim Oficial
B. R.	Boletim da República
Cap.	Capítulo
CC	Código Civil
CPC	Código de Processo Civil
CP	Código Penal
CPP	Código de Processo Penal
CRM	Constituição da República de Moçambique
CRM/2004	Constituição da República de Moçambique de 2004
CRM/90	Constituição da República de Moçambique de 1990
CRPM/1975	Constituição da República popular de Moçambique de 1975
Dec.	Decreto
Eds.	Editores
FRELIMO	Frente de Libertação de Moçambique
P.	Página
PENSEC	Política e Estratégia Nacional de Segurança Cibernética
PP	Páginas
RENAMO	A Resistência Nacional Moçambique
S/D-	Sem data
Sec.	Século
Ss	Seguintes
Sup.	Suplemento
UCM	Universidade Católica de Moçambique
Vol.	Volume

RESUMO

A presente tese tem como tema: “Repercussão dos Crimes Cibernéticos no Direito Penal Moçambicano”. A ideia assenta na predisposição que a rápida evolução das novas tecnologias de informação e comunicação possibilitou a existência de “vazios legais” e à difícil definição do crime informático, num contexto em que o país tem sido alvo de ataques constantes dos criminosos virtuais, dificultando a descoberta do autor e do local da prática do delito. É nesta perspectiva que procuramos trazer um entendimento em relação a posição do legislador moçambicano no âmbito da legislação do quadro existente (CP, CPP e Legislação complementar), bem como as regulamentações que podem ser aplicadas nos crimes cibernéticos, visto que apesar da existência de instrumentos legais, nos últimos anos, os crimes cibernéticos têm crescido a cada dia e os criminosos têm vindo a sofisticar a sua forma de actuação no nosso ciberespaço. A título elucidativo, em 2022 foi registado um ataque cibernético, que afectou o funcionamento normal do Serviço Nacional de Migração, Instituto Nacional de Gestão e Redução de Riscos e Desastres, Direcção Nacional de Identificação Civil e Administração Nacional de Estradas. Diante destes acontecimentos, o país mostra-se ainda não estar preparado para assegurar a segurança jurídica necessária para o ciberespaço moçambicano dos ataques dos criminosos virtuais. Assim sendo, surge a seguinte indagação: Qual é a posição que o legislador penal figura os crimes cibernéticos no ordenamento jurídico moçambicano? A pesquisa teve como objectivo analisar a repercussão dos crimes cibernéticos no Direito Penal moçambicano. O estudo mostra-se oportuno, uma vez que o legislador penal pode fazer um exame minucioso para verificar o nível deficitário da legislação em relação a estes delitos. Outrossim, o resultado do estudo irá ajudar ao sistema da administração da justiça moçambicana a adoptar medidas legislativas eficazes, bem como políticas e estratégias consistentes para fazer face aos delitos virtuais. Quanto aos procedimentos metodológicos, trata-se de uma pesquisa básica, de cariz qualitativa, bibliográfica e documental. O método aplicado para a construção deste saber científico foi jurídico, que se consubstancia na técnica hermenêutica jurídica. As técnicas de análise de conteúdo e de triangulação foram aplicadas no processo de discussão dos resultados. Com este estudo, constatamos a existência de fragilidades no ciberespaço moçambicano, o que põe em causa a segurança cibernética. Contudo, é imperioso que o legislador pátrio considere a criação de um direito penal informático, como uma disciplina jurídico-penal autónoma.

Palavras – chave: Direito Penal, Crimes cibernéticos, Segurança cibernética.

ABSTRACT

The present thesis addresses the theme: "Impact of Cybercrimes on Mozambican Criminal Law." The idea is based on the predisposition that the rapid evolution of new information and communication technologies has led to the existence of "legal gaps" and the challenging definition of cybercrime, in a context where the country has been a constant target of virtual criminals, hindering the discovery of the perpetrator and the location of the crime. In this perspective, we seek to provide an understanding of the position of the Mozambican legislator within the existing legal framework (Criminal Code, Criminal Procedure Code, and complementary legislation), as well as the regulations that can be applied to cybercrimes. Despite the existence of legal instruments, cybercrimes have been growing every day in recent years, and criminals have been sophisticating their methods in our cyberspace. Illustratively, in 2022, a cyberattack was registered, affecting the normal functioning of the National Migration Service, National Institute for Disaster Management and Reduction, National Directorate of Civil Identification, and National Roads Administration. Faced with these events, the country appears to be unprepared to ensure the necessary legal security for the Mozambican cyberspace against virtual criminals' attacks. Therefore, the following question arises: What position does the penal legislator take regarding cybercrimes in the Mozambican legal system? The objective is to analyze the impact of cybercrimes on Mozambican criminal law. The study is timely, as the penal legislator can conduct a thorough examination to assess the deficient level of legislation concerning these offenses. Furthermore, the study's results will help the Mozambican justice administration system adopt effective legislative measures, as well as consistent policies and strategies to address virtual crimes. Regarding the methodological procedures, it is a basic, qualitative, bibliographic, and documentary research. The method applied for constructing this scientific knowledge is legal, embodied in legal hermeneutics. Content analysis and triangulation techniques were applied in the results' discussion process. With this study, we observe vulnerabilities in the Mozambican cyberspace, jeopardizing cybersecurity. However, it is imperative for the national legislator to consider the creation of cybercriminal law as an autonomous legal discipline.

Keywords: Criminal Law, Cybercrimes, Cybersecurity.

Índice

INTRODUÇÃO

Delimitação do Tema

A presente tese tem como tema: Repercussão dos Crimes Cibernéticos no Direito Penal Moçambicano. Uma abordagem que pertence ao campo de Direito Penal, pelo facto de ordenar a boa convivência em sociedade e trazer, em suas linhas normativas, conduta criminosa proibida à pessoa. Outrossim, a nossa abordagem assenta-se no âmbito do Direito Digital, pelo facto de existir, no nosso ordenamento jurídico, alguma normalização e regulamentação do uso dos ambientes digitais, além de oferecer protecção de informações contidas nesses espaços e em aparelhos electrónicos. Nesta abordagem, analisamos as implicações do uso da tecnologia, em particular - a internet e os meios digitais.

Contextualização do Problema

Tal como referimo-nos na delimitação do tema, o objecto do nosso estudo assenta na Repercussão dos Crimes Cibernéticos no Direito Penal do nosso país. A ideia é saber como o legislador penal trata dos delitos digitais na ordem jurídica penal, pelo facto de se verificar que com o aparecimento das novas tecnologias de informação e comunicação surgiram também alguns problemas legais associados. A rápida evolução destas novas tecnologias levou à existência de "vazios legais e à difícil definição do crime informático. A década passada ficou marcada pela revolução no âmbito das telecomunicações e pelo surgimento de um ciberespaço global frequentado por milhares de pessoas do mundo. Neste contexto, tornam-se necessárias análises e reflexões sobre as potencialidades das novas tecnologias ao nosso dispor, quanto a implicação do seu uso no campo de Direito, o que, como consequência da sua utilidade, nos pode pôr em risco.

Moçambique é um Estado de Direito Democrático baseado no respeito e garantia dos direitos e liberdades fundamentais do Homem, conforme estatuído no art. 3 da Lei Fundamental. Assim sendo, cabe-lhe acompanhar todas as mudanças decorrentes da evolução tecnológica pela qual a sociedade passa, buscando adaptar-se às transformações, a fim de promover novas soluções para as novas peculiaridades trazidas pela prática dos crimes virtuais, uma vez que estes são cada vez mais frequentes, sofisticados e mais difíceis de combater. Outrossim, os crimes cibernéticos são uma espécie de crime originária da evolução tecnológica, através da qual a sociedade contemporânea passa. São crimes caracterizados por uma complexidade no processo investigativo, cuja autoria é de difícil identificação.

É evidente que os avanços tecnológicos e as novas descobertas científicas trouxeram novos comportamentos delituosos e os estados enfrentam uma "criminosa máscara", de difícil descoberta no local da prática do delito de natureza cibernética. Neste contexto, procuramos trazer um entendimento em relação a posição do legislador moçambicano no âmbito do quadro legislativo, bem como as regulamentações que podem ser aplicadas aos crimes cibernéticos. É importante adiantar que se não haver tipificação penal sobre crimes cibernéticos, não será cominado como crime, em respeito ao princípio constitucional[1], cuja materialização assenta na Lei Penal (Princípio da Legalidade do Direito Penal[2]. Nesse corolário, temos a legislação seguinte no ciberespaço moçambicano: **Constituição da República de Moçambique** (CRM, 2004) – *lex fundamantallis* que proíbe o acesso à arquivos, ficheiros e registos informáticos ou de banco de dados para o conhecimento de dados pessoais relativos a terceiros nem a transferência de dados pessoais, salvo nos casos estabelecidos na Lei ou por decisão judicial (nº 3 do art. 71 da CRM). Como legislação extravagante, na mesma senda, encontramos na esfera virtual moçambicana o Código Penal (Lei n.º 24/2019, de 24 de Dezembro). O Código Penal configura-se, no âmbito das suas normas, nas Disposições Gerais, que contemplam o Princípio da Territorialidade (artigo 4º) e Factos praticados fora do território nacional (artigo 5º), consentâneos com o artigo 22, da Convenção de Budapeste. No mesmo contexto, o Código Penal vigente prevê infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos. Inclui, igualmente, infracções relacionadas a conteúdos como pornografia de menores. Ainda dentro do Código Penal, são estabelecidas as Formas de Responsabilidade e Sanções das pessoas colectivas em conformidade com os artigos 11 e 12, da Convenção de Budapeste. Dentro do quadro legal pertinente temos o Código do Processo Penal (Lei n.º 25/2019, de 26 de Dezembro), prevendo Princípios Fundamentais e Garantias do Processo Penal, designadamente: Direito fundamental à presunção de inocência (art. 3); Proibição de provas obtidas por meios ilícitos (art. 4); Princípio do contraditório (art. 5); Direitos da pessoa detida (artigo 6); Direito a defensor (art. 7) e Dever de fundamentação (art. 8).

Apesar da existência de instrumentos legais (apontados no parágrafo anterior), nos últimos anos, os crimes cibernéticos têm vindo a crescer em Moçambique, dia-após-dia. Os criminosos têm vindo a sofisticar, cada vez mais, a sua forma de actuação. Esse aumento

[1] Cfr., art. 60 da ***CRM (Aplicação da Lei Penal):*** "Ninguém pode ser condenado por acto no qualificado como crime no momento da sua prática (nº 1)."

[22] Cfr., art. 1 do CP: "Num facto que consista em acção ou omissão, pode se julgar crime sem que uma lei, no momento da sua prática, o qualifique como tal (nº1). Não podem ser aplicadas medidas ou penas criminais que não estejam previstas na lei (nº 2)."

gradual dos crimes cibernéticos tem vindo a preocupar os órgãos da Administração da Justiça, facto que exige novas estratégias, com vista a mitigação desta realidade. A título ilustrativo, em 2018 foram tramitados 357 processos[3] relacionados com crimes cibernéticos e, em 2019 os números subiram para 509 processos, um aumento em 152 processos, o correspondente a 42,68%. De igual modo, em 2020 foram tramitados 692 processos, o que representa um aumento em 133 processos, o correspondente a 36%[4]. Em "2021 foram registados 393 processos, contra 692, de igual período anterior (2020), o que significa um decréscimo de 299, correspondente a 43,2%"[5]. Ainda em conformidade com o informe do Ministério Público, "as Procuradorias Provinciais da República - em Gaza, Maputo e Tete, foram as que registaram maior número, com 64, 44 e 43, respectivamente. As Procuradorias Provinciais da República - em Cabo Delgado, Manica e Sofala, com 13, 20 e 26, são as que registaram menor número de processos. Os tipos legais de crime mais registados foram fraudes relativas aos instrumentos e canais de pagamento electrónico, com 214 e burla informática nas comunicações, com 70 processos" [6].

Ainda na mesma senda, "em 2022, foi registado um ataque cibernético, que afectou o funcionamento normal de várias instituições do Estado (Serviço Nacional de Migração, Instituto Nacional de Gestão e Redução de Riscos e Desastres, Direcção Nacional de Identificação Civil e Administração Nacional de Estradas), cujo processo encontra-se em instrução preparatória." A tendência da ocorrência de crimes informáticos manteve-se crescente, tendo sido registados 560 processos, contra 393 (em 2021)[7]. "Foram concluídos 456, tendo recaído despacho de acusação em 267 e 189 arquivados. A Cidade de Maputo, com 81, e as Províncias de Manica e Gaza, com 74 e 67 processos, respectivamente, foram as que apresentaram maior registo. Continuam frequentes os crimes de fraudes relativos aos instrumentos e canais de pagamento electrónico, com 251, seguida da burla informática e nas comunicações, com 139, e furto de fluídos, com 74"[8].

Nessa alusão, o País ainda não está preparado para assegurar a protecção jurídica necessária para a sociedade mediante os ataques dos criminosos no âmbito virtual. Nota-se a insuficiência ou a ausência de norma penal tipificando, de forma precisa, os crimes digitais,

[3] MOÇAMBIQUE, República de. Procuradoria-Geral da República. ***Informação Anual de 2019 do Procurador-Geral da República à Assembleia da Repdblica***, Maputo, 2019.
[4]Idem, 2020.
[5] Idem, 2022. p. 53.
[6] Ibidem, 2022. pp.53-54.
[7] Idem, 2023. p.35.
[8] Ibidem, 2023. p.35.

facto que limita a função punitiva estatal, uma vez que influencia na sensação de insegurança e impunidade, com repercussão negativa para a sociedade e, em especial, para a comunidade internacional, que há mais de uma década vem chamando a atenção para a necessidade e urgência de controlo e prevenção de condutas delituosas no ciberespaço: 1. A legislação moçambicana ainda não contempla disposições específicas da prova digital no âmbito dos meios de obtenção de prova, como por exemplo, a conservação expedita de dados informáticos, pesquisa de dados informáticos, apreensão de dados informáticos e injunção para apresentação ou concessão do acesso a dados, o que tem dificultado as investigações; 2. Moçambique ainda não ratificou a Convenção de Budapeste, que facilitaria a cooperação internacional e a recolha de obtenção de prova digital; 3. Falta de equipamento tecnológico adequado para os profissionais de justiça criminal, bem como a falta de pessoal qualificado em matéria de criminalidade informática.

Desse modo, a legislação moçambicana tem dificuldades em acompanhar a evolução tecnológica, pois a cada dia surge um novo delito nesse ambiente, do qual o legislador não é capaz de caminhar em paralelo com essas evoluções, daí que, consequentemente, os crimes virtuais não recebem as devidas punições, deixando a sensação de impunidade. Assim sendo, aferimos que o crime digital não possui a devida atenção, sendo tipificado por apenas algumas leis que, no nosso entender, não são específicas para o devido tema, visto que os crimes figurados na legislação penal são comuns e, especificamente, o crime digital, apenas é qualificado como informático ou cibernético. Esta designação deve-se ao meio que o infractor usa para a prática desses crimes no ciberespaço moçambicano. É nesta perspectiva que, no presente estudo, indagamos: ***até que ponto o quadro jurídico-penal moçambicano tutela, cabalmente, os crimes cibernéticos?***

Hipóteses

Para responder à pergunta de partida foram avançadas as seguintes hipóteses: (a) Moçambique tutela cabalmente os crimes cibernéticos, pois ratificou todas convenções internacionais sobre o cibercrime e tipificou totalmente toda a espécie dos cibercrimes, incluindo os mecanismos processuais para a sua investigação. (b) Moçambique ainda não tutelou cabalmente os crimes cibernéticos, pois ainda não ratificou todas convenções internacionais sobre o cibercrime e tipificou parcialmente os cibercrimes e os respectivos mecanismos de investigação.

Objectivos do Estudo

Objectivo Geral

A nossa abordagem apresenta como objectivo geral, analisar a repercussão dos crimes cibernéticos no direito penal moçambicano.

Objectivos Específicos

São decorrentes os seguintes objectivos específicos:

a) Compreender o decurso histórico do Direito Penal moçambicano, desde o tempo colonial, pós-colonial até pós-independência;
b) Verificar a repercussão dos tipos criminais no Direito Penal Moçambicano;
c) Aferir a essência dos crimes cibernéticos/informáticos nas correntes doutrinais, sem descurar a sua tipologia quadro;
d) Fazer uma comparação das formas de Implementação das Políticas para o combate e prevenção dos crimes cibernéticos nas Ordens Jurídicas Moçambicana, Brasileira, Espanhola e Portuguesa;
e) Discutir as implicações dos crimes cibernéticos no Direito Penal Moçambicano.

Justificativa

A análise da presente abordagem parte do princípio de que o Direito sempre foi visto como a norma jurídica elaborada pelos órgãos dos Estados. Porém, o objectivo do Direito Penal é a tutela subsidiária (*de "ultima ratio")* de bens jurídicos com dignidade penal, sublinhando que a realidade do crime não depende somente do conceito material, mas também da construção social, da reacção social, quer pelas instâncias formais (legislador, polícia, Ministério Público, Juiz), quer pelas instâncias informais (família, escolas, igrejas, clubes, vizinhos) de controlo.

A criminologia tem despertado interesse pela realidade jurídica, estendendo o seu objecto de estudo a outras formas de regulamentação de comportamento social que vinculam as pessoas, facto que dá pertinência a análise da presente abordagem (Repercussão dos Crimes Cibernéticos no Direito Penal no Contexto Moçambicano), de forma a verificar a atitude do legislador constituinte, no que tange a realidade moçambicana, no âmbito dos delitos virtuais.

É nessa perspectiva que, no presente estudo, demonstramos que a evolução tecnológica traz desvantagens para a sociedade, relativamente ao surgimento de novos delitos, muito complexos pela sua actuação. Esse aspecto motivou-nos a escolha do tema, objecto do presente estudo, que se prende com a necessidade de os crimes cibernéticos puderem ser compreendidos como um novo mal social. E, para tal, é necessário que o legislador penal, partindo do estudo, estabeleça uma estratégia para manter a segurança no espaço cibernético moçambicano.

O tema - "Repercussão dos Crimes Cibernéticos no Direito Penal" - é actual, razão pela qual levou-nos a sua escolha para a presente abordagem, visto que a internet é um dos avanços mais importantes que a humanidade tem vivido nos dias de hoje. Graças a esse avanço é possível realizar as mais diversas actividades por meio da *World Wide Web*, além das barreiras temporais e espaciais terem sido relativizadas. Contrariamente a isso, todas as faculdades oferecidas pela tecnologia da informação também trazem sérios riscos para as pessoas. A capacidade de ocultar a sua identidade na internet está atraindo uma nova geração de criminosos difíceis de os descobrir. Nesse âmbito, é necessário (interesse da abordagem), que o Estado, por via do presente estudo, actue no sentido de configurar o sistema judiciário contra a prática de crimes cibernéticos, em desenvolvimento tecnológico.

A abordagem do tema é justificável na medida em que pretendemos verificar se o Direito Penal Moçambicano está totalmente adoptado às realidades da sociedade moderna, no que tange aos crimes virtuais. Esta é uma oportunidade para o legislador penal fazer um exame minucioso para verificar o nível deficitário da legislação em relação a estes delitos.

A presente abordagem é importante, pois a positivação dos crimes cibernéticos, no contexto ciberespaço moçambicano é imprescindível, tendo em conta os instrumentos legais que possam regular a forma de prevenção e respectivo combate na sociedade, considerando a volatilidade deste tipo de crime. Igualmente, o estudo vai ajudar ao sistema da Administração da Justiça na adopção de medidas legislativas eficazes, bem como de políticas e estratégias consistentes para fazer face aos delitos virtuais.

Ainda no âmbito da Administração da Justiça, o presente estudo revela-se importante na contribuição de estratégias de combate a este novo tipo de delito e definir formas de adopção de atitudes mais proactivas em relação aos cidadãos que merecem ter sua segurança e boa-fé defendidas, visto que a segurança no ciberespaço moçambicano se mostra frágil devido à incidência de crimes cibernéticos.

Estrutura do Trabalho

O presente trabalho está estruturado em 3 (três) partes:

- A primeira parte compõe os elementos pré-textuais, como a capa, contra-capa (página de rosto), declaração anti-plágio, dedicatória, agradecimentos, listas de abreviaturas/siglas/símbolos, resumo, abstract e o índice.
- A segunda parte corresponde aos elementos textuais, que é composta por, para além da introdução, 6 (seis) capítulos, estruturados da seguinte forma:

1) O primeiro trata da metodologia aplicada ao estudo. Neste capítulo, apresentamos os procedimentos metodológicos relativos ao tipo de pesquisa, tendo sido definida como básica - quanto a finalidade; de cariz qualitativa - quanto a abordagem; explicativa - quanto aos objectivos; bibliográfica e documental no que concerne aos procedimentos técnicos. Tendo em conta o objecto do presente estudo, o método aplicado para a construção deste saber científico foi jurídico, para além dos métodos comparativo e hermenêutico, próprios dos estudos de natureza jurídica. Ademais, nos processos de apresentação, análise e interpretação dos dados, aplicamos as técnicas de categorização, ao passo que as técnicas de análise de conteúdo e de triangulação, aplicamos nos processos de discussão dos resultados.

2) No segundo capítulo, temos presente a descrição da Evolução Histórica do Direito Penal Moçambicano, desde o Direito Penal Tradicional ao Direito Penal Digital. A pretensão deste capítulo foi trazer o decurso do direito penal ao longo do tempo, procurando compreender a sua manifestação a partir do tempo colonial à actualidade. Também, essa evolução permitiu-nos tirar ilações sobre a figura dos crimes cibernéticos naquela época no ordenamento jurídico-penal e perceber qual foi o comportamento actuante do legislador penal nas épocas referenciadas no presente estudo.

3) No terceiro capítulo abordamos os crimes cibernéticos do ponto de vista teórico. A pretensão foi trazer, neste capítulo, a teorização geral do crime e a teorização específica dos crimes cibernéticos, sem descurar dos aspectos processuais dos crimes cibernéticos. Aferimos a essência dos crimes cibernéticos nas correntes doutrinais, para posteriormente fazer um enquadramento no nosso contexto jurídico.

4) No quarto capítulo trazemos a abordagem da tutela jurídica dos crimes cibernéticos no Direito Comparado, tendo como objectivo verificar quais as directrizes assumidas nos demais ordenamentos jurídicos na temática relativa a políticas implementadas no combate e prevenção dos crimes cibernéticos; facto que nos leva a crer que este estudo

servirá de base para perceber em que passos se encontra o nosso ordenamento jurídico face aos demais. Nessa senda, começamos por apresentar as políticas implementadas para o combate e prevenção dos crimes cibernéticos no nosso País (Moçambique), seguindo-se com as do Brasil, Espanha e, finalmente, com as de Portugal.

5) No quinto capítulo fazemos abordagem sobre a tutela jurídica dos crimes cibernéticos no Direito moçambicano, com vista a trazer o acolhimento ou tipificação dos crimes cibernéticos no país.

6) No sexto capítulo dedicamo-nos à análise, interpretação e discussão dos resultados. Num primeiro momento fazemos a triangulação teórica e de localização sobre o cibercrime, realçando os aspectos teóricos e comparativos dos crimes cibernéticos. No segundo momento, fazemos a discussão dos resultados sobre a Repercussão dos Crimes Cibernéticos no Direito Penal Moçambicano, tendo em conta a posição de Moçambique em relação as convenções internacionais sobre o cibercrime e a tutela jurídica do cibercrime no Direito moçambicano; para além de espelhar os desafios ou mesmo lacunas legislativas do direito moçambicano em relação a tutela do cibercrime.

Ainda na estrutura do trabalho, apresentamos as considerações finais, que incluem as principais conclusões e as respectivas sugestões.

E, por último, a terceira parte da estrutura da presente tese, constam as principais referências bibliográficas, configurantes dos elementos pós textuais.

PARTE I – COMPONENTE METODOLÓGICA

CAPÍTULO I: PROCEDIMENTOS METODOLÓGICOS DO ESTUDO

O presente capítulo é referente aos procedimentos metodológicos adoptados, isto é, métodos aplicados e técnicas adoptadas para a materialização do presente estudo, cujo tema circunscreve-se a "Repercussão dos Crimes Cibernéticos no Direito Penal Moçambicano".

1.1. Métodos Aplicados

Para o presente estudo, buscamos a definição do Trujillo Ferrari, no que concerne ao método científico, como um traço característico da ciência, constituindo-se em instrumento básico que ordena, inicialmente, o pensamento em sistemas e traça os procedimentos do cientista ao longo do caminho até atingir o objectivo científico preestabelecido.[9]

Concordando com Santa Ramos, é nesse quadrante que a ciência nos ensina a conduzir, de forma eficaz, um determinado processo para alcançar os resultados desejados, tendo como objectivo dar-nos a estratégia a seguir no processo[10]. Constitui a doutrina do método científico e de transformação do mundo. E é também uma reconfiguração sucessiva de procedimentos de investigação que se empregam em uma ciência[11].

De modo a dar maior ênfase ao conceito de método científico, interessa-nos trazer, nesta abordagem, a perspectiva de Prodanov, ao aludir que "Método científico é o conjunto de processos ou operações mentais que devemos empregar na investigação. É a linha de raciocínio adoptada no processo de pesquisa".[12] Outrossim, Marina Marconi ensina-nos que o método é o conjunto das actividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objectivo, conhecimentos válidos e verdadeiros, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista[13].

Partindo das perspectivas conceptuais dos autores, ora referenciados, é do nosso entendimento aludir que o método é um caminho a seguir para alcance dos objectivos de uma pesquisa de investigação científica. E cada método de pesquisa faz-se acompanhar de técnicas,

---

[9] TRUJILLO, Ferrari A, ***Metodologia da ciência***,3ª edição, editora Kennedy, Rio de Janeiro, 1974, p. 43.
[10]RAMOS, Santa Taciana Carrillo; NARANJO, Ernan Santiensteban, ***Metodologia da Investigação Científica, Escolar Editora***, Lisboa, 2014, p.14.
[11]RAMOS, Santa Taciana Carrillo; NARANJO, Ernan Santiensteban, ***Metodologia da Investigação Científica, Escolar Editora***, Lisboa, 20 p.14.
[12] Prodanov, Cleber Cristiano, e Ernani Cesar de Freitas. *Metodologia do Trabalho Cientifico - Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico, 2ª edição.* Rio Grande do Sul: ASPEUR, 2013, p. 126.
[13]MARCONI, Marina Andrade De; LAKATOS, Eva Maria, ***Fundamentos de Metodologia Científica***, 5ª Edição, editora Atlas, São Paulo-Brasil, 2003, p. 83.

que funcionam como instrumentos que nos auxiliam para atingir um determinado resultado. Nesse corolário, tendo em atenção ao problema da nossa pesquisa, adoptamos os seguintes métodos: jurídico, documental, dedutivo, indutivo, comparativo e hermenêutico.

1.2. Método Jurídico

De forma geral foi usado o método jurídico, tendo em vista a natureza do próprio estudo, que corresponde ao empreendimento de construção do saber científico na vertente jurídica (análise da Repercussão dos Crimes Cibernéticos no Direito Penal Moçambicano), iniciado da fase de investigação (pesquisa) à fase expositiva, que se consubstanciou na colocação dos discursos e de ideias concebidas no momento de levantamento da discussão até às fases conclusivas do presente trabalho.

Métodos jurídicos ou métodos da ciência jurídica têm como importante problema a metodologia jurídica, pois, segundo Kant, o método depende do conhecimento do objecto, ou melhor, do conhecimento resulta o método. O método mais usado no estudo foi o da dedução, que, por sua vez, o jurista deve partir do geral para o particular, isto é, das normas gerais para os casos.

1.3. Método Documental

Os fundamentos do método documental nesta pesquisa assentam-se na discussão do posicionamento do legislador e modos práticos do aplicador da Lei em relação a matéria em análise. A legislação e a doutrina tornaram possível tomar conhecimento sobre a realidade objectiva de matérias sobre os crimes cibernéticos.

1.4. Método Dedutivo

A escolha do método dedutivo por parte do Proponente assenta-se na base do objectivo de pesquisa "analisar a **Repercussão dos Crimes Cibernéticos no Direito Penal Moçambicano**", que partindo das premissas gerais caminha-se a situações ou fenómenos de nível particular. A partir de princípios, leis ou teorias consideradas verdadeiras e indiscutíveis, prediz a ocorrência de casos particulares com base na lógica. "Parte de princípios reconhecidos

como verdadeiros e indiscutíveis e possibilita chegar a conclusões de maneira puramente formal, isto é, em virtude unicamente de sua lógica."[14]

Método proposto pelos racionalistas Descartes, entre outros, pressupõe que só a razão é capaz de levar ao conhecimento verdadeiro. O raciocínio dedutivo tem o objectivo de explicar o conteúdo das premissas, por intermédio de uma cadeia de raciocínio em ordem descendente, de análise - do geral ao particular, chegando a uma conclusão. Usa o silogismo, a construção lógica para, a partir de duas premissas, retirar uma terceira logicamente decorrente das duas primeiras, denominada de conclusão.[15] Outrossim, o método dedutivo procura transformar enunciados explicativos complexos, universais, em particulares. A conclusão sempre resultará em uma ou várias premissas, fundamentando-se no raciocínio dedutivo.

O método dedutivo também pode se realizar nas operações lógicas, nas quais os raciocínios simples podem chegar a enunciados complexos. A dedução como forma de raciocínio lógico tem como ponto de partida um princípio tido, a prior, como verdadeiro. O seu objectivo é a tese ou conclusão, que é aquilo que se pretende provar.[16]

De acordo com o entendimento clássico, o método dedutivo é aquele que parte do geral e, a seguir, desce ao particular. A partir de princípios, leis ou teorias consideradas verdadeiras e indiscutíveis, prediz a ocorrência de casos particulares com base na lógica. "Parte de princípios reconhecidos como verdadeiros e indiscutíveis e possibilita chegar a conclusões de maneira puramente formal, isto é, em virtude unicamente de sua lógica."

De forma geral, no presente estudo, aplicamos o método dedutivo no intuito de verificar a forma como o legislador penal tipificou os crimes cibernéticos no quadro jurídico moçambicano.

1.5. O método Indutivo

O método indutivo baseou-se na análise dos aspectos particulares sobre os crimes cibernéticos no contexto jurídico-penal moçambicano, cujo foco assenta na questão de tipificação dos crimes cibernéticos na Ordem Jurídica moçambicana e, obviamente, na análise dos possíveis instrumentos fundamentais que concorrem para tal normatização.

[14] GIL, António Carlos, ***Métodos e técnicas de pesquisa social***. 6ª edição, Editora Atlas, São Paulo-Brasil, 2008, p. 54.
[15] PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de, Ob. Cit., p. 26-27.
[16] OLIVERIRA, Silvio Luis De, Ob. Cit., p.57.

1.6. Método Comparativo

Tendo em conta ao tema "**Repercussão dos Crimes Cibernéticos no Direito Penal Moçambicano**", pautamos pelo uso do método comparativo, dando um olhar atento aos posicionamentos jurídicos de três Estados, relacionando-os ao nosso país, nomeadamente - Brasil, Espanha e Portugal. Ainda, importa realçar que optamos pelo uso do método comparativo pela predisposição de trazer uma explicação exaustiva sobre as formas de implementação das políticas para combate e prevenção dos crimes cibernéticos, fenómenos que permitem analisar o dado concreto, deduzindo desse, como apregoa Marconi, "os elementos constantes, abstractos e gerais"[17]. Gil comenta que o método comparativo procede pela investigação de indivíduos, classes, fenómenos ou factos, com vista a ressaltar as diferenças e as similaridades entre eles. "Sua ampla utilização nas ciências sociais deve-se ao facto de possibilitar o estudo comparativo de grandes grupamentos sociais, separados pelo espaço e pelo tempo"[18]. É nessa perspectiva de Gil, que pretendemos trazer essa ilação no âmbito da comparação dentro do fenómeno proposto no capítulo V.

Optamos pelo método comparativo na perspectiva de entender os contornos das políticas implementadas, nos países acima referidos, para combate e prevenção dos crimes cibernéticos, cujos procedimentos foram desenvolvidos mediante rigoroso controlo e no entendimento de que os seus resultados proporcionam elevado grau de generalização, como tem ensinado Prodanov[19].

1.7. Método Hermenêutico

Ainda no âmbito dos métodos, também nos valemos do método hermenêutico, materializado pela prática de interpretação de textos constantes na norma constitucional e, com maior destaque, na legislação Penal em geral (Código Penal e Código de Processo Penal), além de outras legislações avulsas em relação ao problema assente no nosso estudo (A problemática dos crimes cibernéticos no ordenamento jurídico-penal em Moçambique).

---

[17] MARCONI, Mariana de Andrade, LAKATOS, Eva Maria, ***Técnicas de Pesquisa: panejamento e execução de pesquisas, amostragens e técnicas de pesquisas, elaboração e interpretação de dados***, 2ª edição, Editora Atlas, São Paulo: 1998. p. 107.

[18] GIL, António Carlos, ***Ob. Cit***., p. 16-17.

[19] PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de, Ob. Cit., p. 38.

Este método consiste na interpretação de textos inspirados em jurisconsultos, ou seja, é o método pelo qual se ocupa da interpretação das normas jurídicas, estabelecendo modos para a compreensão legal[20].

Concordando com Gil, este método, dá ênfase no papel do sujeito da acção e reconhece a parcialidade da visão do observador. Ao propor modelos de representação de variáveis e de tipos, busca a interpretação dos significados das coisas[21].

1.8. Tipos de Pesquisa Aplicados

No âmbito da realização do nosso trabalho recorremos a diferentes tipologias de pesquisa para fazer face a nossa abordagem. Nesse sentido, o nosso entendimento sobre uma pesquisa é que ela tem por objectivo estabelecer uma série de compreensões no sentido de descobrir respostas para as indagações e questões que existem em todos os ramos do conhecimento humano, envolvendo o mundo social, vegetal, animal, mineral, além do espaço e do mundo marinho. Pesquisar significa planear cuidadosamente uma investigação, de acordo com as normas da metodologia científica, tanto em termos de forma como de conteúdo.

No entendimento de Demo, a pesquisa é um "procedimento de fabricação do conhecimento, quanto como procedimento de aprendizagem (princípio científico e educativo), sendo parte integrante de todo processo reconstrutivo de conhecimento"[22]. Enquanto isso, Lakatos e Marconi, a consideram "um procedimento formal com método de pensamento reflexivo que requer um tratamento científico e se constitui no caminho para se conhecer a realidade ou para descobrir verdades parciais." Significa não apenas a procura da verdade, mas também descobrir respostas para perguntas ou soluções para os problemas levantados através do emprego de métodos científicos[23].

A pesquisa tem por finalidade tentar conhecer e explicar os fenómenos que ocorrem nas suas mais diferentes manifestações e a maneira como se processam os seus aspectos estruturais e funcionais a partir de uma série de interrogações. Neste corolário, para a materialização da nossa abordagem, aplicamos a tipologia que se segue:

1.9. Quanto a Natureza da Pesquisa

[20] LAKATOS; Marconi de. ***Fundamentos De Metodologia Científica***, A6. Edição. 5. Reimpressão. São Paulo: Atlas, 2007, p. 107.
[21] GIL, António Carlos, **ob. cit.,** p. 18-24.
[22] DEMO, P, ***Metodologia do conhecimento científico***, editora Atlas, São Paulo-Brasil, 2000, p. 20.
[23] MARCONI, Mariana de Andrade, LAKATOS, Eva Maria, Ob. Cit., p. 157.

1.9.1. Pesquisa Básica

Quanto a natureza, optamos pela pesquisa básica, visto que o nosso estudo está orientado para a análise mais acentuada sobre a Repercussão dos Crimes Cibernéticos no Direito Penal Moçambicano. Aqui, a pretensão foi de aferir a atitude do legislador penal perante os crimes cibernéticos no ciberespaço moçambicano.

Tendo em conta ao objectivo da pesquisa básica, de gerar conhecimentos novos úteis para o avanço da ciência jurídica, procuramos fazer uma conciliação com outros tipos de pesquisa adequáveis. Envolve verdades e interesses universais.

1.9.2. Pesquisa Qualitativa

Quanto ao modo de abordagem, optamos pelo uso da pesquisa qualitativa, na medida em que realizamos, por via dela, um estudo fundamentalmente interpretativo, baseado na análise da repercussão dos crimes cibernéticos no ordenamento jurídico-penal pátrio, com intenção de buscar o entendimento do legislador quanto à esta figura no quadro legislativo penal. Outrossim, o estudo é de carácter qualitativo pelo facto de permitir-nos aprofundar e interpretar, dentro do contexto temático, os dados recolhidos em várias fontes, viabilizando, assim, a pesquisa em causa. A pesquisa qualitativa optada no presente estudo teve como finalidades e características a compreensão dos significados dos dados recolhidos por várias fontes e posteriormente apresentados na presente tese. Em suma, neste tipo de estudo, enquanto pesquisadores, optamos em fazer a análise das informações recolhidas, tendo-nos baseado nas interpretações de natureza subjectiva.

A pesquisa qualitativa permitiu-nos mergulhar na complexidade dos acontecimentos reais e não apenas o evidente, mas também as contradições, os conflitos e as resistências a partir da interpretação dos dados no contexto da sua produção.

Ainda na abordagem qualitativa, a pesquisa teve o ambiente como fonte directa dos dados. Nesta perspectiva mantivemos o contacto directo com o ambiente e o objecto de estudo em questão – com o intuito de aprofundar a questão da repercussão dos crimes cibernéticos no ordenamento jurídico-penal moçambicano, sendo necessário um trabalho mais intensivo de investigação. Nesse caso, as questões foram estudadas no ambiente em que elas se apresentam sem qualquer manipulação intencional do pesquisador. A utilização desse tipo de abordagem difere da abordagem quantitativa pelo facto de não utilizar dados estatísticos como o centro do processo de análise de um problema, não tendo, portanto, a prioridade de numerar ou medir

unidades. Os dados recolhidos nessas pesquisas são, na sua maioria, descritivos, pela natureza do próprio estudo, como são os casos dos capítulos referentes a Evolução do Direito Penal Moçambicano, seguindo-se da Evolução da Legislação Penal Moçambicana e a Políticas Implementadas para o combate e prevenção dos crimes cibernéticos, cuja finalidade é construir bases teóricas e práticas para o desenho de uma Estratégia de Segurança Cibernética em Moçambique. Mesmo com essas vicissitudes, exigiu-nos uma análise minuciosa dos dados descritos, de forma a encontrar uma interpretação mais lógica do estágio actual da legislação penal, no que tange aos crimes cibernéticos no contexto moçambicano.

A escolha dessa tipologia (pesquisa qualitativa) foi pelo facto de que a nossa pretensão no estudo não era de apresentar um estudo com representatividade numérica, mas, sim, trazer o aprofundamento da compreensão da abordagem que se destaca na nossa tese. Dessa fundamentação, apoiamo-nos em Lessard - Hérbet, que nos ensina que o facto de uma investigação poder ser classificada de interpretativa ou qualitativa, provém mais da sua orientação fundamental, do que do procedimento, a pesquisa é qualitativa interpretativa porque pretende compreender, interpretar o fenómeno em estudo.

1.9.3. Do Ponto de Vista de seus Objectivos

1.9.3.1. Pesquisa Explicativa

Quanto aos objectivos, a pesquisa desenvolvida foi de natureza explicativa. O principal objectivo foi de explicar e racionalizar o objecto de estudo e tentar construir um conhecimento totalmente novo. Nessa ordem de ideias, a partir do objecto do estudo, "Análise da Repercussão dos Crimes Cibernéticos no Direito Penal Moçambicano", buscamos construir categorias que possam dar respostas à questão central do nosso estudo. Assim sendo, definimos como objectivos específicos os seguintes: compreender o decurso histórico do Direito Penal moçambicano desde o tempo colonial, pós-colonial até pós-independência; verificar a repercussão dos tipos criminais no Direito Penal moçambicano; aferir a essência dos crimes cibernéticos/informáticos nas correntes doutrinais, sem descurar a sua tipologia quadro; trazer o entendimento no âmbito do direito comparativo sobre as políticas implementadas para a combate e prevenção dos crimes cibernéticos no contexto de outros ordenamentos Jurídicos (Brasil, Espanha e Portugal). E finalmente, discutir as implicações dos crimes cibernéticos no Direito Penal moçambicano.

Importa referir que a opção pela pesquisa explicativa deveu-se ao facto de ela permitir identificar os factores que determinam ou contribuem para a ocorrência dos fenómenos em

estudo, assim como aprofundar o conhecimento da realidade, explicando a razão ou o "porquê" das coisas. Outrossim, a razão da escolha deste tipo de pesquisa justifica-se pela capacidade que este tipo de pesquisa tem em detalhar como decorrem as situações jurídicas identificadas na presente pesquisa. O principal objectivo foi de explicar e racionalizar o objecto do estudo, procurando construir um conhecimento que possa inovar ou dar resposta mais precisa a actual situação dos crimes cibernéticos no Ciberespaço nacional e internacional.

1.9.4. Do Ponto de Vista dos Procedimentos Técnicos

Quanto aos procedimentos técnicos, ou seja, a maneira pela qual obtemos os dados necessários para a elaboração da pesquisa, tornou-se necessário traçar um modelo conceptual e operativo dessa, denominado de *design*, que pode ser traduzido como delineamento, uma vez que expressa as ideias de modelo, sinopse e plano. O delineamento refere-se ao quadro de planificação da pesquisa em sua dimensão mais ampla, envolvendo a previsão de análise e interpretação de recolha de dados. Nesse corolário, foi apenas definida a fonte de papel (pesquisa bibliográfica e pesquisa documental), para fazer face ao processo de compilação dos dados para a construção do presente saber jurídico.

1.9.4.1. Pesquisa Bibliográfica

Usamos a pesquisa bibliográfica pelo facto de ser uma das mais comuns e normalmente considerada obrigatória em quase todos os moldes de trabalhos científicos. Com base neste tipo de pesquisa, recolhemos informações a partir de textos, livros, artigos e demais materiais de carácter científico, tal como podemos observar nas referências bibliográfica ao longo do nosso texto e na lista bibliográfica. A consulta bibliográfica teve em vista o aprofundamento dos conceitos e definições sobre os vários institutos jurídicos do presente estudo, além de ter permitido, em alguns casos, a apresentação de uma abordagem mais aprofundada e abrangente sobre a problemática em análise na presente tese.

Portanto, a pesquisa bibliográfica ajudou a compreender, no âmbito da doutrina, as manifestações dos crimes cibernéticos e a sua adequação no contexto jurídico moçambicano.

1.9.4.2. Pesquisa Documental

A pesquisa documental desempenhou um papel preponderante para a pesquisa, visto ter sido a base ou fonte de dados com conteúdo informacional muito úteis para a pesquisa, como por exemplo, legislação pertinente, relatórios de estudos jurídicos, entre outros, tendo criado um vínculo entre o discurso teórico e a realidade apresentada nos documentos, de modo a sustentar, de forma específica, o tema central do nosso estudo.

No decurso dos procedimentos técnicos, foi qualificado o estudo de natureza documental, por exemplo, legislação pertinente, relatórios de estudos etc., nesse âmbito, foi feita a análise e interpretação da legislação pertinente: documentos normativos (quadro jurídico-legal sobre os crimes cibernéticos em Moçambique, apresentado no capítulo sexto do presente estudo, concretamente no subcapítulo 9.

Nesse âmbito, foi feita análise e interpretação da legislação pertinente, que são documentos normativos, entre eles - o quadro jurídico-legal dos diversos diplomas normativos inerentes aos crimes cibernéticos, como por exemplo, i) Constituição da República de Moçambique (CRM de 2004), que inclui a Lei de Revisão Pontual da Constituição (Lei nº 1/2018, de 12 de Junho, publicado no Boletim da República, 1ª Série – nº 115, 2º Suplemento, de 12 de Junho de 2018; ii) os Códigos Penais de 1889, 2014 e 2019 (*Código Penal* (CP); o Código Penal de 1886, ora vigente, aprovado pelo Decreto de 10 de Setembro de 1886, revogado pela Lei nº 35/2014, de 31 de Dezembro, posteriormente revogada pela Lei nº 24/2019, de 24 de Dezembro, que aprova o CP Vigente, publicada no Boletim da República, 1ª Série, nº 249, de 26 de Dezembro de 2019, o respectivos Códigos do Processo Penal (*Código do Processo Penal* (CPP), ora vigente foi aprovado pelo Decreto nº 16489 de 15 de Fevereiro de 1929 e mandado a vigorar na então colónia de Moçambique, pela Portaria nº 19271, de 24 de Janeiro de 1931, revisto pela Lei nº 25/2019 de 26 de Dezembro, publicada no Boletim da República, 1ª Série, nº 248, de 26 de Dezembro de 2019); iii) o Código Civil vigente e respectivo Código do Processo Civil (O Código Civil (CC) de 1966, aprovado como Código Civil português, pelo Dec. – Lei nº 47344, de 25 de Novembro de 1966 e extensivas as províncias ultramarinas pela Portaria nº 22 869, de 4 de Setembro de 1967 e *Código do Processo Civil* (CPC), ora aprovado pelo Decreto-lei nº 44.129, de 28 de Dezembro de 1961, tornado extensivo ao ultramar pela Portaria nº 19305, de 30 de Julho de 1962, e entrou em vigor a 1 de Janeiro de 1963. Este Código Civil foi revisto pelo Decreto-Lei nº 1/2005, de 27 de Dezembro, publicado no Boletim da República, 1ª Série – nº 51, 5º Suplemento, de 27 de Dezembro de 2005, posteriormente alguns artigos sofreram alterações por força do Decreto-Lei nº 1/2009, de 24 de Abril, Publicado no Boletim da República, 1ª Série, nº 16, 3º Suplemento, 24 de Abril de

2009. Ainda no âmbito documental recorremos a Política de Segurança Cibernética em Moçambique (Resolução 69/2021 de 31 de Dezembro, que ***aprova a política de segurança cibernética e a estratégia de sua implementação,*** *in* Boletim da República, I série, número 253 de 31 de Dezembro). E outra legislação extravagante.

A pesquisa documental, devido as suas características, pode ser confundida com a pesquisa bibliográfica. Destaca-se como principal diferença entre esses dois tipos de pesquisa, a natureza das fontes pesquisadas. Enquanto a pesquisa bibliográfica utiliza-se, fundamentalmente, das contribuições de vários autores sobre determinado assunto, a pesquisa documental baseia-se em materiais que não receberam ainda um tratamento analítico ou que podem ser reelaborados de acordo com os objectivos da pesquisa[24].

A utilização da pesquisa documental é destacada, nesta abordagem metodológica, pelo facto de sentirmos a necessidade de organizar informações que se encontravam dispersas, devido a natureza do tema, que não tem uma legislação específica e documentos sistematizados a volta dos crimes cibernéticos.

1.10. Técnica de Apresentação e Análise de Dados

Para apresentação e análise de dados, a triangulação teórica e de localização foi o principal critério aplicado. Nesse contexto, tivemos em conta as diferentes teorias relativas: a evolução histórica do Direito Penal Tradicional Moçambicano ao Direito Penal Digital; as teorias sobre os conceitos dos crimes cibernéticos; a classificação doutrinal dos crimes cibernéticos. Também foi feita a triangulação da localização mediante a descrição da implementação das políticas para o combate e prevenção dos crimes cibernéticos no âmbito do direito comparado (Brasil, Espanha e Portugal). Finalmente, a triangulação teórica do cibercrime foi associada à Repercussão dos Crimes Cibernéticos no Direito Penal Moçambicano.

Em suma, para permitir a triangulação teórica e comparativa, tivemos de usar a técnica de levantamento bibliográfico e documental, instrumento que nos permitiu uma análise profunda das questões em torno do problema.

[24] GIL, António Carlos, Ob. Cit., p. 107.

1.11. Técnica de Discussão dos Resultados

No que diz respeito a técnica de discussão dos resultados, optamos pela análise do conteúdo, que consistiu na leitura e interpretação dos conteúdos abordados na fase da apresentação e análise dos dados, isto é, a base da discussão assentou nos resultados interpretados a partir da triangulação teórica. A análise de conteúdo foi coadjuvada com o método hermenêutico, o qual se ocupa da interpretação das normas jurídicas, estabelecendo procedimentos para a compreensão legal. Portanto, neste estudo, a sua aplicação fundamenta-se na medida em que representa um conjunto de técnicas de análise das comunicações, visando obter dados, através de procedimentos sistemáticos e objectivos de descrição do conteúdo das mensagens, que permitiram inferir conhecimentos relativos às condições de produção ou de recepção dessas mesmas mensagens.

PARTE II- COMPONENTE TEÓRICA

CAPÍTULO II: DO DIREITO PENAL EM GERAL AO DIREITO PENAL DIGITAL

2.1. Evolução do Direito Penal em Geral

O estudo da evolução histórica do Direito Penal é de extrema importância para um julgamento correto da *mentalidade e dos princípios que norteiam o sistema punitivo contemporâneo. "*Desde o surgimento da humanidade houve o aparecimento e a evolução das ideias penais. Dessa forma, o Direito Penal sofria transformações a cada vez que a própria humanidade se modificava. Neste contexto, podemos dividir a evolução do Direito Penal em períodos e fases que tiveram características marcantes e influenciaram ou ainda influenciam o Direito Penal actual."[25]

2.1.1. As Fases da Evolução Histórica do Direito Penal ao Longo do Tempo

2.1.1.1. Vingança Penal

Antes mesmo da nossa era, surgiram situações das ideias penais. Nisto, o Direito Penal, passou por várias vicissitudes, em virtude da evolução da sociedade ou modificação do seu modo de vida ou de estar. Nesta senda, podemos partilhar a evolução do Direito Penal em etapas ou fazes que, de certa forma, se tornaram momentos importantes ou determinantes e que influenciaram o Direito Penal moderno.

Neste contexto, "várias foram as fases de evolução da vingança penal, etapas essas que não se sucederam sistematicamente, com épocas de transição e adopção de princípios diversos, normalmente envolvidos em sentido religioso. Assim, as primeiras ideias de direito penal foram expressas pela vingança penal que se subdivide em três, designadamente: a vingança privada, a vingança divina e a vingança pública"[26].

2.1.1.2.Vingança Privada

Durante o período da vingança privada, quando houvesse a ocorrência de um crime, em resposta ao mesmo, havia uma reacção da vítima, dos parentes e até mesmo de seu grupo social

[25] JOLO, Ana Flavia, ***Evolução Histórica do Direito Penal***, São Paulo. p.121.
[26] MIRABETE, Júlio Fabbrini; et al, ***Manual de Direito Penal: Parte Geral***, Volume I, 27ª ed., Editora Atlas S.A, 2011. p.16

(tribo), que "agiam desproporcionalmente à ofensa, atingindo não só o agente causador do delito como também todo o seu grupo de convivência. Caso o ofensor fosse pertencente ao mesmo grupo social (tribo), podia ser punido com a "expulsão da paz", uma espécie de banimento, deixando-o a mercê de outros grupos que, normalmente, o apenavam com a morte"[27]. No entanto, "se o ofensor fosse de uma tribo diferente da do ofendido, a reacção era a conhecida por *vingança de sangue*, que era considerada um dever religioso e sagrado, uma verdadeira guerra movida pelo grupo ofendido àquele a que pertencia o ofensor, culminando, não raras vezes, com a eliminação completa de um dos grupos."[28]

Duas grandes regulamentações, com o evoluir dos tempos, encontraram a vingança privada: o talião (olho por olho, sangue por sangue, dente por dente) e a composição.[29] Na verdade não se tratava propriamente de uma pena de talião, mas de um instrumento moderador da pena. A primeira noção de proporcionalidade entre a ofensa e a punição advinda dela consistia em aplicar ao agente ofensor o mal que este causou à vítima, na mesma proporção[30].

No entanto, há previsão no Código de Hamurabi (2083 a.C.) neste sentido, nos seus artigos 209 e 210, respectivamente, onde se estatuía que "*Se alguém bate numa mulher livre e a faz abortar, deverá pagar dez ciclos pelo feto"* e *"Se essa mulher morre, então deverá matar o filho dele".* A Bíblia Sagrada, no Livro Levítico, 24, 17, também dispõe que: *"todo aquele que ferir mortalmente um homem será morto".* Nesta senda, versa a Lei das XII Tábuas, conforme se extrai do artigo 11 que determina que "*Se alguém fere a outrem, que sofra a pena de Talião, salvo se houver acordo"*[31].

Depois, surgiu a ideia da composição, que consistia num sistema no qual o delinquente se livrava da punição com a compra de sua liberdade. Abraçada, ainda, pelo Código de Hamurabi (Babilónia), pelo Pentateuco (Hebreus) e pelo Código de Manu (Índia), que foi largamente aceita pelo Direito Germânico, constituindo um dos precedentes da moderna reparação do dano, no Direito Civil e das penas pecuniárias, no Direito Penal[32].

---

[27] DOTTI, René Ariel, ***Curso de direito penal: parte geral,*** 3ª. ed., rev., atual. e ampl, Editora Forense, Rio de Janeiro 2010.
[28] FRAGOSO, Heleno Cláudio, ***Lições de Direito Penal: parte geral***, Rio de Janeiro, Forense, 2006.
[29] MIRABETE, Júlio Fabbrini; et al. **ob., cit**. p.16.
[30] JOLO, Ana Flavia, ***ob., it.***.
[31] MIRABETE, Júlio Fabbrini; et al. **ob., cit**. p.16.
[32] DOTTI, René Ariel, ***et al.*** 2010.

2.1.1.3. Vingança Divina

A vingança divina nasce sob fortes ditames da religião dos povos antigos. O Direito Penal foi profundamente influenciado pela religião, visto que havia uma cultura e a crença de que se deveria censurar o crime como agradecimento aos deuses pelos comportamentos ilícitos criminais cometidos no meio social.

Na vingança divina, a punição era entendida como responsabilidade divina e era aplicada pelos sacerdotes. Estes impunham penas totalmente severas, cruéis e até consideradas desumanas, tendo como principal objectivo, criar um pânico que permitisse intimidar a sociedade. Pune-se com rigor, antes com notória crueldade, pois "o castigo deve estar em relação com a grandeza do deus ofendido"[33]. Tratava-se do Direito Penal religioso, que tinha como objectivo a purificação da alma do ofensor, através da aplicação de uma sanção[34]. Seus princípios podem ser verificados no Código de Manu (Índia) e no Código de Hamurabi, assim como nas regiões do Egipto, Assíria, Fenícia, Israel e Grécia. Um exemplo disso é o artigo 6º do Código de Hamurabi que dispõe que: "Se alguém furta bens do Deus ou da Corte deverá ser morto; e mais, quem recebeu dele a coisa furtada também deverá ser morto"[35].

2.1.1.4. Vingança Pública

Com a maior organização social, atingiu-se a fase da vingança pública. No sentido de se dar maior estabilidade ao Estado, visava dar mais segurança ao príncipe ou soberano pela aplicação da pena, ainda severa e cruel. Nesta época, libertou-se a pena do seu carácter religioso, transformando-se a responsabilidade do grupo em individual (do autor do facto), em positiva contribuição ao aperfeiçoamento de humanização dos costumes penais[36].

A vingança pública passou a ser praticada pressupondo um maior desenvolvimento das sociedades, mas o seu conteúdo ainda era permeado pela influência religiosa. Nesta fase, o poder punitivo passou a ser exercido também pelo monarca, segundo o seu arbítrio, mas em nome de Deus. No entanto, "a primeira finalidade reconhecida desta fase era garantir a segurança do soberano, por meio da aplicação da sanção penal, ainda dominada pela crueldade e desumanidade, característica do direito criminal da época".[37] Não obstante a inexistência de

[33] JESUS, Damásio E. de Direito ***Penal: parte geral***, Saraiva, São Paulo, 2010.
[34] JORGE, Wiliam Wanderley. ***Curso de Direito Penal: Parte Geral***, Volume 1, Editora Forense, Rio de Janeiro. 1986.
[35] CAPEZ, Fernando**, *Curso de Direito Penal***. 15ª Ed., Saraiva Editora, São Paulo, 2011.
[36] MIRABETE, Júlio Fabbrini; et al. ob., **cit**. p.16.
[37] Ibidem, p.16.

garantias aos transgressores, esta fase corresponde a uma evolução na aplicação das penas, porquanto confere a sua aplicação ao Estado, ainda que este a exerça com rigor desmedido, mas representa um limite para a actuação individual[38].

2.1.2. O Direito Romano

No princípio, "o direito e a religião eram fortemente ligados, o *Pater Famílias* detinha o poder de exercitar o direito de vida e de morte sobre todos os seus dependentes, até mesmo em relação às mulheres e aos escravos. Com o advento da República Romana ocorreu a ruptura e o desmembramento destes dois alicerces. A partir desse momento, aboliu-se o período das vinganças e os crimes passaram a ser divididos em crimes públicos e crimes privados"[39].

Os crimes públicos eram aqueles que traziam algum mal à sociedade e eram punidos pelo Estado, enquanto os crimes privados eram aqueles cometidos contra os particulares, cuja punição ficava a cargo deles mesmos, sendo que o Estado apenas regulamentava estas punições caso fosse necessário. As principais características do Direito Penal Romano são:

a) A afirmação do carácter público e social do Direito Penal;
b) O amplo desenvolvimento alcançado pela doutrina da imputabilidade, da culpabilidade e de suas excludentes;
c) O elemento subjectivo doloso se encontra claramente diferenciado: o dolo (*animus)*, que significava a vontade delituosa, que se aplicava a todo campo do direito, tinha, juridicamente, o sentido de astúcia, e *dolus malus*, reforçada, a maior parte das vezes, pelo adjectivo má, o velho *dolus malus*, que era enriquecido pelo requisito da consciência da injustiça[40];
d) A teoria da tentativa, que não teve um desenvolvimento completo, embora se admita que era punida nos chamados crimes extraordinários;
e) O reconhecimento, de modo excepcional, das causas de justificação (legitima defesa e estado de necessidade);
f) A pena constituiu uma reacção pública, correspondendo ao Estado a sua aplicação;
g) A distinção entre crimina publica, *delicta* privada e previsão dos *delicta* extraordinária;
h) A consideração do concurso de pessoas, diferenciando a autoria e a participação.

[38] ZAFFARONI, Eugenio Raúl; et., al, ***Manual de Direito Penal Brasileiro: Parte Geral***, 5 ed. rev. e atual, Editora Revista dos Tribunais, São Paulo, 2004, p.342.
[39] MIRABETE, Júlio Fabbrini; et al. ob., cit. p.19.
[40] JOLO, Ana Flavia, ***ob., cit***. p.116.

A partir dessas características entendemos que o Direito Romano, desde sempre, influenciou o Direito Penal, inclusive trazendo algumas ideias que acabaram sendo incorporadas pelo Direito Penal pátrio estando vigente até hoje.[41]

Assim sendo, o Direito Romano contribuiu decisivamente para a evolução do Direito Penal, com a criação de princípios penais sobre o erro, culpa, dolo, imputabilidade, coacção irresistível, agravantes, legitima defesa, etc.[42].

2.1.3. O Direito Germânico

O direito germânico tem como característica principal o facto de ser baseado nos costumes (direito consuetudinário), razão pela qual não era um direito escrito.[43] Naquele período, o direito era visto como uma ordem de paz, cuja violação consistia em uma ruptura dessa paz, podendo ser pública ou privada, conforme a natureza do delito e sujeita a repressão. Na hipótese de perda da paz pública havia uma autorização para que qualquer pessoa do povo matasse o transgressor, contudo, no caso de delito privado o agente era entregue à família da vítima para que esta exercesse o direito de vingança.[44] Além disso, entre o povo germânico vigorava a vingança de sangue, que somente após o avanço da sociedade, com o fortalecimento do poder do Estado, foi sendo gradativamente substituída pela composição[45].

A composição judicial era dividida em três espécies principais: (i) composição - paga ao ofendido ou ao seu grupo familiar, a título de reparação pecuniária; (ii) Busse - soma que o delinquente pagava a vítima ou sua família, pela compra do direito de vingança e (iii) Friedgeld ou Fredus - que era o pagamento ao chefe tribal, ao tribunal, ao soberano ou ao Estado, como preço da paz[46].

Outra característica importante do Direito Germânico foi a ausência de distinção entre dolo, culpa e caso fortuito, determinando-se a punição do autor do facto sempre em relação ao dano por ele causado e não de acordo com o aspecto subjectivo de seu acto. Surgiu assim a primeira ideia de responsabilidade objectiva. Dessa forma já se tinha uma ideia de reparação do dano e até mesmo uma forma de substituição da pena aplicada pela prestação pecuniária utilizada inclusive em nosso Direito Penal nacional actualmente. O Direito Germânico foi ainda

---

[41] JESUS, Damásio E. de, ***Direito Penal: parte geral***, Saraiva, São Paulo, 2010.
[42] MIRABETE, Júlio Fabbrini; et al, ob., cit. p.17.
[43] NORONHA, E. Magalhães, ***Direito Penal: Introdução e Parte Geral,*** 36ª edição, Saraiva, São Paulo 2001.
[44] MIRABETE, Júlio Fabbrini; et al. ob., cit. p.17.
[45] MEHMERI, Adilson. ***Noções Básicas de Direito Penal,*** São Paulo, Saraiva, 2000.
[46] JOLO, Ana Flavia, ***et., cit***.

um dos "primeiros a utilizar uma política criminal consciente para a punição do agente criminoso"[47].

2.1.4. O Direito Canónico

O Direito Canónico, também conhecido como o ordenamento jurídico da Igreja Católica Apostólica Romana, "exerceu grande e importante influência na legislação penal. Essa influência teve início com a declaração da liberdade de culto pelo imperador romano Constantino, acentuando-se quando o imperador Teodósio I proclamou-a como a única religião do Estado. No entanto, com o governo de Clodoveu, rei dos francos, emanaram a conversão e o baptismo fazendo com que a religião cristã se firmasse na monarquia franca introduzindo uma verdadeira jurisdição eclesiástica"[48].

Apesar da união da Igreja com o Estado, esta continuou independente e superior no âmbito religioso. Inicialmente o Direito Penal Canónico detinha carácter meramente disciplinar, porém com o enfraquecimento do poder estatal este passou a regulamentar e aplicar punição em muitas situações. Neste sentido, a jurisdição eclesiástica dividia-se em "*rationare persona*, que levava em consideração a pessoa, assim o religioso era sempre julgado por um tribunal da Igreja, independentemente do tipo de delito cometido por ele, e *rationare matéria*, em razão da matéria, assim firmava-se a competência eclesiástica ainda que o agente do delito não fosse religioso"[49].

Dessa forma, os delitos eram classificados conforme o bem jurídico violado. Quando ofendiam o direito divino, eram chamados de *delicta* eclesiástica, estando sob a competência dos tribunais eclesiásticos e, portanto, tendo como repressão as *penitentiae*. Quando feriam tão-somente a ordem jurídica leiga, estavam sob a competência do Estado e eram punidos com penas comuns, eventualmente sofrendo punição eclesiástica, estes crimes eram conhecidos como *delicta mere secularia*.[50] Nos casos em que a atividade delitiva transgredia tanto a ordem laica como a religiosa esta era julgada pelo tribunal que primeiro conhecesse o facto, eram os *delicta mixta*. Para Heleno Cláudio Fragoso "a influência do direito canónico foi benéfica porque trouxe a humanização das penas, conquanto politicamente a sua luta metódica se

[47] NORONHA, E. Magalhães, et., cit. 2001.
[48] ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique, ***Manual de Direito Penal Brasileiro: Parte Geral***, 5 ed. rev. e atual, Editora Revista dos Tribunais, São Paulo, 2004.
[49] MEHMERI, Adilson. ***Noções Básicas de Direito Penal,*** São Paulo, Saraiva, 2000.
[50] CAPEZ, Fernando***, Curso de Direito Penal***. 15ª Ed., Saraiva Editora, São Paulo, 2011.

propusesse a obter a superioridade do papado sobre o poder estatal visando proteger os interesses religiosos de dominação"[51].

O Direito Canónico apregoou "a igualdade de todos os homens, enfatizando o aspecto subjectivo do crime, opondo-se assim ao sentido puramente objectivo da ofensa, que prevalecia no direito germânico. Posicionava-se contrariamente a pena capital entendendo que o indivíduo precisava manter-se enclausurado para que se arrependesse do mal que cometeu e se convertesse"[52]. Além disso, "o Direito Canónico também fez oposição às ordálias e aos duelos judiciários e introduziu as penas privativas de liberdade, suprindo as penas patrimoniais, para permitir o arrependimento e a ressocialização do réu. Apesar das vantagens trazidas por essa concepção religiosa do direito existiu também seu lado negativo como, por exemplo, no caso das punições desumanas aplicadas pela Santa Inquisição"[53].

2.1.5. O Período Humanitário

O período humanitário "surgiu durante o Século XVIII, também conhecido como Século das Luzes, devido a uma concepção filosófica que se firmou naquela época, caracterizada por uma ampliação do domínio da razão em todas as áreas do conhecimento humano. Durante esta época, surgiram muitos pensadores que defendiam a propagação do uso da razão para conduzir o desenvolvimento da vida em todos os seus aspectos. Dentre as ideias, trazidas por estes pensadores, algumas delas influenciaram directamente o Direito Penal, estabelecendo uma nova concepção frente às punições aplicadas aos transgressores da lei penal"[54].

Para a filosofia penal iluminista, o problema punitivo estava totalmente desvinculado das apreensões éticas e religiosas, assim o crime se fundava no contrato social infringido e a pena era tida como uma simples medida preventiva"[55]. Neste contexto político-cultural, destacou-se "o pensador Cesar Bonessana, marquês de Beccaria, que publica em 1764 a famosa obra *Dei delitti e delle pene* (Dos delitos e das penas) influenciado pelas ideias de Montesquieu, Rousseau, Voltaire, Locke e Helvétius. As ideias trazidas nesta obra marcaram o início do Direito Penal moderno"[56].

Segundo Jesus, "Cesare Beccaria trouxe uma nova concepção sobre a finalidade da punição de um delito e do estabelecimento de uma proporcionalidade entre a gravidade da

[51] JOLO, Ana Flavia, ***ob., cit.***.
[52] MIRABETE, Júlio Fabbrini; et al., ***ob., cit.*** p.17
[53] NORONHA, E. Magalhães, ***ob., cit.***.
[54] Ibidem.
[55] MIRABETE, Júlio Fabbrini; et al., ***ob., cit***. p.18.
[56] ZAFFARONI, Eugenio Raúl; et al., ***ob., cit***..

repressão com relação a gravidade do delito praticado"[57]. Além disso, segundo o autor citado, "desenvolveu a ideia da estrita legalidade dos crimes e das penas"[58]. Na sua Obra Dos Delitos e Das Penas, Beccaria alegou que "a finalidade das penalidades não é torturar e afligir um ser sensível, nem desfazer um crime que já está praticado. Quanto mais terríveis forem os castigos, tanto mais cheio de audácia será o culpado em evitá-los. Praticará novos crimes, para subtrair-se à pena que mereceu pelo primeiro"[59]. Para que cada pena não seja uma violência de um ou de muitos contra um cidadão particular, deve ser essencialmente pública, eficaz, necessária, a mínima das possíveis nas circunstâncias dadas, proporcional aos crimes, ditada pelas leis.

Para além de Beccaria, merecem destaque também outros pensadores como - "John Howard, que inspirou uma corrente penitenciarista preocupada em construir estabelecimentos apropriados para o cumprimento da pena privativa de liberdade; Jeremias Bentham, que foi um dos primeiros autores a expor com ponderada ordem sistemática as suas ideias, e Paulo Anselmo Von Feuerbach, que publicou a primeira obra sistemática e moderna de Direito Penal"[60].

2.1.6. Escolas Penais

2.1.6.1. Escola Clássica

Esta escola teve como base as ideias iluministas que se difundiram naquela época, era defendida por escritores, pensadores, filósofos e doutrinadores que compartilhavam dessas ideias. A Escola Clássica comparava a alma humana a uma balança, em cujos pratos estavam os motivos de nossas acções: a vontade, poderosa e decisiva, seria capaz de fazer subir o prato que apresentasse os motivos mais pesados, mesmo contra a lei da gravidade[61]. No livre arbítrio, está "o fundamento da imputabilidade moral, que é por sua vez o fundamento da responsabilidade penal. Só se pode imputar delito a alguém, quando dotado de livre arbítrio, quando possua a liberdade de optar entre os motivos"[62].

Aqui, "o Direito tem uma natureza transcendente, segue a ordem imutável da lei natural: O Direito é congénito ao homem, porque foi dado por Deus a humanidade desde o primeiro momento de sua criação, para que ela pudesse cumprir seus deveres na vida terrena. O Direito

[57] JESUS, Damasio E. de, ***ob.cit***.
[58] Ibidem.
[59] JESUS, Damásio E. de, ***ob. cit.***
[60] Ibidem.
[61] MIRABETE, Júlio Fabbrini; et al. ***ob., cit***. p.19.
[62] JORGE, Wiliam Wanderley, ***Curso de Direito Penal: Parte Geral***, Volume 1, Editora Forense, Rio de Janeiro. 1986.

é a liberdade. Portanto, a ciência criminal é o supremo código da liberdade, que tem por objecto subtrair o homem da tirania dos demais, e ajudar a se livrar da tirania de si mesmo e de suas próprias paixões. O Direito Penal tem sua génese e fundamento na lei eterna da harmonia universal"[63].

O delito é um ente jurídico, já que constitui uma violação a um direito. Isto significa que o delito é definido como infracção. Nada mais é que a relação de contradição entre o facto humano e a lei e a responsabilidade penal é lastreada na imputabilidade moral e no livre arbítrio humano.

A pena é vista como meio de tutela jurídica e como retribuição da culpa moral comprovada pelo crime. O fim primeiro da pena é o restabelecimento da ordem externa na sociedade, alterada pelo crime. Em consequência, a sanção penal deve ser aflitiva, exemplar, pública, certa, proporcional ao crime, célere e justa. O método utilizado é o dedutivo ou lógico-abstracto.

O delinquente é, em regra, um homem normal que se sente livre para optar entre o bem e o mal e preferiu o último. Os objectos de estudo do Direito Penal são o crime, a pena e o processo. Neste contexto, "três grandes pensadores foram considerados como precursores da Escola Clássica: na Alemanha, Anselmo Von Fewerbach; na Itália, Gian Domenico Romagnosi; e na Inglaterra, Jeremias Benthan. Esta Escola foi marcada pela sua divisão em dois períodos: o filosófico (idealizado por Cesar e Beccaria) e o jurídico (idealizado por Francisco Carrara), sendo este último mais importante para a análise do Direito"[64].

2.1.6.2. Escola Positiva

Esta nova corrente filosófica, denominada Escola Positiva, teve como seu percursor o pensador e filósofo Augusto Comte. A Escola Positiva proclamava uma nova concepção do direito e consequentemente do crime. Dessa forma, para os defensores dessa Escola, o direito é resultante da vida em sociedade e submisso a modificações no tempo e espaço, segundo a lei da evolução. Como fundamentos e características dessa escola, temos os seguintes:

i. Método indutivo, segundo Fragoso, "o crime como fenómeno natural e social, oriundo de causas biológicas, físicas e sociais; a responsabilidade

[63] JOLO, Ana Flávia, ***ob., cit.***
[64] ZAFFARONI, Eugenio Raúl; et al., ob. cit.

social como decorrência do determinismo e da periculosidade; a pena tendo por fim a defesa social e não a tutela jurídica"[65]

ii. Destacou-se, neste período, o médico italiano e professor César Lombroso, que considerava o crime "como uma manifestação da personalidade humana e produto de várias causas já que estudou o delinquente sob o ponto de vista biológico.

A Escola Positiva, não obstante, tem seu maior expoente em Henrique Ferri, criador da Sociologia Criminal. Foi considerado um discípulo de Lombroso e defendia a importância de um trinómio causal do crime, quais sejam factores antropológicos, sociais e físicos. "Classificou os criminosos em cinco categorias: nato, louco, habitual, ocasional e passional"[66].

2.1.6.3. Escolas Eclécticas

Com a finalidade de harmonizar os princípios da Escola Clássica e da Escola Positiva, surgiram as Escolas Eclécticas, como a Terceira Escola e a Escola Moderna Alemã. Aproveitando as ideias de clássicos e positivistas, separava-se o Direito Penal das demais ciências penais, contribuindo de certa forma para a evolução dos dois estudos. Referiam-se os estudiosos à causalidade do crime e não à sua fatalidade, excluindo, portanto, o tipo criminal antropológico e pregavam a reforma social como dever do Estado no combate ao crime. Estas escolas tiveram como pensadores principais os filósofos Bernardino Alimena, Giuseppe Impalomeni, Carnevale e Von Liszt[67].

2.2. Evolução do Direito Penal Moçambicano

2.2.1. O Direito Moçambicano Durante a Colonização Portuguesa

Torres ensina que "que durante o período de colonização portuguesa em Moçambique, o sistema jurídico aplicado no país foi predominantemente baseado no direito português. Os colonizadores portugueses introduziram suas leis e instituições jurídicas no território, buscando impor seu sistema legal sobre a população moçambicana"[68]. Durante esse período, segundo Silva, "Moçambique era considerado uma colónia de Portugal e estava sujeito às leis e

[65] FRAGOSO, Heleno Cláudio; ***ob. cit***.
[66] DOTTI, René Ariel, ***ob. cit.***
[67] ibidem.
[68] TORRES, Adelino, ***O Império Português entre o Real e o Imaginário***, S/Ed., Esher, Lisboa, 1991, p. 291.

regulamentos estabelecidos pelas autoridades coloniais portuguesas. O Direito Penal em vigor na época colonial em Moçambique era essencialmente o Direito Penal português[69]".

Em conformidade com Boxer, "as leis coloniais portuguesas estabeleciam uma hierarquia legal em que as normas e regulamentos impostos pelos colonizadores prevaleciam sobre as leis e costumes tradicionais do povo moçambicano"[70]. Partindo dos pressupostos do autor citado, somos de entendimento que o sistema legal português foi usado como uma ferramenta de controlo e dominação, visando principalmente a exploração dos recursos naturais e a manutenção do domínio colonial.

Durante o período colonial, "os colonizadores portugueses estabeleceram tribunais, órgãos administrativos e uma estrutura legal que reflectia o sistema jurídico português. Os tribunais coloniais aplicavam as leis e regulamentos portugueses, e os juízes eram, em sua maioria, de origem portuguesa. Os costumes e tradições locais do povo moçambicano muitas vezes não eram reconhecidos ou considerados no sistema legal colonial"[71].

2.2.2. Tentativa de Codificação dos Costumes e Elaboração do Código Penal para a Colónia (Moçambique)

A partir da década de 1920, segundo Newitt "a administração colonial portuguesa em Moçambique tentou codificar os costumes dos Moçambicanos, um dos objectivos era criar códigos jurídicos específicos para os colonizados"[72]. Enquanto isso, Thomaz diz que "os discursos colonialistas apresentavam diferentes justificativas, que oscilavam entre a imagem dos "africanos" como seres humanos inferiores e a retórica de respeito pelos seus usos e costumes. Tais discursos e práticas foram marcados por conflitos que envolviam funcionários administrativos coloniais e juristas (na colónia e na metrópole). Foi deste modo que a tentativa de criar um código penal para os Moçambicanos da época evidenciou as disputas existentes no campo jurídico e político colonialista"[73].

Durante os primeiros anos do colonialismo português em Moçambique, em conformidade com Thomaz, "entre o final do século XIX e o início do XX, havia pouco interesse em codificar os usos e costumes dos Moçambicanos. As campanhas militares e o

[69] SILVA, Nuno J. ESPINOSA Gomes da, ***História do Direito Português – Fontes de Direito***, 3ª Ed. Fundação Calouste Gulbekian, Lisboa, 2000, p. 111.
[70] BOXER, Charles, ***ob. cit.*** p. 27.
[71] NEWITT, Malyn. ***ob. cit***. p. 38.
[72] Ibidem, p. 38.
[73] THOMAZ, Fernanda. ***ob. cit***. p.105.

avanço da ocupação colonial ao longo do território, actualmente Moçambique, foram finalizados somente no princípio da década de 1920. No entanto, a consequente burocratização desse domínio nas áreas ocupadas exigia a expansão de diferentes mecanismos de controlo, que pudessem submeter todas as povoações de Moçambique"[74].

Para Betts, a "a administração da justiça apresentava-se como um dos critérios mais importantes para a manutenção da soberania do Estado colonial. Ainda que as potências europeias utilizassem da força para ocupar o continente africano, com as expedições militares, a justiça se constituía em um mecanismo essencial para a conservação dessa ocupação"[75]. Portanto, Thoma apregoa que "o controlo judicial, mas precisamente a lei, tornou-se um instrumento fundamental para a implementação do domínio colonial. Nessa sequência, antes mesmo de finalizar a ocupação do território, um número significativo de leis e instituições foram transferidas da metrópole e (re) criadas para as colónias"[76]. O autor ainda avança dissertando que "no processo de implementação do sistema jurídico colonial, sobretudo as questões consideradas criminais pelos colonizadores, pretendia-se impor os valores dos europeus sem preocupação com os costumes dos povos colonizados. Ou seja, usava-se o código penal e a estrutura judiciária portuguesa para determinar as penalidades a todos os indivíduos na colónia Moçambicana"[77].

O interesse em criar uma legislação específica para os povos colonizados de Moçambique e, ao mesmo tempo, codificar seus usos e costumes foi enfatizado na segunda metade da década de 1920, por João Belo, como afirma Thomas, ora citado. Com o fim da Primeira República, ainda na locução do autor, "houve uma significativa mudança na formulação de leis a serem aplicadas às suas colónias. Tal mudança foi iniciada pelo ministro das colónias João Belo, com a publicação em 1926 do Estatuto Político, Civil e Criminal dos Indígenas. Apesar de ter sido elaborado pelo poder central, o Estatuto reconheceu um princípio importante: a necessidade de codificação do direito indígena"[78].

O objectivo era facilitar a aplicação da justiça colonial aos Moçambicanos através da elaboração de um corpo legislativo para cada colónia face à sua multiplicidade sociocultural. O que era pouco mencionado nas discussões sobre a administração da justiça passou a receber uma atenção diferente. A justificativa consistia no respeito pelos usos e costumes desde que os direitos individuais de liberdade e existência não ferissem os princípios de humanidade e

[74] Ibidem, p.104.
[75] BETTS, Raymond F, ***ob. cit.***
[76] THOMAZ, Fernanda, ***ob., cit***., p.105.
[77] THOMAZ, Fernanda do Nascimento, ***ob. cit.*** pp.105-106.
[78] Ibidem, p.107

soberania portuguesa. Outro passo para essa mudança ocorreu três anos depois, quando foi aprovado o Regulamento dos Tribunais Privativos dos Indígenas, que determinava a criação de tribunais exclusivos para os africanos. Com esses tribunais, tentava-se conciliar o ofício dos administradores coloniais em colaboração com os chefes africanos, considerados como os conhecedores da lei especial do meio indígena, razão pela qual os informadores, seguros dos usos e tradições da tribo, podiam ser atendidos na administração da justiça.[79]

A mudança na década de 1920 reflecte o que o pesquisador Alan Smith enfatizou, ao afirmar que "apenas a partir desse período, com os primeiros passos para o Estado Novo, que algum projecto colonialista começou a ser aplicado para Moçambique. Antes disso, havia uma ausência de projecto colonial efectivo, que possibilitasse criar bases de análise de métodos e formas administrativas para as colónias"[80]. Ademais, "Portugal possuía precárias condições económicas para ampliar seu domínio, sustentar e explorar suas colónias, apoiando-se em investimentos ingleses e na própria concessão de parte do território às companhias majestáticas"[81]. Nos dizeres do Thomaz, "houve um processo de centralização e fortalecimento do Estado Português. A falta de iniciativa para aplicar métodos mais eficazes de exploração e controle dos povos colonizados passava a ser reavaliada pelo Estado Português a partir de 1926. Isso possibilitou uma reestruturação do sistema jurídico colonial, com propostas de políticas privativas a determinados africanos, cujo objectivo era impor maior controle e explorar a mão-de-obra"[82].

O esforço mais conhecido e paradigmático ocorreu na década de 1940, quando o jurista José Gonçalves Cota foi nomeado, pelo governador-geral, para dirigir estudos etnográficos sobre as populações de Moçambique, com o fim de elaborar um código penal e civil específico para os Moçambicanos. Com esse objectivo, "foi criada em 31 de Julho de 1941 a Missão Etognóstica da Colónia de Moçambique"[83]. Os trabalhos realizados pela missão resultaram na elaboração de um vasto material, produzido por Gonçalves Cota, sobre os costumes dos povos da colónia, do qual se podem listar os seguintes: Etnografia da Colónia de Moçambique; Mitologia e direito consuetudinário dos indígenas de Moçambique; Projecto do Regulamento dos Tribunais Indígenas da Colónia de Moçambique; Projecto definitivo do Estatuto do Direito

[79] NEWITT, Malyn, ***ob.cit***.
[80] SMITH, Alan K, ***The Idea of Mozambique and Its Enemies, c. 1890-1930***. Vol. 17, N.º 3. Journal of Southern African Studies, 1991.
[81] NEWITT, Malyn**.** ***ob. cit***.
[82] THOMAZ, Fernanda do Nascimento; p.106-107.
[83] COTA, Gonçalves, ***Projecto Definitivo do Código Penal dos Indígenas da colónia de Moçambique***, Imprensa Nacional de Moçambique, Lourenço Marques, 1946.

Privado dos indígenas; Projecto Definitivo do Código Penal dos Indígenas da Colónia de Moçambique.[84]

As duas primeiras obras mencionadas serviram de base para a elaboração dos projectos jurídicos de Gonçalves Cota.[85]. O discurso colonialista sustentava-se na concepção de que os "africanos" enquanto seres primitivos estavam mergulhados na preguiça e ociosidade. A acção civilizadora dos portugueses seria inserir os povos colonizados no trabalho colonial. Assim, justificava-se a exploração da mão-de-obra "africana".[86]

Diante do crescente interesse em controlar e explorar a mão-de-obra africana, as políticas de codificação dos usos e costumes dos povos colonizados permitiam ampliar e fortalecer o controlo colonial na região. Por esse motivo, acreditava-se que era fundamental o conhecimento dos costumes dos africanos. Neste ponto, reconheceu-se a dificuldade dos administradores coloniais em estabelecer parâmetros jurídicos para julgar os povos de Moçambique a partir do código português, uma vez que estavam mergulhados num significativo desconhecimento das culturas locais.[87]

> Afirmando-se que, as autoridades administrativas, em toda a Colónia, não ocultam o embaraço quase insuperável em que se vêm quando forçadas a julgar delitos precedidos ou acompanhados de circunstâncias imprevistas que lhes ditam, como juízes de facto, o dever de decidir de modo bem diverso daquele que o Código de 1886 lhes impõe, como juízes de direito também.[88]

Assim, compreendia-se que era necessário realizar um estudo analítico das principais instituições jurídicas e sociais, religiões e mentalidade de cada grupo étnico definido e diferenciado.[89] O trabalho etnográfico de buscar conhecer as sociedades africanas constituiu-se num método para elaborar códigos jurídicos específicos para os povos colonizados. Ao considerar os colonizados como seres humanos primitivos, acreditava-se também que viviam incrustados numa imobilidade ou num lento movimento evolutivo, devendo ser gratos à postura humanitária dos portugueses por se preocuparem em conhecer seus hábitos e costumes.[90] Esse processo de codificação possibilitava definir povos e configurar culturas, traduzindo relações dinâmicas e conflituosas em ideias homogeneizantes e imóveis, como se fossem provenientes de um costume antigo e intacto.[91]

---

[84] THOMAZ, Fernanda; ***ob. cit***. p.105
[85] COTA, Gonçalves; ***ob. cit***.
[86] COVANE, Luís António, ***As relações económicas entre Moçambique e a África do Sul, 1850-1964: acordos e regulamentos principais***, Núcleo Editorial da Universidade Eduardo Mondlaane. Maputo, 1989.
[87]COVANE, Luís António. ***ob. cit***.
[88] THOMAZ, Fernanda. ***ob. cit***. p.108
[89] COTA, Gonçalves. ***ob. cit***.
[90] Ibidem.
[91] THOMAZ, Fernanda. ***ob. cit***. p.105.

Gonçalves Cota procurou as similaridades de determinadas instituições existentes entre os "africanos" de Moçambique como forma de codificar seus costumes. Cota partiu do princípio de que as similaridades encontradas entre tais culturas eram fruto de coincidências, devido ao estado de evolução social. Assim, identificou-as a partir de sua organização familiar, acreditando que a sua evolução obedecia a leis fixas.[92] Deste modo, dividiu os povos de Moçambique em dois grandes grupos: o *matriarcal e o patriarcal*. Ainda que tenha sido o método encontrado pelo jurista para melhor identificar os costumes desses povos e seu estágio evolutivo, essa dicotomia, evidentemente, não dava conta das complexidades, o que permitiu Gonçalves Cota a apresentar a existência de um estágio intermediário entre os sistemas matriarcal e patriarcal.[93]

Esse esquema sobre os povos de Moçambique serviu para Gonçalves Cota identificar determinadas diferenças entre os "africanos". Procurava, portanto, os aspectos ligados ao direito privado português para comparar os grupos. Através de incursões em inúmeras povoações de Moçambique, com conversas com autoridades africanas, Gonçalves Cota colectou determinadas informações e procurou codificá-las. A finalidade desse trabalho era a interferência do mundo ocidental, mediante os instrumentos jurídicos específicos, para homogeneizar os colonizados, assimilando-os aos europeus. Embora também tenha sido o método que Gonçalves Cota utilizou para codificar os costumes das populações de Moçambique. Deste modo, o jurista elaborou os projectos do código civil e penal para os indígenas de Moçambique a partir do que era utilizado na metrópole.[94]

A expectativa de Gonçalves Cota e dos administradores coloniais reflectia a concepção evolucionista baseada na unilinearidade. Uma classificação racional foi criada através da generalização dos usos e costumes, de acordo com a perspectiva colonial assim como em relação a condição social dos povos colonizados. Esse pensamento estava muito próximo do evolucionismo do século XIX de Morgan.[95]

Foi a partir dessa concepção que Gonçalves Cota elaborou os seus projectos jurídicos. Embora apresentasse algumas alterações, o Projecto do Regulamento dos Tribunais Indígenas da Colónia de Moçambique apresentou uma estrutura da organização dos tribunais similar ao Regulamento dos Tribunais Privativos dos Indígenas de 1929. Uma das principais mudanças

---

[92] COTA, Gonçalves. ***ob. cit***.
[93] THOMAZ, Fernanda. ***ob. cit***. p.105.
[94] THOMAZ, Fernanda. ***ob. cit***. p.105.
[95] PEREIRA, Rui Mateus, ***Conhecer para Dominar: o Desenvolvimento do Conhecimento Antropológico na Política Colonial Portuguesa em Moçambique, 1926-1959***. Tese de Doutorado. Lisboa: Universidade Nova de Lisboa, 2005.

apresentadas pelo jurista foi a inclusão do direito de queixa do indígena contra as violências e os abusos das autoridades judiciais. Apesar do empenho de Gonçalves Cota, o Tribunal da Relação de Lourenço Marques, em 1950, reprovou o referido projecto, justificando que havia disposições deslocadas, repetidas, contraditórias e com conteúdo impreciso.

Tal como o projecto de regulamento, os demais projectos apresentados por Gonçalves Cota ao Tribunal da Relação de Lourenço Marques também foram reprovados. O projecto de código civil recebeu críticas veementes de alguns clérigos católicos em Moçambique.

A reprovação do Projecto Definitivo do Código Penal dos Indígenas da Colónia de Moçambique foi um caso ainda mais intrigante. Sua recusa pelo Tribunal da Relação ocorreu em virtude da base do projecto ter sido a doutrina criminal do Código Penal Português de 1886, orientado pelas escolas clássicas. Mesmo ao concordar que era urgente a aprovação de um Código Penal para os "africanos" de Moçambique, o presidente da Relação sugeriu que o projecto retornasse ao seu autor para fazer as devidas alterações. Informou também que esperava a opinião da mais alta competência em ciência penal da Universidade de Coimbra, o professor Beleza dos Santos, que estava elaborando o novo Código Penal Português, em substituição ao de 1886.[96]

O projecto do Código Penal de Gonçalves Cota foi criticado por não acompanhar as inovações teóricas no campo penal, a informação era: É certo que o Código de 1886 está atrasado em doutrina criminal em relação à escola positiva e muito à margem das correntes científicas modernas acerca da psique humana, sobretudo quanto à forma de interpretar os fenómenos da consciência, ao determinismo individual, ao conceito da responsabilidade.[97]

Ainda que essa assertiva estivesse correta, poder-se-ia alegar que o autor do Código Penal Português de 1886 também não estava actualizado. Isso porque as teorias clássicas do direito criminal já haviam recebido várias críticas da recém-formada, no final do século XIX, corrente do direito positivo. Gonçalves Cota observou que as obras dos principais teóricos do direito positivo foram publicadas antes da elaboração do Código Penal, a saber: Homem Delinquente, de Cesare Lombroso, em 1876; Critério Positivo da Criminalidade, de Rafael Garofalo, em 1878; Negação do Livre Arbítrio e responsabilidade e Sociologia Criminal, de Enrico Ferri, o primeiro em 1878 e o segundo 1880. Seria inocência acreditar em descuido tanto de Gonçalves Cota quanto de quem elaborou o código de 1886. Parece mais uma perspectiva

[96] THOMAZ, Fernanda. ***ob. cit***. p.105.
[97] COTA, Gonçalves. ***ob. cit***.

teórico-ideológica desses juristas do que uma desactualização sobre as discussões acerca do Direito Penal.[98]

A aclamada Escola Positiva surgiu na segunda metade do século XIX, juntamente com o desenvolvimento das Ciências Sociais que possibilitaram novas perspectivas nos estudos criminais, passando do abstracto individualismo para a defesa do corpo social frente à atitude do delinquente. Preocupava-se com a protecção da sociedade em relação ao criminoso, afastando-o dela como atribuição da penalidade. No que se refere à aplicação da pena, o livre arbítrio e a responsabilidade na acção, defendidos pelas escolas clássicas, perderam a importância, passou a valorizar o delito e o criminoso como patologias sociais. O carácter vingativo e retributivo foi substituído pela acção utilitarista. Na corrente positiva, o método mais usado era o indutivo, de modo que a sanção poderia ser aplicada antes da prática do crime, com definições preconcebidas.[99]-[100]

A finalidade da pena era a defesa social, uma vez que o crime passava a ser visto como um fenómeno natural e social. O exemplo mais conhecido foi o de Cesare Lombroso, fundador da Escola Penal Biológica. Influenciado pela teoria darwinista social, Lombroso defendia que a criminalidade era um atributo físico e hereditário, podendo ser detectável nas diferentes sociedades. Assim como na antropologia criminal, acreditou-se na possibilidade de capturar o criminoso antes que o crime fosse praticado. Alguns teóricos raciais do final do século XIX e princípio do XX basearam-se nesta concepção.[101]

Diante de toda essa crítica feita a Gonçalves Cota, o jurista respondeu de forma bastante inteligente e sútil. Alegou que havia uma miscelânea teórica que muitos acreditavam ter substituído a ideia de liberdade absoluta (voltada para a perspectiva de responsabilidade moral), defendida pelas escolas clássicas, pelo princípio de liberdade limitada, parcial, atenuada, que o jurista considerava de pseudo-harmonia entre o livre arbítrio e o determinismo. Portanto, Gonçalves Cota estava ciente de que as divergências, em relação ao seu projecto, não foram simplesmente escolásticas, o cerne da questão residia na definição da pena a ser tomada e na forma de certificar a segurança social.[102] Com todas essas justificativas, a reprovação do Código

[98] BITTENCOURT. ***ob. cit***.
[99]BARATTA, Alessandro, ***Criminologia Crítica e Crítica do Direito Penal: Introdução à Sociologia do Direito Penal***, Editora Revan, Rio de Janeiro, 2002.
[100] THOMAZ, Fernanda. ***ob. cit.*** p.105.
[101] SCHWARCZ, Lilia K. Moritz, ***Usos e abusos da mestiçagem e da raça no Brasil: uma história das teorias em finais do século XIX***, ***Afro-Ásia***, 1996.
[102] COTA, Gonçalves, ***ob. cit***.

Penal mais parecia representar um conflito político do que uma divergência, meramente teórico e prática.

O projecto foi contundentemente criticado por repetir a tipificação de crimes existentes no Código Penal Português. Na crítica, exigiu-se que Gonçalves Cota deveria apresentar somente o que fosse considerado pelos portugueses como uma anormalidade criminosa, os factos por eles (africanos) praticados que no seu meio social produzem acção nefasta diferente da produzida nos meios civilizados. Este facto deixa explícita a existência de um discurso contraditório do próprio presidente do Tribunal da Relação, visto que, por um lado censurava a influência directa do código de 1886 no referido projecto e, por outro, exigia que continuasse dependente desse código, apresentando somente o que fosse uma anormalidade para a sociedade ocidental.[103]

Ainda nesta perspectiva, Gonçalves Cota readaptou o projecto do Código Penal às ressalvas feitas pelo presidente do Tribunal da Relação, considerou a perspectiva do direito criminal positivo e atentou para as práticas criminais de maior anomalia para a sociedade ocidental. O novo projecto foi publicado, em 1946, por autorização do governador-geral de Moçambique, José Bettencourt. O objectivo era de divulgar esse material entre os administradores coloniais, antes mesmo de sua aprovação, para orientá-los e instruí-los no exercício de juízes dos tribunais privativos.[104]

Gonçalves Cota seguiu, detalhadamente, as indicações feitas pelo presidente do Tribunal da Relação. O interessante é que se falava em contemporização, em respeito pelos usos e costumes e em criação de leis específicas para as áreas coloniais, mas a maior parte dos projectos que indicavam esses caminhos estava marcada por interesses políticos obscuros. Há dúvidas sobre os reais desagrados das autoridades judiciais em relação aos projectos de Gonçalves Cota. Até mesmo a publicação do material escrito pelo jurista parece ter sido pouco aproveitada, somente uma parte do seu material chegou a ser publicada pela Imprensa Nacional de Moçambique, em 1944 e 1946.[105]

2.2.3. Segundo Projecto do Código Penal na Época Colonial

Sob orientação da escola positiva, o segundo projecto do Código Penal de Gonçalves Cota tinha seus princípios baseados na defesa social, com o intuito de prevenir e reprimir o

[103] Ibidem.
[104] THOMAZ, Fernanda. ***ob. cit.*** p.105.
[105] COTA, Gonçalves. ***ob. cit***.

crime ajustada à mentalidade e ao actual estado de civilização das populações nativas da Colónia de Moçambique. Assim sendo, a defesa social, a prevenção indirecta da criminalidade através da intimidação e a reeducação moral do delinquente no momento da correcção eram os principais objectivos da aplicação da pena aos criminosos africanos. Além disso, Gonçalves Cota seguiu as indicações do presidente do Tribunal da Relação, defendendo que o novo projecto do código penal voltaria somente para crimes existentes entre os "africanos", que não faziam parte do imaginário europeu. Ou seja, o direito criminal nas colónias contaria com a presença de dois códigos penais: um específico para os africanos; e outro a ser usado para os africanos, mas que também fosse utilizado na metrópole.

A decisão no campo do direito penal era considerar ambos os códigos, constando no primeiro código somente prescrições existentes entre africanos, tais como acções criminosas exclusivas aos costumes de determinados povos de Moçambique; que, por sua vez, seriam julgados à luz dos valores éticos e morais do Ocidente.[106]

Este novo projecto do código penal pautava por questões relacionadas com os crimes indígenas. Para efeito, definiam-se crimes indígenas como os delitos praticados pelos africanos, sob influência directa ou indirecta das crenças e superstições peculiares da raça negra e que levam o criminoso à persuasão da legitimidade do fim ou dos motivos que determinam o facto punível. Mediante isso, considerava-se culpado um delinquente corrigível, devendo, obrigatoriamente, ser educado para uma futura integração no meio social como um importante caminho ao combate das suas superstições.[107]

A responsabilidade criminal do culpado era avaliada através do que considerava a mentalidade atrasada da sua raça, a gravidade da acção criminosa e o nível de perigo que o criminoso representava para segurança social. A ignorância em relação à lei eximia o condenado da responsabilidade criminal, devendo ser esta provada e relacionada aos factos que passaram a ser instituídos como crime pelo código penal dos indígenas. No entanto, Gonçalves Cota fez algumas considerações em relação a determinados costumes locais, como se pode observar no artigo 17.º, que determinava que pudesse ser considerada como atenuante da penalidade a existência de ilusão sobre a criminalidade do facto, caso a finalidade do crime estivesse relacionada às crenças locais, sem ameaçar a ordem social.[108]

O jurista caracterizou as ofensas corporais e os homicídios cometidos contra os acusados de feitiçaria de crimes indígenas. Contudo, Gonçalves Cota determinou que tais casos não

[106] THOMAZ, Fernanda. ***ob. cit***. p.105.
[107] COTA, Gonçalves. ***ob. cit***.
[108] Ibidem.

poderiam ser considerados como atenuantes do delito, mesmo que fizessem parte do imaginário social dos Moçambicanos. Segundo o jurista, os povos colonizados consideravam a feitiçaria como uma ameaça a ordem social. Por esse motivo, o assassinato do suposto feiticeiro apresentava-se como uma acção legítima entre vários povos de Moçambique. Vale ressaltar que algumas sociedades africanas acreditavam que a pessoa acusada de feitiçaria havia proporcionado um mal a alguém (e a sua família), por isso era assentido, colectivamente, que esta pessoa deveria ser eliminada, considerando-se como um acto de justiça.[109] Neste contexto, o juiz deveria considerar que o culpado era educado por um senso moral próprio de seu meio cultural, desde que tal avaliação não afectasse a ordem social.

Ao pensar na perspectiva das escolas clássicas do Direito Penal (ou mesmo na escola ecléctica), no que concerne a responsabilidade criminal, as acções contra os curandeiros (das pessoas que identificavam os acusados de feitiçaria) diante da legitimidade social não se constituíam em crime, nem em intenção criminosa; consistiam apenas numa forma de exercício de legítima defesa. Tudo isto, porque nas teorias clássicas a responsabilidade penal era derivada da responsabilidade moral decorrente do exercício de livre arbítrio.

Diante disso, a nova concepção era de que essa posição trazia um resultado negativo na luta contra a criminalidade, mediante um sentimentalismo pecaminoso e absolutamente contrário ao fim utilitário do Direito Penal. Este defendia que o ideal seria afastar o agressor da sociedade por um tempo suficiente para reeducá-lo moralmente, a fim de preparar o seu espírito no sentido de se libertar das obsessões determinadas pela crença na feitiçaria. O tempo de reclusão do indivíduo deveria estar de acordo com a necessidade de eliminar tal crença através de um tratamento profilático.[110]

Por esse motivo decretou-se, nos artigos 28.º e 29.º, do projecto do código penal de Gonçalves Cota, a não aplicação de penas fixas aos Moçambicanos, constando somente o tempo de duração mínimo e máximo. O tempo da pena deveria ser decidido por uma comissão directiva das reclusões de acordo com as agravantes e atenuantes do crime, bem como com a classe do delinquente e com a sua conduta moral. A exclusão prisional, em caso de pena maior (crimes mais graves), deveria ser realizada em uma colónia prisional, fora da região onde residia o condenado. A pena correccional, com duração máxima de até dois anos, deveria ser cumprida em cadeia ou estabelecimentos públicos para esta finalidade. Os dois casos de prisão seriam

[109] THOMAZ, Fernanda. ***ob. cit***. p.105.
[110] THOMAZ, Fernanda. ***ob. cit***. p.105.

convertidos, automaticamente, por dias de trabalho enquanto não tivessem sido construídas as estruturas prisionais necessárias.[111]

Depois de todo esse esforço para adaptar às críticas apresentadas pelo presidente do Tribunal da Relação, Gonçalves Cota teve novamente seu projecto reprovado. Não se sabe quais foram os motivos para essa última reprovação. Diante desse arrazoado, vale ressaltar que todo o trabalho etnográfico de Gonçalves Cota esteve mais presente no projecto do estatuto do direito privado do que no do código penal. É bastante possível que as alterações feitas para o segundo projecto de código penal tenham sofrido transformações significativas quanto às informações colectadas em seu trabalho de campo. Assim sendo, as indicações sobre os usos e costumes dos povos de Moçambique projecto do código penal eram mais gerais e homogéneas do que em relação ao projecto do estatuto do direito privado. Os aspectos criminais extraordinários à cultura europeia apresentados no segundo projecto do código penal tinham mais um carácter homogeneizante das culturas africanas do que jurídico-etnográfico.[112]

As críticas e as reprovações dos projectos de Gonçalves Cota contradizem o crescente discurso de respeito e necessidade de codificação dos costumes dos "africanos". Um discurso que era pouco frequente durante a primeira República Portuguesa, adquiriu uma maior adesão a partir de 1926, quando se passou a aclamar pelo conhecimento da cultura dos povos colonizados. Sem dúvida, essa era uma agenda do novo governo português. Para implementar as políticas de controlo do Estado Novo, tornava-se necessário que se adequasse o sistema jurídico colonial às instituições de determinadas sociedades africanas.

Entretanto, as disputas políticas e os diferentes interesses colonialistas não permitiram que a proposta de codificação dos costumes dos africanos de Moçambique resultasse na aprovação de códigos jurídicos, em particular o Código Penal. O esforço em torno do que chamavam de respeito aos usos e costumes permaneceu, em grande parte, no discurso. Falavam em emergência de um código penal e estatuto de direito privado específico para os "africanos", mas inúmeras restrições abortaram a sua aprovação. Em suma, essa tentativa de adaptação do sistema jurídico colonial não correspondia com respeito às normas jurídicas dos povos colonizados. Apenas foram formas e mecanismos de controlo colonial através do sistema jurídico. Sabia-se que o exíguo conhecimento das áreas coloniais e a falta de recursos dificultavam o governo colonial alcançar seus objectivos.[113]

[111] COTA, Gonçalves. ***ob. cit***.
[112] THOMAZ, Fernanda. ***ob***. cit. p.105
[113] THOMAZ, Fernanda. ***ob***. cit. p. 105.

2.2.4. A Aplicação das Penas na Época Colonial em Moçambique

Com o processo de ocupação colonial do território moçambicano, entre o final do século XIX e o início do XX, e a consequente burocratização desse domínio, novas identidades foram criadas.[114] Portanto, preocupados em justificar o novo domínio e identificar a população a ser colonizada, vários códigos e regulamentos foram criados, estabelecendo as características dessa nova identidade subordinada ao poder colonial.

A primeira legislação colonial a definir o termo indígena foi o decreto de 27 de Setembro de 1894, que instituía a pena de trabalhos públicos a ser aplicada aos "indígenas das terras portuguesas em África". Designava-se "indígena" somente a pessoas nascida nas colónias, com pai e mãe "indígena", que não se "distinguissem pela sua ilustração e costumes do comum de sua raça".[115]

O principal objectivo desse decreto não era, simplesmente, a definição de um grupo de pessoas, mas saber a quem seria aplicada a pena de trabalhos públicos. Essa disposição legislativa isentava os africanos que possuíam alguma ascendência não "indígena" e que tivessem determinados comportamentos diferenciado dos demais daquela localidade. Era, de facto, a reconstrução de novas distinções e de novos grupos. Ainda que a ascendência e a origem espacial fossem importantes, as características socioculturais dos indivíduos tornaram-se fundamentais para definir quem poderia ser classificado como indígena.[116]

Isso percebe-se na definição do termo "indígena" apresentada no Estatuto Político, Civil e Criminal dos Indígenas de 1929, que considerava "indígenas os indivíduos da raça negra ou delas descendentes que, pela sua ilustração e costume, não se distingam do comum daquela raça; e não indígenas os indivíduos de qualquer raça que não estejam nestas condições.[117]

O decreto de 1894 demonstra o interesse do governo colonial em instituir leis diferenciadas para determinados grupos colonizados. A penalidade específica para os "indígenas" era uma forma de explorar a mão-de-obra africana, inserindo-a forçosamente na lógica colonial. Era o resultado da ineficácia das leis de mercado europeias nas colónias. O capitalismo no final do século XIX exigia a criação de uma força de trabalho estável que

---

[114] Ibidem. p. 314.
[115] MACAGNO, Lorenzo. ***Outros muçulmanos: Islão e narrativas coloniais,*** Imprensa de Ciências Sociais, Lisboa, 2006.
[116] ZAMPARONI, Valdemir. ***Da escravatura ao trabalho forçado: teorias e práticas***. 7ª Edição da Faculdade de Letras da Universidade do Porto, Africana Studia, Porto, 2004.
[117] THOMAZ, Fernanda Nascimento. ***ob. cit***. p.316

estivesse integrada no meio da produção colonial, o que não foi possível nas áreas colonizadas, porque as populações estavam voltadas para as suas próprias lógicas de trabalho. Por esse motivo o governo colonial procurou usar uma forma utilitarista e prática para dar conta de tais necessidades.[118]-[119]

Essa concepção foi reforçada, alguns anos depois, por um dos pensadores do colonialismo português em África, António Enes. Enes afirmava que Portugal deveria encontrar uma maneira de defender e obter a produção nas suas colónias mediante a imposição da obrigatoriedade do trabalho indígena.

O trabalho forçado foi a forma "de fazer com que este potencial produtivo desperdiçado se transformasse numa força de trabalho disponível e abundante para servir ao mercado".[120] Assim sendo, o trabalho prisional foi o primeiro recurso utilizado pelos colonizadores, aplicado através de multas de trabalho aos "indígenas" quando condenados por embriaguez, desordem, ofensa à moral e ao pudor, desobediência às autoridades e infracções dos regulamentos policiais. Durante a administração da Companhia do Niassa foram utilizados outros mecanismos violentos para adquirir braços para o trabalho forçado. Em 1894, a prisão foi substituída pela condenação ao trabalho forçado, enquanto, em 1903, o imposto a ser pago pelos "indígenas" passou a ser trocado por trabalho.

A utilização do trabalho forçado era a principal forma de penalização dos "indígenas", bastante distinta das exigências impostas aos "não indígenas". A virtude do trabalho era enaltecida nos discursos e nas práticas colonialistas. Sua recusa pelos "indígenas" levaria à punição por trabalho forçado, enquanto o "vadio não indígena será apresentado na secretaria do concelho a fim de se lhe obter emprego ou passagem para fora do território".

Justificava-se que a rejeição à venda da força de trabalho nas relações coloniais propiciava o surgimento de vícios, a miséria e a inveja, que juntas constituíam as mais importantes causas do crime. Aos poucos, o trabalho passava a ser considerado o oposto do crime; os criminosos cometiam delitos, principalmente o roubo, por que não possuíam qualquer disciplina de trabalho.[121]

Com efeito, isso demonstra que essa concepção se espalhou na sociedade urbana, especificamente entre os não indígenas, que passaram a entender que era fundamental

---

[118] ZAMPARONI, Valdemir. ***ob. cit.***

[119] OLIVEIRA Martins, J. P. ***O Brasil e as colónias portuguesas.*** 5 ed. Lisboa: Parceria António Maria Pereira Lived, 1920.

[120] THOMAZ, Fernanda Nascimento. ***ob. cit.*** p.317.

[121] VAZ, Ma ria João. ***Crime e sociedade: Portugal na segunda metade do século XIX***. Oeiras: Celta Editora, 1998.

reivindicar e apoiar medidas para combater o crime, devido à sua crescente ameaça, accionando e respaldando a acção do corpo policial e da autoridade colonial. Ademais, com essa concepção pautava-se pela ideia da incapacidade do indivíduo de lutar pela sobrevivência ou de obter alguma disciplina no trabalho, o que não lhe permitia acostumar-se do ritmo e das condições do trabalho assalariado. O interesse pela prevenção do crime e pela classificação de determinados comportamentos como crime tornava-se imperativo e justificado pela necessidade de reprimir tais comportamentos. Cada vez mais, a vadiagem e sócio passavam a ser considerados peculiares aos indígenas.[122]

Obviamente, as condições e os contextos haviam-se modificado nesse período de 20 anos, mas a criminalidade não estava directamente relacionada com os indígenas, nem mesmo era apresentada como resultado da recusa do trabalho. Havia, portanto, de forma crescente, uma linha muito ténue entre indígena e criminoso nas áreas urbanas coloniais. As condições económicas históricas dos africanos nas relações coloniais fizeram dos indígenas a população com menos recursos materiais. A ideia de preto e de pobre avizinhava-se da criminalidade, visto que o primeiro recusava o trabalho, mantendo-se pobre, estando apto ao crime.[123]

2.2.5. O Trabalho como Pena Exclusiva para o Indígena

As concepções veiculadas sobre "indígena", "civilização" e "trabalho" ajudavam a moldar uma legislação penal específica para os africanos moçambicanos. A identificação de grupos colonizados, a demarcação de superioridade e a importância da mão-de-obra propiciaram uma constante reflexão em relação à penalidade a ser aplicada aos "indígenas" na execução das leis coloniais. Não é coincidência que a primeira legislação colonial a definir "indígena" instituiu a utilização da pena de trabalhos públicos somente para esse grupo de africanos. Esse decreto foi uma iniciativa, em 1894, do comissário régio António Enes, que criticava a aplicação do Código Penal Português nas colónias sem nenhuma alteração. Para o efeito, António Enes foi um dos primeiros a apresentar e a defender uma reforma judiciária diferenciada para Moçambique, justificando que: Os regimes penais vão, por toda a parte, associando o trabalho á expiação, como meio de utilizar e moralizar o criminoso.[124]

O comissário régio não fazia crítica às doutrinas do Código Penal Português de 1886. A insatisfação era com a sua utilização em Moçambique, porque considerava que o uso de penas

[122] THOMAZ, Fernanda Nascimento. ***ob. cit***. p.320.
[123] Ibidem. p.321.
[124] THOMAZ, Fernanda Nascimento, ***disciplinar o "indígena" com pena de trabalho: políticas coloniais portuguesas em Moçambique***, 2012. p.322.

de prisão prisional não propiciaria o desenvolvimento moral e cultural dos indígenas. António Enes enfatizava que somente a prisão não causava intimidação, visto que a passividade e a inércia dos "indígenas" faziam com que estes se acostumassem rapidamente com a privação da liberdade.[125] António Enes defendia a existência de um sistema penal voltado para o trabalho público e correccional, como forma de inserir os indígenas na relação de trabalho colonial. Segundo o comissário régio, o período em que os infractores tivessem em trabalho prisional deveria ser um momento de correcção.

Na virada do século, um dos adeptos e impulsionadores das ideias de António Enes foi Manuel Moreira Feio, que considerava que a aplicação do mesmo regime penal português era bastante grave, porque acabava se constituindo como um prémio para os "indígenas". Entretanto, Manuel Moreira Feio discordava de António Enes sobre alguns mecanismos a serem utilizados para moralizar os "indígenas". Na sua obra, intitulada Indígenas de Moçambique, feio atentou para o desconhecimento de que a administração colonial tinha leis e costumes dos povos colonizados, ressaltando que o carácter jurídico das sociedades "indígenas" reflectia o seu estágio de evolução.[126]

Assim, devido ao atraso das sociedades africanas, o governo colonial não deveria contrariar as suas fantasias, mas procurar meios de civilizá-las. As leis e instituições dos povos colonizados seriam aceitas até que fosse amenizada a "sua crueldade" e unificada a sua forma legislativa na colónia. Ainda que discordassem do método a ser imposto pelo sistema jurídico português aos colonizados, Enes e Feio defendiam a não aplicação das mesmas penalidades determinadas no Código Penal Português para os indígenas moçambicanos.

As questões que envolviam a criminalidade poderiam ser baseadas nesse código, enquanto as penas deveriam ser excepcionais para os "indígenas", como parte do processo de civilização das áreas coloniais. E, de facto, durante todo o período colonial, a justiça penal nas colónias portuguesas baseou-se no código de 1886. Mesmo com a criação de tribunais coloniais específicos para julgar os "indígenas" e com as políticas de codificação dos costumes dos povos colonizados, a partir da segunda metade da década de 1920, utilizou-se o mesmo Código Penal. Somente na década de 1940 surgiu um projecto de Código Penal específico para os "africanos" de Moçambique, que não foi aprovado.[127]

No entanto, as penalidades foram sendo construídas de forma diferenciada para os "indígenas" ao longo do colonialismo em Moçambique, sempre baseadas em trabalhos públicos

[125] Ibidem. pp.322-323.
[126] THOMAZ, Fernanda Nascimento***. ob. cit***. pp.324-325.
[127] COTA, Gonçalves. ***ob- cit***.

ou correccionais. Em contrapartida, o uso da pena de trabalho em Portugal foi bastante criticado durante a segunda metade do século XIX. Justificava-se que não havia eficácia nessa forma de penalidade, porque ela não causava a intimidação e a moralização do "delinquente", proporcionando-lhe apenas o desprezo público. Por conseguinte, do Código Penal Português constavam somente as penas de prisão prisional e de degredo, ou seja, não havia penas de trabalho.[128]

O Código Penal Português de 1886 estava baseado na perspectiva do ressurgimento das ideias retributivas.[129] Era um retorno às teorias clássicas do Direito Penal, que, de uma forma geral, defendiam que a repreensão servia para revidar o mal ao infractor.

Neste contexto, o acusado não era considerado diferente das demais pessoas, como se a sua acção fosse predeterminada. Acreditava-se que o delito havia surgido mediante o livre arbítrio do indivíduo e não a partir de motivações patológicas. O autor do delito deveria ser responsabilizado pelas suas próprias acções como qualquer outra pessoa. Além disso, a pena era concebida como "instrumento legal para defender a sociedade do crime, criando, onde fosse necessário, um dissuasivo, ou seja, um contra motivação em face do crime. A principal preocupação era o delito, compreendido como um conceito jurídico, devido à violação do direito e do pacto social pelo seu autor, causando um distúrbio na sociedade".[130]

2.2.6. Aplicação do Código Penal Português em Moçambique

A aplicação do Código Penal Português em Moçambique foi marcada por uma contradição no que se referia à responsabilidade do acusado em relação ao delito cometido. O código determinava que a "ignorância" em relação à lei criminal portuguesa não isentava ninguém da pena a ser cumprida, nem mesmo tornava o acusado digno de atenuação. Nos tribunais coloniais existentes em Moçambique, o "grau de civilização" do acusado era enfatizado com frequência. Alegava-se que a responsabilidade criminal do acusado deveria seguir de acordo com o seu desconhecimento da lei metropolitana, o que era admitido somente para os chamados "indígenas". Essa diferenciação chegou a servir para amenizar a pena do acusado, embora a sua principal função fosse a de determinar quem deveria ser condenado a

[128] THOMAZ, Fernanda Nascimento. ***ob. cit***. p.326.
[129] BARREIROS, José António. ***As instituições criminais em Portugal no século XIX: subsídios para sua a história.*** Análise Social. Lisboa, vol. XVI, 1980.
[130] THOMAZ, Fernanda Nascimento. ***ob. cit***. pp.324-325.

pena de trabalho. Essa adaptação tinha um significado explícito: a aceitação da "ignorância dos indígenas" em relação à penalidade do código português.[131]

As críticas dos portugueses em relação ao uso de penas de trabalho para os condenados na metrópole faziam-se repercussões contrárias nas colónias. As penas de prisão correccionais e maiores, atribuídas de acordo com os delitos cometidos, foram substituídas pelas penas de trabalho correccional e trabalhos públicos em Moçambique. O condenado a pena de trabalho ficava sob a vigilância especial da polícia, devendo receber um salário fixo pelos serviços prestados. A pessoa não recebia seus vencimentos enquanto não terminasse o tempo da pena. Após cumprir a pena, o vencimento salarial deveria ser entregue ao trabalhador. O valor a ser recebido era um terço do salário vencido (bruto) e o restante ficava para o fundo do governo colonial.

A pena de trabalho correccional não poderia ser inferior a três dias e superior a dois anos, cumprida na própria área administrativa do tribunal que julgou o acusado. Já a pena de trabalho público, atribuída a delitos considerados graves, deveria ser cumprida entre 10 a 28 anos em região diferente daquela onde foi realizado o crime, podendo ser na colónia ou fora dela. As penas de trabalho público eram cumpridas nas colónias agrícolas, e somente as pessoas com idade superior a 60 anos e os portadores de alguma deficiência física estavam isentos. As mulheres e os menores de 14 anos deveriam cumprir pena nos hospitais, nas missões religiosas, estabelecimento de beneficência e ensino, entre outros.[132]

Apesar de os castigos corporais terem sido abolidos em Portugal, as penas disciplinares para os presos "indígenas" chegavam-se a usar castigos corporais como forma de repreensão. O estudo das acções e debates jurídicos nas colónias portuguesas indica que a principal finalidade das sanções criminais para os "indígenas" era a intimidação. Havia uma acentuada tendência à aplicação das penas máximas sempre que se tratava de "indígena". Os trabalhos mais pesados eram atribuídos aos condenados a trabalho público e os mais leves às pessoas que cumpriam pena de trabalho correccional.[133]

2.2.7. Principais Características e Políticas Penais Durante o Domínio Colonial

Durante o período colonial em Moçambique, que durou aproximadamente entre meados do século XIX e a independência do país, em 1975, as políticas penais eram estabelecidas pelas

[131] Ibidem. p.325
[132] THOMAZ, Fernanda Nascimento. ***ob. cit***. pp.325-326.
[133] Ibidem, p.326.

potências coloniais que controlavam a região, principalmente por Portugal.[134] Algumas das principais características e políticas penais durante esse período incluíam:

- Código Penal Colonial: Moçambique era regido pelo Código Penal Colonial português, que foi aplicado na colónia. Esse código definia os diferentes tipos de crimes e as respectivas penalidades.
- Discriminação Racial: durante o domínio colonial, havia uma clara discriminação racial nas políticas penais. As leis, muitas vezes, tratavam os indivíduos africanos de forma desigual em relação aos colonos europeus. A punição por crimes cometidos por africanos era frequentemente mais severa.
- Criminalização da Resistência: a resistência ou oposição ao domínio colonial eram frequentemente criminalizadas e duramente reprimidas. Líderes e activistas anticoloniais eram perseguidos e muitas vezes submetidos a prisão, tortura e execução.
- Prisões Coloniais: durante o período colonial, foram estabelecidas várias prisões em Moçambique para abrigar os infractores das leis coloniais. Essas prisões muitas vezes tinham condições precárias, e os prisioneiros eram submetidos a tratamentos desumanos.
- Trabalho Forçado: o trabalho forçado era uma prática comum durante o domínio colonial em Moçambique. Prisioneiros e pessoas consideradas rebeldes eram frequentemente enviados para campos de trabalho forçado, onde eram obrigados a realizar trabalho pesado sob condições difíceis.[135]

É importante ressaltar que as políticas penais e as práticas durante o domínio colonial eram altamente injustas e opressivas para a população moçambicana. Após a independência, o país introduziu reformas significativas no seu sistema legal e de justiça para superar as injustiças do passado colonial.[136]

2.2.8. Pós-Independência

2.2.8.1. O Direito Penal Moçambicano no Pós-Independência

Mesmo antes da divisão da ordem jurídica nos diferentes ramos, que actualmente é, em geral, adoptada, o Direito Penal alcançara, pela sua especificidade, relevante e autónoma

[134] NEWITT, Malyn. **ob. cit.** p. 42.
[135] ANDERSON, Benedict. ***Nação e consciência nacional***, Companhia das Letras, São Paulo, 2008, p. 274
[136] NEWITT, Malyn. ***ob. cit.*** p. 46

posição. A complexidade da legislação moderna não tinha equivalência, em tempos mais recuados, mas o Direito Penal foi, em toda a sua evolução, o direito titular dos interesses fundamentais do homem em sociedade e da coexistência social.[137]

Enquanto os diferentes ramos do Direito se distinguem pelo conteúdo e natureza das relações sociais que os regulam, o Direito Penal distingue-se de todos os demais pela natureza da sanção que comina. Crime e Pena são e sempre foram, em toda sua evolução, os polos fundamentais do Direito Penal. Sendo o Crime, uma espécie do acto ilícito e a Pena uma espécie de sanção jurídica.[138]

No entanto, após a independência de Moçambique, ocorrida em 25 de Junho de 1975, houve uma série de mudanças no sistema legal do país, tendo iniciado, a partir daquele momento, a vigorar a primeira constituição, com a designação de Constituição da República Popular de Moçambique, um texto com 73 artigos. Com efeito, tais mudanças afectaram, para além da constituição, todo o sistema jurídico do actual país independente, como é o caso do sistema jurídico-penal, pois o novo Governo Moçambicano tencionava estabelecer um sistema jurídico-penal que reflectisse a soberania e os valores do país, ao mesmo tempo em que promovesse a justiça social e a protecção dos direitos humanos.[139]

A seguir, com a conquista da Independência Nacional, o discurso político sobre a unidade ganha uma nova dinâmica, pois a unidade de todo o povo em torno da vanguarda da FRELIMO era uma exigência para o sucesso das tarefas de reconstrução nacional, na luta contra os reaccionários, contra o tribalismo e o obscurantismo. Os grupos dinamizadores, unidades de base de Frente de Libertação, assumem um papel extraordinariamente e importante na triagem política dos inimigos da revolução, na mobilização popular em torno da FRELIMO e na forja do homem novo.[140]

Essencialmente, o sistema comportava elementos do direito estatuário herdado do colonialismo, elementos traduzidos pela prática da aplicação da justiça nas zonas libertadas durante a luta armada e certamente alguns elementos de direito costumeiro. A transformação do sistema de justiça penal em Moçambique correspondeu à necessidade de adequar as instituições jurídicas e o próprio direito herdado do colonialismo à nova concepção de Estado

[137] FERREIRA, Manuel Cavaleiro De. ***Direito Penal Português***, ***Parte Geral I***, 2ª Edição, Editorial Verbo, Lisboa/São Paulo, 1982. p.9.
[138] Ibidem, p. 9.
[139] GOUVEIA, Jorge Bacelar, ***Direito constitucional de Moçambique,*** ASPRINT Editora, 2015, p.237
[140] MARCOS, Rui Manuel de Figueiredo, ***A história do Direito e o seu ensino na Escola de Coimbra***, p.25

de Democracia Popular, no quadro da definição do Direito como expressão do poder da classe dominante.[141]

Assim, logo após a independência, o governo moçambicano, liderado pela Frente de Libertação de Moçambique, promulgou uma série de leis e decretos para abolir as leis colónias e estabelecer um novo marco legal. Essas leis eram conhecidas como legislação do período de transição e tinham como objectivo principal romper com as normas e práticas jurídicas do período colonial.[142] Em relação ao Direito Penal, durante esse período de transição, foram adoptadas medidas para revogar ou modificar as leis penais coloniais que eram consideradas injustas ou incompatíveis com a nova ordem jurídica do país.[143]

Por conseguinte, durante os primeiros anos pós-independência, houve desafios significativos para o país, incluindo a reconstrução e a reorganização das instituições estatais. O processo de desenvolvimento de um sistema jurídico independente e abrangente, incluindo o direito penal, foi um empreendimento gradual que se estendeu ao longo do tempo.[144] A construção de um sistema jurídico independente evolveu a formação de juristas, a capacitação de profissionais de direito, criação de tribunais e órgãos judiciais, além do desenvolvimento de um sistema de aplicação da lei e de justiça criminal eficaz. Esses esforços foram essenciais para estabelecer um sistema jurídico funcional que pudesse garantir a justiça, segurança e a protecção dos direitos dos cidadãos.[145]

2.2.8.2. Moçambique: Direito Penal ou Direito Criminal

O primeiro problema a que nos propomos discutir, logo à partida, é a designação do Direito Penal ou Direito Criminal em Moçambique. A denominação Direito Penal não é a única que tem designado ou designa este ramo do Direito. Atentos a sua própria evolução e anteriormente a codificação, em Portugal como em outros países, prevalecia a denominação Direito Criminal. Porém, com a publicação dos códigos penais durante o séc. XIX, em quase todos os países, generalizou-se a denominação de Direito Penal. Em França manteve-se na doutrina, indiferentemente, uma e outra das expressões indicadas.[146]

Porém, comecemos com o Direito Comparado. Na Alemanha, a denominação Direito Penal é quase unânime desde os princípios do Século XIX. Na Itália, sucede outro, tanto as

[141] MIRABETE, Fabbrini Julio. ***ob. cit***. p.159.
[142] Ibidem.
[143] Ibidem.
[144] PALMA, Maria Fernanda, ***Direito Constitucional Penal, 1ª edição***, Almedina, 2011, p.15
[145] PALMA, Maria Fernanda. ***ob. cit***. p.15.
[146] FERREIRA, Manuel Cavaleiro. ***ob. cit***. p.20.

obras mais importantes dos clássicos, como Carmignani, Carrara e Ferri, optaram pela denominação Direito Criminal, sem embargo de, por exemplo, Petrocelli e Battaglini adoptarem a designação Direito Penal. Na França, a nomenclatura Direito Penal não goza do mesmo trato que na Alemanha. Os termos *Droit Criminel e Droit Pénal* se utilizam indistintamente.[147]

A prestigiosa Professora Teresa BELEZA, sobre este debate, introduz as suas Lições, afirmando que: A questão não tem importância nenhuma. A única argumentação que se pode fazer em relação a isto é que, se se fala em Direito Penal, pode ser que se considere que ficam de fora as medidas de segurança e, portanto, isso não abrangeria essa zona importante do Direito Penal, se se fala em Direito Criminal, se está a usar o crime no sentido subjectivo, pleno de crime, do qual uma pessoa é culpada, também se está a deixar de fora os actos dos inimputáveis e, portanto, também as medidas de segurança.[148]

No entanto, a designação Direito Penal é recente, pois, surge com rigor, com o aparecimento dos Códigos Penais a partir do Século XIX, embora tivesse sido utilizada, pela primeira vez, no Século XVIII. Já a designação Direito Criminal é mais clássica, historicamente anterior e goza de uma brilhante tradição jurídica, embora perdendo, na actualidade, o seu uso.[149] A designação Direito Criminal é mais compreensiva, na medida em que abrange não só o crime, mas também as respectivas consequências jurídicas.

A denominação Direito Penal assenta unicamente na ideia de pena, deixando de lado as chamadas medidas de segurança. O debate designatório gira em torno de dois elementos nucleares: o crime e a pena. Ora, neste debate todo, importa a nossa escolha que se encontra delimitada pela opção do legislador moçambicano.

Assim, em Moçambique, a designação mais acertada é a de Direito Penal, em obediência ao Código Penal, aprovado pela Lei n.°35/2014, de 31 de Dezembro ou ao Código Penal de 2019. Não existe, em nenhum país, Direito Penal senão em face daquilo que é o direito positivo e a lei que cria o crime e as respectivas consequências jurídicas.[150]

Um conjunto de argumentos a favor da designação Direito Penal: é o conteúdo e o fim fundamental do sistema de normas. O objecto do nosso estudo é a repressão do delito mediante a pena. O termo pena, por efeito da linguagem tradicional e comum é suficientemente idóneo para distinguir as sanções estabelecidas para verdadeiros delitos de outras sanções para outras

[147] MACIE, Albano. ***ob. cit***., p.1.
[148] Ibidem, p.2.
[149] MACIE, Albano***. ob. cit***., p.1.
[150] Ibidem. p.2.

formas de ilícito, cuja disciplina jurídica não é compreendida pelo Direito Penal. O Código Penal conhece delitos e suas penas e só de modo complementar as medidas de seguranças.[151]

Ainda neste âmbito, alguns criminalistas discordavam por motivos de fundo, da manutenção da denominação de Direito Penal. Este, após a inclusão no seu âmbito das medidas de segurança, não poderia ser designado com referência exclusiva a natureza da sanção penal, e antes seria mais congruente com o seu objecto designá-lo com referência ao crime, que tanto seria o fundamento da pena como o sintoma ou pressuposto da perigosidade criminal. Entretanto, não é assim. O crime, enquanto facto ilícito penal, é sempre um facto culpável, este, como sintoma ou pressuposto de perigosidade, pode ser aquilo que a doutrina italiana chama de facto de crime, pois que senão trata de facto culpável.[152]

A natureza essencial dos dois actos, um humano porque é livre e racional e o outro acto do homem, em que não se verificam tais qualidades, é totalmente diversa e não podem verdadeiramente reconduzir-se a uma unidade que não seja formal. De maneira que parece poder manter-se a ambivalência dos dois vocábulos que sucessiva ou concomitantemente se tem utilizado. Portanto, em Moçambique, a razão de preferência passa a situar-se no uso mais comum e sobretudo na designação da legislação codificada como Código Penal, motivo de se preferir a designação Direito Penal.[153]

2.2.8.3. Influência do Sistema Jurídico Português no Direito Penal Moçambicano

O sistema jurídico português exerceu uma significativa influência no desenvolvimento do Direito Penal moçambicano, devido ao passado histórico e à relação colonial entre Portugal e Moçambique. Durante o período colonial, que durou até a independência de Moçambique em 1975, o sistema jurídico português foi aplicado no país.[154] Assim, como resultado, o Direito Penal moçambicano foi inicialmente moldado pelo sistema jurídico português, que se baseia no sistema romano-germânico. Várias leis portuguesas foram adoptadas em Moçambique e serviram como a base para o Código Penal e outras legislações penais moçambicanas.

Após a independência, Moçambique passou a adoptar um sistema jurídico próprio, mas a influência do direito penal português permaneceu presente. Embora o país tenha feito esforços para desenvolver a sua legislação penal de acordo com as necessidades e realidades locais,

---

[151] Ibidem, p.3.
[152] FERREIRA, Manuel Cavaleiro. ***ob. cit*** p.20.
[153] FERREIRA, Manuel Cavaleiro De. ***ob. cit***. pp.20-21.
[154] SANTOS, Maria Emília Madeira, ***A África e a instalação do sistema colonial (c. 1885-1930): III Reunião Internacional de História de África***, Centro de Estudos de História e Cartografia Antiga, Lisboa, 2000, p. 153

muitos princípios e conceitos jurídicos do sistema português ainda são reconhecidos e aplicados em Moçambique. Além disso, a cooperação entre Portugal e Moçambique no campo do direito penal continua a existir. Existem acordos de cooperação bilateral que abrangem áreas como a extradição de criminosos, assistência judicial mútua e formação de profissionais jurídicos. Essa colaboração também contribui para a influência contínua do sistema jurídico português no direito penal moçambicano.[155]

No entanto, é importante ressaltar que Moçambique tem trabalhado para adaptar a sua legislação penal às suas próprias necessidades e realidades sociais. O país tem promovido reformas legais e actualizações no Código Penal e em outras leis penais, levando em consideração as especificidades culturais e sociais moçambicanas.

2.2.8.4. Mudanças Legislativas e Institucionais Após a Independência de Moçambique

Após a independência de Moçambique, em 1975, houve várias mudanças legislativas e institucionais no âmbito penal do país.[156] O novo governo moçambicano estabeleceu um sistema jurídico que reflectisse os valores e as necessidades da nação recém-independente. A seguir, estão algumas das principais mudanças ocorridas nesse contexto:

- Constituição de 1975: após a independência, Moçambique adoptou uma nova Constituição, que estabeleceu os princípios fundamentais do Estado e os direitos e deveres dos cidadãos. A Constituição de 1975 previa a igualdade perante a lei, a protecção dos direitos humanos e garantias fundamentais, bem como a proibição da tortura e de tratamentos cruéis, desumanos ou degradantes.[157]
- Código Penal de 1981: em 1981, foi promulgado um novo Código Penal em Moçambique, substituindo o antigo código colonial português. O Código Penal de 1981 estabeleceu os crimes e as penas aplicáveis no país. Ele abordou questões como homicídio, roubo, tráfico de drogas, corrupção, entre outros delitos, de acordo com os princípios do novo Estado moçambicano.
- Reformas institucionais: após a independência, ocorreram reformas institucionais significativas no sistema de justiça criminal de Moçambique. O país estabeleceu instituições e órgãos responsáveis pela aplicação e administração da justiça, como o

[155] ANDERSON, Benedict. ***ob. cit.*** p. 271.
[156] CABAÇO, José Luís, ***Moçambique: Identidade, colonialismo e libertação***, Editora UNESP, São Paulo, 2009, p. 58.
[157] Ibidem, p. 59.

Ministério Público, a Polícia da República de Moçambique (PRM) e os tribunais. Essas instituições foram fundamentais para garantir a ordem, a segurança e a administração da justiça em Moçambique.

- Lei de Amnistia de 1992: em 1992, foi aprovada uma lei de amnistia que visava promover a reconciliação nacional e encerrar o período de guerra civil que assolou o país. Essa lei concedeu amnistia a vários crimes políticos e militares cometidos durante o conflito, como uma medida para promover a paz e a estabilidade.
- Reformas posteriores: ao longo dos anos, Moçambique passou por várias revisões e actualizações legislativas no âmbito penal. O país tem alinhado a sua legislação com as normas internacionais de direitos humanos e combate ao crime, bem como enfrentar desafios emergentes, como o combate à corrupção, ao terrorismo e ao tráfico de drogas.[158]

2.2.8.5. Adaptação do Direito Penal às Necessidades e Valores Moçambicanos

Após a independência, em 1975, o sistema jurídico moçambicano passou por um processo de adaptação, incluindo o Direito Penal, com vista a atender às necessidades e valores moçambicanos. A adaptação do Direito Penal foi parte de um esforço mais amplo de construção de um sistema legal e de justiça que reflectisse a identidade e as aspirações do povo moçambicano.[159]

Uma das principais mudanças foi a abolição da pena de morte. A pena de morte foi considerada contrária aos valores humanitários e à visão de justiça do novo Estado moçambicano. Em vez disso, o país adoptou a pena máxima de prisão perpétua como a mais grave sanção penal.[160]

Outra adaptação importante foi a incorporação de princípios do direito consuetudinário moçambicano no sistema jurídico. O direito consuetudinário é baseado em tradições, costumes e práticas locais, e sua inclusão no Direito Penal moçambicano buscou fortalecer a identidade cultural do país e garantir uma maior legitimidade e aceitação do sistema legal. Além disso, houve uma revisão e actualização das leis penais existentes para adequá-las à realidade moçambicana pós-independência. Com efeito, isso envolveu a revisão dos tipos penais, das penas aplicáveis e das medidas de prevenção e ressocialização dos infractores. O objectivo era

[158] NEWITT, Malyn. ***ob. cit.*** p. 47.
[159] CABAÇO, José Luís. ***ob. cit***. p. 67.
[160] NEWITT, Malyn. ***ob. cit.*** p. 51.

garantir que as leis penais reflectissem as necessidades específicas do país, levando em consideração questões sociais, económicas e culturais.

No contexto da justiça criminal, foram realizados esforços para fortalecer as instituições responsáveis pela aplicação da lei e pelo sistema judicial. Foram promovidas iniciativas para capacitar policiais, promotores e juízes, melhorar a investigação criminal e garantir um julgamento justo. Também houve investimentos na construção e manutenção de infra-estruturas judiciais para tornar a justiça mais acessível a todos os moçambicanos.

É importante ressaltar que as adaptações no Direito Penal moçambicano, após a independência, reflectem o contexto e os valores específicos do país. Cada nação tem as suas próprias necessidades e desafios e a adaptação do direito penal é um processo contínuo, sujeito a revisões e ajustes para garantir que as leis sejam eficazes e estejam em conformidade com os valores e as necessidades em constante evolução da sociedade moçambicana.[161]

2.2.8.6. O Direito Penal Moçambicano no Período Socialista

Segundo os ensinamentos de Aprah, "o período socialista em Moçambique ocorreu durante o governo do Partido FRELIMO (Frente de Libertação de Moçambique) desde a independência do País, em 1975, até meados dos anos 1990. Durante esse período, o país adoptou uma ideologia socialista e marxista-leninista, buscando estabelecer uma sociedade mais igualitária e promover o desenvolvimento socioeconómico"[162]. Após a independência, o governo socialista liderado pela FRELIMO implementou uma série de políticas e medidas baseadas nos princípios socialistas. Essas políticas incluíam a nacionalização de indústrias, terra e recursos naturais, bem como a implementação de programas de reforma agrária e colectivização da produção (vide o artigo 6 da CRPM). O governo também promoveu a educação e a saúde públicas, buscando melhorar o acesso aos serviços básicos (vide o artigo 15 da CRPM).

No entanto, é importante notar que o período socialista em Moçambique também foi marcado por desafios e conflitos, como a guerra civil que ocorreu entre o governo socialista e a Resistência Nacional Moçambicana (RENAMO), um movimento de oposição armada apoiado por governos estrangeiros. A guerra civil, que durou de 1977 a 1992, teve um impacto

[161] Ibidem. p. 53.
[162] APPIAH, Kwame Anthony, ***Na casa de meu pai: a África na filosofia da cultura***, Contraponto, Rio de Janeiro, 1997, p. 69.

significativo na sociedade moçambicana e na implementação das políticas socialistas.[163] A partir da década de 1990, Moçambique passou por mudanças políticas e económicas, adoptando políticas de economia de mercado e abertura ao investimento estrangeiro.

Ainda em Aprah, "essa transição resultou em ajustes significativos nas políticas e no sistema legal do país, afastando-se em certa medida do socialismo e abraçando uma economia mais liberal. No geral, o período socialista em Moçambique teve um impacto considerável na formação do país, influenciando o sistema legal, as políticas sociais e económicas, bem como a estrutura política e administrativa. Embora Moçambique tenha passado por mudanças substanciais desde então, algumas das influências desse período ainda podem ser observadas na sociedade moçambicana actual"[164].

2.2.8.7. Influência do Socialismo no Direito Penal Moçambicano

A influência do socialismo no direito penal moçambicano pode ser observada principalmente durante o período em que Moçambique era governado pelo Partido FRELIMO (Frente de Libertação de Moçambique, *que governa até hoje*), que adoptou princípios socialistas e marxistas-leninistas em sua ideologia política. Durante esse período, que compreendeu a independência do País em 1975 até meados dos anos 1990, houve uma influência significativa do socialismo na legislação penal e na justiça criminal moçambicana.

Uma das principais mudanças promovidas pelo governo socialista de Moçambique foi a reestruturação do sistema legal e judiciário do país para se adequar aos princípios socialistas. Foi promulgada uma nova Constituição em 1975, que estabeleceu a base para a legislação penal e criminal do país. Essa Constituição incluía direitos e garantias fundamentais, como o princípio da legalidade, a presunção de inocência e o direito a um julgamento justo.

Além disso, o governo socialista implementou políticas e medidas para promover a justiça social e a igualdade, o que teve reflexos no sistema penal. O Código Penal moçambicano foi actualizado durante esse período, reflectindo uma abordagem mais progressista em relação aos crimes contra a propriedade e crimes económicos. Por exemplo, foram introduzidas leis que visavam combater o enriquecimento ilícito e a corrupção, crimes considerados prejudiciais ao ideal socialista de igualdade e justiça.[165]

---

[163] BELLUCCI, Beluce, ***Economia contemporânea em Moçambique: sociedade linhageira, colonialismo, socialismo, liberalismo***, EDUCAM, Rio de Janeiro, 2007, p. 119.
[164] Ibidem, p. 121.
[165] HEDGES, David. ***História de Moçambique: Moçambique no auge do colonialismo***, UEM, Maputo, 2004, p. 121.

No entanto, é importante ressaltar que, após o fim do governo socialista e a adopção de políticas económicas mais liberais na década de 1990, o sistema legal e judiciário de Moçambique passou por mudanças significativas. Essas mudanças reflectiram uma transição para um sistema mais orientado para o mercado e com influências jurídicas de diferentes origens, incluindo o direito anglo-saxão e o direito romano-germânico.[166]

Actualmente, o sistema penal moçambicano é influenciado por uma combinação de princípios socialistas e direito ocidental, com o Código Penal de 2014, por exemplo, reflectindo essa fusão de influências. Embora o socialismo ainda possa ser considerado como uma influência em certos aspectos do direito penal moçambicano, é importante reconhecer que o país passou por mudanças significativas nas últimas décadas, e outras influências também moldaram o sistema jurídico actual.

2.2.8.8. Princípios e Políticas Penais durante o Período Socialista

No início do período socialista, houve uma ênfase na reforma do sistema de justiça criminal em Moçambique. A nova legislação penal foi promulgada, e o sistema legal foi baseado no princípio de que a justiça criminal deveria ser usada como uma ferramenta para transformar a sociedade e promover a justiça social. Alguns dos princípios e políticas penais adoptados durante esse período incluíam:

- Justiça social: o sistema penal foi orientado para alcançar a justiça social e a igualdade económica. O objectivo era combater a desigualdade e a exploração através da punição de crimes económicos e da redistribuição de riqueza.[167]
- Reforma prisional: houve uma ênfase na reforma das instituições prisionais. O sistema penitenciário foi visto como uma oportunidade para a reabilitação e a transformação dos infractores. Programas de trabalho e educação foram implementados nas prisões para preparar os indivíduos para a reintegração na sociedade.[168]
- Enfoque na prevenção: houve uma ênfase na prevenção do crime por meio da educação e do fortalecimento da comunidade. Foram implementados programas de conscientização e educação para promover uma sociedade justa e igualitária.[169]

[166] Ibidem. p. 123.
[167] HEDGES, David. ***ob. cit.*** p. 127.
[168] SOUTO, Amélia Neves de, ***Caetano e o ocaso do Império: Administração e Guerra Colonial em Moçambique durante o Marcelismo (1968 – 1974),*** Edições Afrontamento, Porto, 2007, p. 100.
[169] HEDGES, David. ***ob. cit*** p.128.

- Participação popular: o sistema de justiça criminal foi projectado para ser acessível e envolver a participação popular. Os tribunais populares foram estabelecidos para permitir que os cidadãos participassem activamente na administração da justiça.
- Luta contra o colonialismo: durante o período socialista, Moçambique estava em guerra contra as forças coloniais da Rodésia (actual Zimbabué) e da África do Sul, que apoiavam a Resistência Nacional Moçambicana (RENAMO). Nesse contexto, houve uma forte repressão aos crimes considerados contra-revolucionários ou colaboracionistas.[170]

No entanto, é importante observar que as políticas penais e os princípios durante esse período não foram uniformemente aplicados em todo o país, e houve relatos de abusos e violações dos direitos humanos cometidos pelo Estado. Após o fim do período socialista, Moçambique passou por uma transição para uma economia de mercado e uma democracia multipartidária, e houve mudanças significativas nas políticas penais do país. [171]

2.2.8.9. Reformas Legais e Constitucionais e sua Influência do Direito Penal

Para alinhar o direito penal com os princípios democráticos e os padrões internacionais de direitos humanos, muitos países, incluindo Moçambique, passaram por reformas legais e constitucionais. Essas reformas visam fortalecer o Estado de Direito, garantir a protecção dos direitos fundamentais e promover um sistema de justiça criminal mais justo e equitativo. Algumas das áreas-chave que geralmente são abordadas durante essas reformas incluem:

- Constituição e direitos fundamentais: muitas vezes, as reformas começam com uma revisão da constituição para garantir que ela estabeleça claramente os direitos e liberdades fundamentais dos cidadãos. Isso pode incluir a inclusão de disposições relacionadas aos direitos humanos, separação de poderes, garantias de um julgamento justo e proibição da tortura e tratamento cruel, desumano ou degradante.[172]
- Código Penal: o Código Penal é revisto para assegurar que os tipos de crimes e suas penalidades estejam em conformidade com os princípios democráticos e os padrões internacionais de direitos humanos. Isso pode envolver a descriminalização de certas condutas, a revisão das penas para torná-las proporcionais e a introdução de medidas alternativas à prisão.

[170] Ibidem. p. 128.
[171] SERRA, Carlos***, História de Moçambique***, Livraria Universitária, Maputo, 2000, p. 117.
[172] GOUVEIA, Jorge Bacelar, ***Direito Constitucional de Moçambique***, Editor IDLP, Lisboa, 2015, p. 199.

- Protecção dos direitos dos acusados: Reformas são realizadas para fortalecer as garantias processuais e os direitos dos acusados. Isso pode incluir a presunção de inocência, o direito a um julgamento justo, o acesso a um advogado, a proibição de detenção arbitrária e a protecção contra a auto-incriminação.
- Abolição da pena de morte: Muitos países que buscam alinhar seu direito penal com os padrões internacionais de direitos humanos optam por abolir a pena de morte, considerada uma violação do direito à vida e uma punição cruel e desumana.[173]
- Prevenção da tortura e maus-tratos: São implementadas medidas para prevenir a tortura e os maus-tratos nos sistemas de justiça criminal. Isso pode envolver a criação de mecanismos de monitoramento independentes, treinamento de agentes da lei sobre direitos humanos e a responsabilização de pessoas que cometem esses abusos.
- Cooperação internacional: Países em processo de reforma legal também buscam cooperar com organismos internacionais, como as Nações Unidas e a Organização dos Estados Americanos (OEA), para receber assistência técnica, compartilhar boas práticas e promover a harmonização com os padrões internacionais de direitos humanos.[174]

Essas são apenas algumas das áreas-chave que podem ser abordadas durante as reformas legais e constitucionais para alinhar o Direito Penal com os princípios democráticos e os padrões internacionais de direitos humanos. É importante destacar que cada país tem seu próprio contexto e desafios específicos, e as reformas devem ser adaptadas às necessidades e realidades locais.

2.2.9. Mudanças nas Leis Penais e nos Procedimentos Judiciais

Algumas mudanças nas leis penais e nos procedimentos judiciários foram:

- Constituição de 1990: a Constituição de Moçambique, adoptada em 1990, estabeleceu os princípios fundamentais para o sistema legal do país. Ela garante direitos fundamentais, como a igualdade perante a lei, o direito a um julgamento justo e o princípio da presunção de inocência.[175]
- Código Penal: o Código Penal de Moçambique foi revisto em 2014, com o objectivo de modernizar as leis penais e alinhá-las com os padrões internacionais de direitos humanos. Essa revisão incluiu a descriminalização de algumas

[173] SOUTO, Amélia Neves de. ***ob. cit.*** p. 109.
[174] SOUTO, Amélia Neves de. ***ob. cit***. p. 111.
[175] MIRANDA, Jorge; ***Manual de Direito Constitucional***, Tomo IV, 4.ª Edição, Coimbra Editora, 2008, p. 197.

condutas, a reformulação de tipos criminais e a introdução de penas alternativas à prisão.[176]

- Reformas na justiça penal: foram realizadas reformas nos procedimentos judiciais para fortalecer as garantias processuais e os direitos dos acusados. Isso incluiu a promoção de um julgamento justo, a implementação do princípio da oralidade, a agilização dos processos, a melhoria da investigação criminal e o reforço da independência do poder judicial.
- Protecção de direitos humanos: Moçambique é signatário de diversos tratados e convenções internacionais de direitos humanos. As mudanças nas leis penais e nos procedimentos judiciais têm procurado garantir a protecção dos direitos humanos, proibindo a tortura, tratamento cruel e degradante e assegurando o respeito aos direitos das vítimas e testemunhas.[177]
- Combate à corrupção: Moçambique tem implementado medidas para combater a corrupção, um desafio significativo no país. Isso incluiu a aprovação de leis anticorrupção mais rigorosas e o fortalecimento de instituições responsáveis pela investigação e punição de crimes relacionados à corrupção.
- Cooperação Internacional: Moçambique tem procurado cooperação com organizações internacionais e parceiros bilaterais para fortalecer o sistema legal e judicial do país. Isso envolve a troca de informações, assistência técnica e apoio na capacitação de profissionais do sistema de justiça.

É importante ressaltar que as mudanças nas leis penais e nos procedimentos judiciais em Moçambique são um processo contínuo e estão em constante evolução. O país enfrenta desafios na implementação efectiva dessas reformas, incluindo a necessidade de capacitação de profissionais do sistema de justiça, o acesso equitativo à justiça e a garantia da aplicação consistente das leis em todo o País.

2.3. Evolução dos Códigos Penais em Moçambique

2.3.1. Código Penal Aprovado pelo Decreto de 16 de Setembro de 1886

Na tentativa de estabelecer um sistema jurídico-penal que reflectisse a soberania e os valores do país no estado em que este se encontrava, verificasse a adopção do Código Penal de

[176] CISTAC, Gilles et. al, ***Contributo Para o Debate Sobre a Revisão Constitucional***, Faculdade de Direito da UEM, Maputo, 2004, p. 48.
[177] CISTAC, Gilles et. al. ***ob. cit***. p. 50.

1886, conhecido como o Código Penal português, este código esteve em vigor em Moçambique durante o período de domínio colonial português. Este código reflectia os valores e as normas jurídicas da época e estabelecia os crimes e suas sanções correspondentes aplicáveis no contexto colonial.[178]

Ora, a adopção e desenvolvimento do Código Penal português de 1886, envolveu a revisão e adaptação das normas existentes, levando em consideração as necessidades e os valores do país pós-colonial.[179] A entrada em vigor do Código Penal de 1886 marcou uma mudança significativa no sistema legal moçambicano. Esse código reflectia as aspirações e os objectivos do país pós-independência, buscando estabelecer um sistema jurídico baseado na justiça social, na protecção dos direitos humanos e na soberania nacional.

No entanto, o Código Penal de 1886 nada mais era do que uma compilação da legislação penal ou, se preferirmos, uma vasta reforma do Código Penal de 1852, foi este diploma que regeu o Direito Penal moçambicano logo após a independência.[180]

2.3.1.1. Estrutura do Código Penal de 1886

O Código Penal estrutura-se em dois Livros, sendo ao todo composto por 486 artigos. O Primeiro Livro, relativo à Parte Geral e o Segundo à Parte Especial. Desta forma, o Código Penal de 1886 compreende: o primeiro livro, relativo à parte Geral, é composto por IV títulos, dos quais:

O primeiro título, com a epígrafe dos "Crimes em Geral e dos Criminosos", composto por IV capítulos, nomeadamente: as "Disposições Preliminares", previsto no capítulo 1 do Código Penal de 1886 (art. 1 a 7 do CP); enquanto só o capítulo 2, com epigrafe "Da Criminalidade" (arts. 8 a 18 do CP), "Dos Agentes do Crime" abordado no capítulo 3 (arts 19 a 25 do CP), e o último, relativo à "Responsabilidade Criminal (arts. 26 a 53 do CP).

O segundo título, com a epigrafe "Das Penas e seus Efeitos", com dois capítulos, sendo o primeiro "Das Penas e Das Medidas de Segurança" (arts 54 a 73 do CP). O segundo capítulo e último aborda sobre o "Efeito das Penas" previstos nos arts 74 a 83 do CP.

O terceiro título, relativo à "Aplicação e Execução das Penas", com seis capítulos, dos quais: o da "Aplicação das Penas em Geral" previstos nos arts 84 a 90 do CP; O segundo capítulo fala da "Aplicação das Penas Quando há Circunstâncias Agravantes ou Atenuantes"

[178] SERRAO, Joaquim Veretissimo, ***História de Portugal***, Vol I, 2ª edição, Editorial Verbo, Lisboa, 1990, p.122
[179] Ibidem. p.122.
[180] MARCOS, Rui Manuel de Figueiredo, ***A história do Direito e o seu ensino na Escola de Coimbra***, p.25

(arts 91 a 99 do CP); enquanto isso o terceiro capítulo é referente "Da Aplicação das Penas, nos Casos de Reincidência, Sucessão e Acumulação de Crimes, Cumplicidade, Delito Frustrado e Tentativa" (arts 100 a 105 do CP); o quarto capítulo cinge-se "Da Aplicação das Penas em Alguns Casos Especiais" (arts 106 a 112 do CP); o quinto capítulo é atinente "Da Execução das Penas e Medidas de Segurança" (arts 113 a 124 do CP) e, por último, o capítulo sexto relativo à "Extinção da Responsabilidade Criminal (arts 125 a 128 do CP).

Na parte geral, encontra-se previsto o quarto título, sendo o último com a epígrafe "De Disposições Transitórias (art. 129 do CP).

No livro II, Parte Especial, com VII Títulos, desdobrando-se em:

O primeiro título, relativo aos "Crimes Contra a Religião do Reino e dos Cometidos por Abuso de Funções Religiosas", sendo integrado por dois capítulos referentes aos "Crimes Contra a Religião (arts 130 a 135 do CP); o segundo "Dos Cometidos por Abusos de Funções Religiosas (arts 136 a 140 CP).

O título II, À Crimes Contra a Segurança do Estado, desdobrando-se em III capítulos, nomeadamente: "Os crimes Contra a Segurança Exterior do Estado (arts 141 a 151 do CP); o segundo capítulo relativo "A crimes que Ofendam os Interesses do Estado em Relação às Nações Estrageiras (arts 152ª 162 do CP); e o último capítulo relativo aos "Crimes Contra a Segurança Interior do Estado" (arts 163 a 176 do CP).

O título III, relativo à "Crimes Contra a Ordem e Tranquilidade Pública", com V capítulos, sendo o primeiro com epigrafe "Reuniões Criminosas, Sedição e Assuada (arts 177 a 180 do cp); o segundo relativo a "Injúrias E Violência Contra Autoridades Públicas, Resistência e Desobediência" (181 a 189); o terceiro relativo a "Tirada e Fugida de Presos e dos que não Cumprem as suas Condenações" (arts 190 a 196 do CP); o capítulo seguinte relativo a " que Acolhem Malfeitores" (arts 197 a 198 do CP); o quinto referente "Dos Crimes Contra o Exercício dos Direitos Políticos" (arts 199 a 205 do CP), o sexto, com epigrafe "Falsidades" (arts 206 a 245); o sétimo capítulo é referente a Violação das leis sobre inumações e da violação de túmulos e dos crimes contra a saúde pública (arts 246 a 252); enquanto isso, o oitavo capítulo é sobre as Armas, caças e pescarias, defesas (arts 253 a 254 do CP); enquanto isso o nono capítulo é relativo a "Dos Vadios e Mendigos, e das Associações de Malfeitores (arts 256 a 263 do CP); capítulo décimo relativo a "Jogos de Lotarias, Convenções Ilícitas sobre Fundos Públicos e Abusos em Casas de Empréstimos sobre Penhores (arts 264 a 274 do CP); capítulo 11, a epígrafe é "Do Monopólio e Contrabando (arts 275 a 281 do CP), capítulo 12 relativo a

"Associações Ilícitas" (arts 282 a 283 do CP) e o capítulo 13 refere-se aos "Crimes dos Empregados Públicos no Exercício de suas Funções" (arts 284 a 389 do CP).

O título IV, relativo aos "Crimes Contra as Pessoas", com cerca de V capítulos, aborda, no essencial, "Os Crimes Contra a Liberdade das Pessoas" (primeiro capítulo), cujas normas estão assentes nos arts 328 a 335; o segundo capítulo é "Dos Crimes Contra o Estado Civil das Pessoas" (arts 336 a 348 do CP); o terceiro capítulo relativo aos "Crimes Contra a Segurança das Pessoas, os Crimes Contra Honestidade" (arts. 349 a 389); o capítulo quarto relativo aos "Crimes Contra Honestidade" (arts 390 a 406 do CP) e Crimes Contra a Honra, Difamação, Calunia e Injuria", previstos no capítulo V (arts 407 a 420 do CP).

O título V, com a epígrafe "Dos Crimes Contra a Propriedade", é composto por quatro capítulos, dos quais: "Do Furto e do Roubo e da Usurpação de Coisa Imóvel (primeiro capítulo), arts 421 a 446 do CP); o segundo "Das Quebras, Burlas e outras Defraudações (arts 447 a 460 do CP); o terceiro é relativo aos que "Abrem Cartas Alheias ou Papéis e da Revelação dos Segredos (arts 461 a 462 do CP); por último, o quarto capítulo é relativo a "Incêndio e Danos" previstos nos arts 463 a 482 do CP).

E para finalizar, encontramos os títulos VI e VII, sendo o primeiro com epígrafe "Da Provocação Pública ao Crime" (previsto no art. 483 do CP) e o segundo "Das Contravenções de Polícias", previstos nos arts 484 a 486 todos do CP).

2.4. O Código Penal de Aprovado pela Lei n.° 35/2014, de 31 de Dezembro

A expressão Lei Penal compreende tanto o Código Penal, aprovado pela lei n.°35/2014, de 31 de Dezembro, bem como também o conjunto de leis extravagantes que completam o Código Penal, as leis especiais, e outras que constituem o chamado Direito penal secundário.[181] O Código Penal constitui a lei geral penal, a qual é aplicada às matérias reguladas por outras leis penais, salvo se tais disposições penas o afastarem. A Lei Penal é a principal fonte de Direito Penal, sendo dela que nascem os crimes e as respectivas sanções jurídicas.

O Código Penal de 2014 foi uma revisão abrangente do Código Penal de 1886. Essa revisão teve como objectivo modernizar a legislação penal de Moçambique, levando em consideração as mudanças sociais e legais que ocorreram desde a promulgação do Código Penal anterior.[182]

[181] MACIE, Albano. ***ob. cit***. p.46

[182] IESE, ***Desafios para Moçambique 2017***, Disponível em: https://www.iese.ac.mz/wp-content/uploads/2018/05/Desafios2017.pdf, acesso: 25/06/2023, as 14: 21mn

O Código Penal de 2014 reflectiu uma série de mudanças sociais, políticas e jurídicas que ocorreram desde a década de 1950. Houve uma evolução significativa na compreensão dos direitos humanos e das garantias individuais, bem como uma ênfase crescente na prevenção e ressocialização. Uma das principais mudanças foi a incorporação de penas alternativas ao encarceramento para certos crimes, como medidas socioeducativas, prestação de serviços à comunidade e penas restritivas de direitos. O código também introduziu medidas mais específicas para combater crimes económicos, como corrupção e lavagem de dinheiro.[183]

Segundo Macie, "com a proclamação da independência Nacional e da Constituição, a 25 de Junho de 1975, novos princípios estruturantes conduziram a alterações ao Código penal. No entanto, com as alterações constitucionais de 1990 e de 2004 denunciam a obsolescência e o desajuste do Código Penal aprovado pelo Decreto de 16 de Setembro de 1886, à realidade política, social, cultural e económica"[184]. Com efeito, tal facto contribui para a necessidade de reformar o Código Penal de 1886, com vista a garantir o gozo de direitos e liberdades ao cidadão e a sua conformação com as hodiernas concepções da dogmática penal.[185] Assim, à coberto da Resolução n° 46/2010, de 28 de Dezembro, a Assembleia da República mandatou a Comissão dos Assuntos Constitucionais, Direitos Humanos e de Legalidade, 1ª Comissão, para apresentar os instrumentos adequados para atingir o desiderato da revisão do Código Penal.

Ocorre lembrar que o sistema penal moçambicano tem a sua origem no Direito colonial português, através do Código Penal aprovado no longínquo ano de 1886, que recebeu materialmente o Código de 1852, embora com algumas alterações que foram sendo introduzidas. Portanto, a Lei n.°35/2014, de 31 de Dezembro, constitui um novo Código Penal e o primeiro elaborado pelo Legislador moçambicano.

Nas palavras do Macie, "toda a sociedade moçambicana era unânime em considerar aquele Código de obsoleto e desajustado para a realidade actual. Aliás, o desajustamento daquele instrumento é, desde logo, notório com a proclamação da Independência Nacional, em 1975, momento em que várias disposições do mesmo cederam perante as normas e princípios constitucionais" [186]. O autor referenciado afirma ainda que "com a aprovação da Constituição de 1990, e consequente introdução do Estado de Direito Democrático e de Justiça social aumentaram-se as contestações ao Código Penal, por este não ser mais capaz de se integrar nas

[183] PAUL, Leandro, ***Noções Sobre História do Direito Clássico e Moçambicano***, S/Ed. Edições FDS, Maputo, 2018, p. 95.
[184] MACIE, Albano. ***ob. cit***. p.47.
[185] Ibidem. p.47
[186] MACIE, Albano. ***ob. cit***. p.47.

mudanças políticas e sociais operadas"[187]. Este desajustamento, em conformidade com Macie[188], acabou por afectar o gozo pleno dos direitos, liberdades e garantias individuais dos cidadãos, consagrados na Constituição de 1990, ao substituir o antigo código colonial.

A sistematização oitocentista e tradicional arrancava da ideia da primazia do Estado. Neste sentido, as generalidades das codificações começavam por definir os crimes contra o Estado. Mas é evidente que a própria sistemática não pode ser vista como axiologicamente neutra; ela é reveladora, entre outras coisas, do lugar que se concede ao homem no mundo normativo, princípio que obteve clara consagração constitucional. Pelo pouco que já se disse, mas pelo muito que ficou implícito no que concerne ao carácter axiologicamente prioritário do homem, não se deve estranhar que a parte especial abra justamente pelos crimes contra as pessoas (título I).

Estabelece-se, deste modo, um corte radical, altamente salutar com o sistema tradicional que só vem dignificar a cultura e a doutrina portuguesas. Mas esta compreensão, no desenvolvimento do seu fio lógico, leva a remeter os crimes contra o Estado (título V) para lugar derradeiro. Facilmente se apreenderá que esta sistematização tem de ser olhada pelo seu lado positivo. Quer dizer, ela representa a afirmação da dignidade da pessoa, mas não significa o menoscabo dos interesses e valores que o Estado assume e sintetiza em determinado momento histórico.[189]

O Código Penal, aprovado pela Lei n.º 35/2014, de 31 de Dezembro, introduziu novos tipos penais, estabeleceu penas actualizadas e incorporou os princípios fundamentais do direito penal moçambicano, como legalidade, irretroactividade da lei penal, proporcionalidade e humanidade.

Macie alude que "a entrada em vigor do novo código marcou uma ruptura com o passado colonial e permitiu que Moçambique desenvolvesse um sistema jurídico mais adequado às suas necessidades. O Código Penal de 2014 revolucionou a técnica legislativa de 1886, quanto á estruturação básica do articulado. Neste contexto, na parte especial, os crimes contra a vida e integridade física tem preferência sobre os crimes contra o património e contra o Estado"[190].

2.4.1. Estrutura do Código Penal de 2014

[187] Ibidem, p.47.
[188] Ibidem,p.47.
[189] Ibidem. p.48.
[190] Ibidem. p.48.

O Código Penal[191] estrutura-se em dois Livros, com 567 artigos, antecedidos de uma Lei Preambular, dedicando-se a primeira à parte geral e o segundo à parte especial. Assim o respectivo Código Penal compreende: uma Lei Preambular que procede à aprovação do Código e integra dispositivos que estabelecem regras atinentes ao direito *inter temporal*, revogando disposições de algumas leis por incorporação e consagrando garantias relativas à promoção da soltura e libertação de presos, bem como a instituição do salário mínimo da função pública como critério para a determinação do valor de multas decorrentes das medidas penais e criminais previstas no Código Penal.

Relativamente ao texto do Código Penal, salienta-se no Livro Primeiro, na parte geral, dois títulos:

O primeiro título, com quatro capítulos, sendo o primeiro com "Disposições Gerais" (arts 1 do 10 do CP); o segundo dedicado à criminalidade (arts 11 a 19 do CP); o terceiro capítulo, relativo a agentes do crime (arts 20 a 26 do CP) e o quarto referente a responsabilidade criminal, previstos nos arts 27 a 56 do CP).

O segundo título tem 8 capítulos: o primeiro relativo a "Penas e medidas criminais" arts 57 a 104 do CP); o segundo aborda sobre efeitos das penas (arts 105 a 109 do CP); o terceiro relativo a Aplicação das Penas Privativas da Liberdade e de Medidas Criminais (arts 110 a 115 do CP); o quarto capítulo assenta na aplicação das penas quando há circunstancias agravantes ou atenuantes (arts 116 a 124 do CP); o quinto fala das Aplicação das Penas em Casos Especiais (arts 125 a 131 do CP); Enquanto isso, o sexto capítulo com a epigrafe " Aplicação das Penas em Alguns Casos Especiais (arts 132 a 138 do CP); o sétimo capítulo fala da "execução das Penas e Medidas de Segurança" previstos nos arts 139 a 150 do CP; o último capítulo (Oitavo), é relativo a "Extinção da Responsabilidade Criminal" previsto nos arts 151 a 154 do CP).

No livro II "Parte Especial", com dez títulos, o Primeiro (Crime contra as Pessoas) é composto por XII capítulos, destacando-se:

O primeiro " Crimes Contra Vida" (arts 155 a 169 do CP); o segundo dedicado à "Crimes contra a Integridade Física" (arts 170 a 181 do CP); o terceiro capítulo, relativo a "Disposições Aplicáveis aos Capítulos Antecedentes" (arts 182 a 189 do CP) e o quarto é referente a "Duelo em Participação em Rixa", previstos nos arts 190 a 195 do CP.

Enquanto isso, o quinto fala dos "Crimes contra a Liberdade das Pessoas" (arts 196 a 204 do CP); o sexto capítulo tem a epígrafe " Crimes Contra o Estado das Pessoas" (arts 205 a 217

[191] Cfr., Lei n.º35/2014, de 31 de Dezembro, que *aprova* ***o Código Penal***.

do CP); o sétimo capítulo fala de “Crimes contra a Liberdade Sexual” previstos nos arts 218 a 228 do CP; o oitavo é relativo a “ A Crimes Contra a Honra ” previsto nos arts 229 a 245 do CP; o nono capítulo aborda sobre “ Violência Doméstica” (arts 155 a 169 do CP); assim como “Crimes contra a Integridade Física” (arts 245 a 257 do CP); o décimo capítulo é relativo a “Crimes contra a Reserva da Vida privada” (arts 258 a 261 do CP); o décimo primeiro capítulo é referente a “Violação das Leis sobre as Inumações, Violação dos Túmulos”, previstos nos arts 262 e 263 todos do CP., e por último, o décimo segundo capítulo, fala dos “Crimes contra a Saúde Pública” (arts 264 a 268 do CP).

O segundo título (Crimes contra o Património em Geral), é composto por dois capítulos: o primeiro “Crimes contra a Propriedade (arts 269 a 294 do CP); o segundo dedicado à Falências, Burlas e outras Defraudações (arts 295 a 315 do CP).

O terceiro título tem três capítulos: o primeiro relativo a Crimes Informáticos (arts 316 a 323 do CP); o segundo referente a Agravação, Atenuação e Perdão dos Crimes Informáticos (arts 324 a 325 do CP), enquanto isso, o terceiro fala das Crimes contra a Liberdade das Pessoas (arts 196 a 204 do CP).

O quarto título, com epigrafe “Crimes de Perigo Comum”, é composto por três capítulos. O primeiro fala do “Incêndio e Danos” previstos nos arts 327 a 348 do CP; o segundo é relativo a Crime contra a Ambiente” previsto nos arts 349 a 357 do CP e, por fim, o terceiro capítulo aborda sobre “Armas, Caça e Pesca (arts 358 a 361 do CP).

O quinto título, com três capítulos: o primeiro é referente a Crimes contra a Segurança Exterior do Estado (arts 362 a 372 do CP); o segundo capítulo é relativo a Crimes que Ofendem os Interesses do Estado em relação as Naçôes Estrangeira (arts 373 a 382 do CP); enquanto isso, o terceiro capítulo é referente a Crimes contra a segurança no Interior do Estado, previstos nos arts 383 a 400, todos do CP.

O sexto título, é composto por oito capítulos: primeiro é relativo a “Reuniões Criminosas, Sedição e Assuada” (arts 401 a 404 do CP); o segundo é dedicado à Injúrias e Violências contra as Autoridades Públicas, Resistência e Desobediência (arts 405 a 420 do CP); o terceiro capítulo é relativo a Tirada e Fugida de Presos e dos que não cumprem as suas Condenações (arts 421 a 428 do CP); o quarto é referente a Acolhimento de Malfeitores, previstos nos arts 429 a 430 do CP; o quinto fala dos Ilicitos Eleitorais (arts 431 a 457 do CP); o sexto capítulo com a epigrafe “ Associação de Malfeitores (arts 458 a 459 do CP); o sétimo capítulo fala da “Lotarias, Convenções ilícitas sobre Fundos Públicos e Abusos em casas de Empréstimos sobre Penhores,

previstos nos arts 460 a 466 do CP; o oitavo e último capítulo deste título, é relativo a "Açambarcamento, Especulação e Contrabando " previsto nos arts 467 a 476 do CP.

O sétimo título tem três capítulos, nomeadamente: o primeiro referente a Crimes cometidos no Exercício de Funções (arts 477 a 500 do CP); o segundo capítulo é relativo a Crimes de Corrupção, Peculato e Concussão (arts 501 a 519 do CP); enquanto o terceiro capítulo é referente a "Disposições Gerais", previstos nos arts 520 a 522, todos do CP.

O oitavo título, com cinco capítulos: o primeiro é da "Falsidade de Moeda, Bancos Nacionais e de alguns Títulos do Estado" (arts 523 a 533 do CP); o segundo dedicado à Falsificação dos Escritos (arts 534 a 547 do CP); o terceiro capítulo, relativo a "Falsificação dos Selos, Cunhos e Marcas (arts 548 a 552 do CP); o quarto referente é referente a Nomes, Trajos, Empregos e Títulos Supostos ou Usurpados (arts 553 a 557 do CP); e por último, o quinto capítulo, é relativo a epigrafe " Falso Testemunho e outras Falsas Declarações perante Autoridade Pública" (arts 558 a 564 do CP).

O nono título (Provocação Pública ao Crime), preceituado no art. 565 do CP.

Por último, o décimo título é reservado a epígrafe "Contravenções de Polícias" com duas normas, previstas nos artigos 566 e 567 (coimas).

2.4.2. Críticas ao Código Penal de 2014

O Código Penal, aprovado pela Lei nº 35/2014, de 31 de Dezembro, trouxe grandes inovações ao introduzir novos tipos legais de crimes, alterações na redacção e nas molduras penais e incorporação de matérias que constavam da legislação avulsa. Sobretudo, adoptou o movimento da descriminalização e a preferência por penas não privativas de liberdade à pena de prisão, passando a situar no Homem a sua dimensão máxima.

Entretanto, por razões de fundo, traduzidas na limitação à abordagem dos seus valores axiológicos e a necessidade de tratamento jurídico particular, nomeadamente em sede de articulação entre normas substantivas e processuais específicas, passaram a justificar a afectação sistemática dos lapsos e omissões por uma vicissitude legal.

2.5. Código Penal Aprovado pela Lei nº 24/2019 de 24 de Dezembro

O Código Penal de 2019, em comparação com o de 2014, pode não ter sofrido mudanças tão substanciais, uma vez que apenas alguns anos se passaram entre as duas versões. No entanto, foram feitas alterações pontuais para aprimorar o sistema penal com base em experiências práticas e necessidades emergentes. Por exemplo, pode ter havido ajustes nas penas, definições

de crimes e procedimentos penais para melhorar a eficácia e a justiça do sistema. Outrossim, o novo Código Penal, como apregoa Souza[192], traz nas suas normas uma "tendência cada vez mais universalizante para a afirmação dos direitos do homem como princípio basilar das sociedades modernas, bem como o reforço da dimensão ética do Estado, imprimem à justiça do estatuto do primeiro garante da consolidação dos valores fundamentais reconhecidos pela comunidade, com especial destaque para a dignidade da pessoa humana".

Alude ainda Souza, que "ciente de que ao Estado cumpre construir os mecanismos que garantam a liberdade dos cidadãos, o programa do Governo para a justiça, no capítulo do combate à criminalidade, elegeu como objectivos fundamentais a segurança dos cidadãos, a prevenção e repressão do crime e a recuperação do delinquente como forma de defesa social"[193].

O autor acima referenciado destaca que "um sistema penal moderno e integrado não se esgota naturalmente na legislação penal. Num primeiro plano, há que destacar a importância da prevenção criminal nas suas múltiplas vertentes, relativamente a operacionalidade e articulação das forças de segurança e, sobretudo, a eliminação de factores de marginalidade através da promoção da melhoria das condições económicas, sociais e culturais das populações e da criação de mecanismos de integração das minorias"[194].

Paralelamente, o combate à criminalidade não pode deixar de assentar numa investigação rápida e eficaz e numa resposta atempada dos tribunais. Na verdade, mais do que a moldura penal abstractamente cominada na lei, é a concretização da sanção que traduz a medida da violação dos valores pressupostos na norma, funcionando, assim, como referência para a comunidade[195]. Finalmente, a execução da pena revelará a capacidade re-socializadora do sistema com vista a prevenir a prática de novos crimes.

O autor alude ainda que "o Código Penal, não sendo o único instrumento de combate à criminalidade, deve constituir o repositório dos valores fundamentais da comunidade. As molduras penais mais não são, afinal, do que a tradução dessa hierarquia de valores, onde reside a própria legitimação do direito penal"[196]. Ainda na visão do autor "a alteração de qualquer diploma legislativo, em particular no domínio da legislação penal substantiva, deve sempre ter subjacente o objectivo de adequá-lo à nova realidade face aos desafios colocados pelos factos do dia-a-dia. Isto é, actualiza-lo face ao contexto ditado pelas circunstâncias em que for aprovado, seja introduzido novos tipos legais de crime, seja descriminalizando algumas

[192] SOUZA, Elísio de, ***Código Penal Moçambicano comentado***, Plural Editora, Maputo.
[193] Ibidem.
[194] HUNGRIA, Nelson, FRAGOSO, Heleno Cláudio, ***Comentários ao Código Penal***, 4ª Edição, Lisboa, p.53.
[195]SOUZA, Elísio de. ***ob. cit***..
[196] ibidem

condutas que não exijam intervenção do direito penal para protecção dos bens jurídicos tidos como essências para a sobrevivência da sociedade"[197].

Para o Souza[198]. "o Código Penal de 1886 permanece válido na sua essência. A experiência da sua aplicação ao longo de mais de uma década tem demonstrado, contudo, a necessidade de várias alterações com vista não só a ajustá-lo melhor à realidade mutável do fenómeno criminal como também aos seus próprios objectivos iniciais, salvaguardando-se toda a filosofia que presidiu à sua elaboração e que permite afirmá-lo como um código de raiz democrática inserido nos parâmetros de um Estado de direito".

Entre os vários propósitos que justificam a revisão, como destaca Húngria[199], afiguram-se: a necessidade de corrigir o desequilíbrio entre as penas previstas para os crimes contra as pessoas e os crimes contra o património, propondo-se uma substancial agravação para as primeiras. Assume-se ainda a importância de reorganizar o sistema global de penas para a pequena e média criminalidade com vista a permitir, por um lado, um adequado recurso às medidas alternativas às penas curtas de prisão, cujos efeitos criminais são pacificamente reconhecidos, e, por outro, concentrar esforços no combate à grande criminalidade.

2.5.1. Estrutura do Código Penal de 2019

O Código Penal de 2019 estrutura-se em dois Livros, com 449 artigos. Dos dois livros, o primeiro é referente à Parte Geral que se traduz, essencialmente, no estabelecimento de princípios e conceitos fundamentais do Direito Penal, abordando temas essências para a compreensão do sistema penal e servindo de base para a aplicação das normas penais, e o segundo livro é reservado à Parte Especial. Assim, relativamente ao texto do Código Penal, salienta-se no Livro Primeiro, uma Parte Geral, com três títulos:

O primeiro título, com epigrafe "Garantias e Aplicação da Lei Penal" é de capítulo único (Disposições Gerais) (arts 1 a 9 do CP).

O segundo título (Criminalidade e Agentes do Crime), é constituído por cinco capítulos, nomeadamente: primeiro capítulo relativo a "Pressupostos da Punição" (arts 10 a 14 do CP); o segundo é dedicado à "Criminalidade" (arts 15 a 22 do CP); o terceiro capítulo, relativo a "Agentes do Crime" (arts 23 a 27 do CP); o quarto é referente a "Responsabilidade Criminal",

[197] Ibidem.
[198] SOUZA, Elísio de. ***ob. cit***..
[199] HUNGRIA, Nelson et al. ***ob. Cit***. p.54.

previstos nos arts 28 a 50 do CP) e o quinto capítulo é relativo a "Causas que excluem a ilicitude e a culpa" arts 51 a 58 do CP).

O terceiro título aborda sobre "Penas, Medidas Criminais e Efeitos," e é constituído por doze capítulos, sendo o primeiro, relativo a Disposições Gerais - "Finalidades das Penas e Medidas de Segurança" (arts 59 e 60 do CP); o segundo capítulo fala sobre "Pessoas Singulares" (arts 61 a 84 do CP); o terceiro, relativo a "Pessoas Colectivas e Entidades Equiparadas" (arts 85 a 94 do CP); o quarto capítulo aborda sobre as "Medidas de Segurança" (arts 95 a 111 do CP); o quinto fala da "Determinação da Pena" (arts 112 a 115 do CP); enquanto isso, o sexto capítulo com a epígrafe " Aplicação das Penas Quando há Circunstâncias Agravantes ou Atenuantes (arts 116 a 122 do CP); o sétimo capítulo fala da "Aplicação das Penas em Alguns Casos Especiais" previstos nos arts 123 a 133 do CP; o oitavo capítulo é relativo a "Efeitos das Penas", previsto nos arts 134 a 141 do CP. O nono capítulo é referente a "Suspensão da Execução da Pena de Prisão" (arts 142 a 147 do CP), o décimo é atinente a "Execução das Penas e Medidas de Segurança" (arts 148 a 152 do CP); o décimo primeiro é relativo a "Liberdade Condicional", previsto nos arts 153 e 154 do CP; o último capítulo, aborda sobre a "Extinção da Responsabilidade Penal" previsto nos arts 155 a 158 do CP).

Já o livro II - "Parte Especial", é composto por seis títulos, sendo o primeiro título (Crime Contra as Pessoas), composto de XI capítulos, destacando-se:

O primeiro é referente a "Crimes contra Vida (arts 159 a 170 do CP); o segundo, dedicado à "Crimes contra a Integridade Física" (arts 171 a 184 do CP); o terceiro é relativo a "Disposições Aplicáveis aos Capítulos Anteriores" (arts 185 a 187 do CP); o quarto é referente a "Participação em Rixa", previstos nos arts 188 e 189 do CP; o quinto fala dos "Crimes contra a Humanidade, Identidade Cultural e Integridade Pessoal" (arts 190 a 194 do CP); o sexto capítulo com a epigrafe " Crimes Contra a Liberdade das Pessoas" (arts 195 a 200 do CP); o sétimo capítulo fala de " Crimes Contra a Liberdade Sexual" previstos nos arts 201 a 217 do CP; o oitavo é relativo a "A Colocação das Pessoas em Perigo" previsto nos arts 218 a 232 do CP; o nono capítulo aborda sobre " Crimes Contra a Dignidade das Pessoas " (arts 233 a 249 do CP); o décimo é dedicado à Crimes contra a Reserva da Vida Privada (arts 250 a 258 do CP); enquanto isso, o último capítulo (o décimo primeiro) é referente a "Crimes contra a Família", previstos nos arts 259 e 260 do CP.

O segundo título (Crimes Contra o Património em Geral), é composto por três capítulos: o primeiro capítulo aborda sobre "Crimes Contra a Propriedade" (arts 270 a 285 do CP); o

segundo é referente à "Crimes Contra Direitos Patrimoniais" (arts 286 a 302 do CP) e o último, fala dos "Crimes de Receptação e Auxílio Material", previstos nos arts 303 a 305 do CP.

O terceiro título (Crimes de Perigo Comum), com dois capítulos: o primeiro é relativo a "Incêndio e Danos" (arts 306 a 313 do CP) e o segundo é referente a "Crimes Contra o Ambiente", preceituados nos arts 314 a 321 do CP.

O quarto título (Crimes Contra a Fé Pública), tem dois capítulos: o primeiro, fala dos "Crimes de Falsificação" (arts 322 a 341 do CP) e o segundo é referente a "Nomes, Trajos, Empregos e Títulos Supostos ou Usurpados" (arts 342 a 344 do CP).

O quinto título (Crimes Contra a Ordem e Tranquilidade Pública), com Oito capítulos: o primeiro é sobre a " Instigação Pública e Associação Criminosa" (arts 345 a 348 do CP); o segundo é dedicado à "Participação em Motim, Desobediência à Ordem de Dispersão e Outros" (arts 349 a 354 do CP); o terceiro capítulo é relativo a "Violação de Providências Públicas" (arts 355 a 357 do CP); o quarto capítulo fala da "Tirada e Fuga de Presos e dos que não Cumprem as suas Condenações" (arts 358 a 362 do CP); o quinto é referente "Acolhimento de Malfeitores", previsto no art. 363 do CP; o sexto é referente a Imigração Ilegal (arts 364 a 368 do CP); o sétimo fala da "Lotarias, Convenções Ilícitas sobre Fundos Públicos e Abusos em Casas de Empréstimos sobre Penhores", previstos nos arts 369 a 372 do CP; o oitavo é relativo à "Fraudes ou Violência nas Arrematações e Licitações" (art. 373 do CP).

O sexto título (Crimes contra o Estado) tem três capítulos, nomeadamente: o primeiro é referente a "Crimes Contra a Segurança do Estado" (arts 374 a 400 do CP); o segundo capítulo é relativo a "Crimes Contra a Realização da Justiça" (arts 401 a 424 do CP) e o terceiro capítulo é referente a "Corrupção e Crimes Conexos", previstos nos arts 425 a 449 do CP.

2.6. A Evolução do Direito Penal na Era Digital

2.6.1. O Advento da Internet e a Popularização do Uso de Computadores

Em conformidade com Júnior, "o surgimento da Internet, segundo pesquisa da rede de notícias norte-americana CNN e do Instituto de Tecnologia de Massachussets, remete-se ao período da Guerra Fria, em meados do século XX. Em que duas potências mundiais, Estados Unidos e União Soviética, disputavam uma corrida bélica, armamentista e espacial, à vista disso, surgiu a internet, por objectivos militares"[200]. Ainda na mesma senda, Wendt et al, alude

[200] JUNIOR, Júlio Cesar Alexandre, ***Cibercrime: um estudo acerca do conceito de crimes informáticos.*** Revista Eletrônica da Faculdade de Direito de Franca. Disponível em:

que “a rede ainda não possuía a denominação de internet, mas teve como denominação ARPANET (Agência de Pesquisa Avançada e Rede, em inglês, Advanced Research Projects Agency Network) em 1969. Já a primeira conexão internacional foi realizada em 1973, até então pela ARPANET, que interligou a Inglaterra e a Noruega”[201].

Carneiro[202], alude-nos que o título “Internet” sobreveio posteriormente, quando houve a invenção da Teia Mundial em 1986, com isso ficou mais acessível ao público, tornando esse meio de comunicação popular na década de 90. Essa tecnologia, segundo Carneiro, “passou a ser utilizada com outro objectivo, para estabelecer uma ligação entre as universidades americanas e, após isso, também para institutos de pesquisa de outros países”[203].

Na mesma visão do Carneiro, Sobrinho afirma que: “

> Com a maior distribuição da internet, a pretensão era que os usuários fossem anônimos e usufruíssem de igualdade na utilização desse espaço, visando com isso garantir uma velocidade superior e eficiência, gerando assim, maior segurança nas relações interpessoais e comerciais nesse ambiente. Desse modo, o seu objectivo inicial foi afastado, houve a democratização desse meio, sendo disponível a toda a população mundial e tornando-se um espaço sem fronteiras, assim, a rede de acesso e comunicação se universalizou, contudo, tornou-se um ambiente favorável para o surgimento e propagação de ameaças”[204].

De facto, na actualidade, a internet proporciona, uma imensurável quantidade de informações, facilitando a comunicação, como por exemplo, o e-mail, que funciona como uma correspondência digital, praticamente actuando em tempo real; fazer transacções bancárias; fazer compras online fora do país. Está evidente que a internet trouxe uma profunda mudança cultural que se enraizou numa nova forma de consumismo e nova maneira de relacionamento social. Sem dúvidas, essa crescente evolução tecnológica desenhou um mundo sem fronteiras, e com isso a sociedade modernizou-se e evoluiu. No entanto, a facilidade da comunicação instantânea, em razão das novidades virtuais, trouxe junto consigo a ***delinquência tecnológica, ou seja, a possibilidade de se praticar delitos no meio digital***.

---

https://www.revista.direitofranca.br/index.php/refdf/article/view/602#:~:text=Cibercrime%20est%C3%A1%20ass ociado%20ao%20%E2%80%9Cfen%C3%B3meno,12). Acesso em: 07 abr. 2021., Apud SOBRINHO, Jéssica Rafaela Nunes; et.al, ***OS SUJEITOS ATIVOS NO CIBERCRIME E A RESPONSABILIDADE PENAL DO OFENSOR. REVISTA CIENTÍFICA MULTIDISCIPLINAR DO CEAP*** (REV. MULT. CEAP). V. 4, N. 2, JUL./DEZ. 2022, p. 2.

[201] WENDT, Emerson; JORGE, Higor Vinícius Nogueira***, Crimes cibernéticos: Ameaças e procedimentos de investigação***. Rio de Janeiro: Brasport, 2012. Apud SOBRINHO, Jéssica Rafaela Nunes; et.al, ibidem***. p.2.***

[202] CARNEIRO, Adeneele Garcia, ***Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação***. Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012. Disponível em: https://egov.ufsc.br/portal/conteudo/crimes-virtuaiselementos-para-uma-reflex%C3%A3o-sobre-o-problemana-tipifica%C3%A7%C3%A3o/. Acesso em: 08 abr. 20. Apud SOBRINHO, Jéssica R. Nunes; et.al, ibidem. p. 2.

[203] ibidem.p.2.

[204] SOBRINHO, Jéssica Rafaela Nunes; et.al, ***ob. cit***. p. 2.

Nesse quadrante, Aranha *et al* apregoa que "a sociedade se organiza em rede das relações sociais aumenta: no entanto, em época alguma se atingiu tal nível de inter-relacionamento que agora nos permite falar em um mercado mundial que determina a produção, a distribuição e o consumo de bens e em uma cultura da "virtualidade real", que liga todos os pontos do globo, modelando comportamentos[205]".

Ressalta-nos afirmar que a internet, não só trouxe inúmeros e imensuráveis benefícios proporcionados à sociedade na era contemporânea, mas também, também, na internet, se dão os crimes digitais. Assim sendo, o âmbito de actuação daqueles que cometem os referidos crimes rompe fronteiras,

> "constituindo uma preocupação que está chamando a atenção da polícia de todo o mundo, especialmente no que diz respeito à colecta de evidências e materialidade; há também de se considerar o princípio de territorialidade, pois, se o computador está num determinado país, e o crime é cometido em outro, como processá-lo se nunca entrou naquele país? Policiais do mundo inteiro, tais como FBI, Scotland Yard, e Real Polícia Montada do Canadá, já há alguns anos, vêm formando os chamados "Cybercops", policiais especialmente treinados para combater esses delitos - o desafio criminal do próximo século - sendo a tónica, a maximização da cooperação entre os Países, alertando para o potencial das perdas económicas, ameaças a privacidade e outros valores fundamentais"[206].

Chega-se, com essa ilustração, a frisar que a internet surgiu como um meio poderoso, capaz de interligar computadores entre si e possibilitar a comunicação entre estes computadores, cujas finalidades variam de interesse de cada usuário. Deve entender-se que a internet como um meio de comunicação poderoso "baseia-se na ideia de haver comandos centrais, o que faz com que todos os pontos sejam equivalentes, não importando onde estejam os computadores, se no Brasil, EUA, China, etc., sendo um pressuposto da internet, que ela seja aberta a qualquer computador ou rede que deseje se conectar, mesmo de sistemas diferentes ou de línguas diferentes[207]. Ademais, ressalta-nos trazer a compreensão de Silva, quando alude que a Internet, denominada pela Mídia de Superestrada da Informação, nada mais é do que a

---

[A] ARANHA, Maria Lúcia de Arruda; et al***, Temas de Filosofia.*** São Paulo: Moderna, 2005. p.83. Apud PADILHA, Palma, ***Crimes Digitais e sua Tipicidade no Direito Penal***, Monografia de Graduação, Faculdade Baiana de Direito, Salvador, Barasil, 2012, p. 7.

[206] FERREIRA, Fabio Jânio Lima, ***Crimes Digitais. Disponível em< http://segurancadigital.info/ dicas/49-seguranca-da-informacao/59-crimes-digitais***. Acesso em: 4 dez 2011. Apud PADILHA, Palma, ob. cit. p. 9.

[207] CORRÊA, Gustavo Testa, ***Aspectos Jurídicos da Internet***. 2 ed. São Paulo: Saraiva, 2000. Apud PADILHA, Palma, ***Crimes Digitais e sua Tipicidade no Direito Penal***, Monografia de Graduação, Faculdade Baiana de Direito, Salvador, Barasil, 2012, p. 9.

interligação simultânea de computadores de todo o planeta, algo que os futuristas em seus exercícios de suposição jamais imaginaram"[208].

É válido afirmar que, actualmente, a sociedade tornou-se dependente dessa tecnologia da informação, assim como, das relações comerciais, as escolas, faculdades, empresas e até a administração pública e, recentemente, passou a assumir uma postura bastante comercial através da sua utilização. Segundo Schoueri (2000, p. 157): "A internet é uma gigantesca rede mundial de computadores que interliga entre si desde grandes computadores até micros pessoais ou *note-books* através de linhas comuns de telefone, linhas de comunicação privada, cabos submarinos, canais de satélite e diversos outros meios de comunicação"[209].

Com efeito, "essa imensa rede de computadores foi concebida, inicialmente, para fins bélicos, mas seu grande trunfo foi ser acessível a toda a população, principalmente diante da ausência de um proprietário que a explore financeiramente"[210]. Na mesma linha de reflexão, Paesani diz que com o seu conhecimento: "a internet não pertence a ninguém, não é financiada por instituições, governos ou organizações internacionais, e também não é um serviço comercial"[211] .

No entendimento de Sobrinho,

> "a rede de internet possui papel essencial mundialmente, sendo hoje utilizada como uma das plataformas mais eficientes que impulsiona a economia mundial, bem como aplicada em variados sectores, entre eles, económicos, militares, de segurança, de transportes, de telecomunicações, de educação e saúde, ando origem ao que hoje é conhecido como sociedade da informação, vez que tudo que acontece ao redor é repleto de informação"[212].

Considerando esse contexto socioeconómico desempenhado pela internet, é possível perceber os danos que podem advir de ameaças e ataques pela rede mundial de computadores e a imensidão dos prejuízos que essa insegurança pode ocasionar. Dado que a sociedade da informação se correlaciona com a crescente dependência dos sistemas de tecnologias de informação, que são dotadas de dinamismo e volatilidade, motivo pelo qual cibercrimes encontram incontáveis formas de serem praticados, e assim, os tornam um evento frequente, perigoso e violador de direitos fundamentais. Uma vez que "os crimes cibernéticos deixaram

---

[208] ibidem, p. 9.
[209] SCHOUERI, Luís Eduardo, ***Internet; o direito na era virtual.*** São Paulo; Ed. Lacaz Martins, Halemberck, Pereira Neto, Gurevich e Schoueri Advogados, 2000. Apud PADILHA, Palma, ob. cit. p. 10.
[210]RECUERO, Raquel da Cunha, ***Internet e a Nova Revolução na Comunicação Mundial***. Disponível em: Acesso em 6 nov. 2011. Apud PADILHA, Palma, ob. cit., p. 10.
[211] PAESANI, Liliana Minardi, ***Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil***. 2ª ed. São Paulo: Atlas, 2003. Apud PADILHA, Palma, ***ob. cit.*** p. 10.
[212] SOBRINHO, Jéssica Rafaela Nunes; et.al. ***ob. cit***. p. 2.

de se utilizar da internet somente como objecto final do delito, para utilizar também como meio para consumação de outros crimes"[213]. Com infinitas possibilidades de aparatos para o cometimento desses crimes no meio digital, veja-se:

> "Com a utilização de vírus, o criminoso conseguia obter acesso ao computador de suas vítimas. O advento da internet e a sua forma de concepção, que permite interconectar equipamentos ao arrepio da distância geográfica e do controlo, aliado à facilidade de troca de informações entre usuários que nunca se viram, e provavelmente, nunca se verão, criou uma propícia para o estabelecimento de uma outra classe de programas com objectivos voltados para causar danos a terceiros. Um destes tipos de programas de computador é o chamado vírus. Vírus, então, nada mais são do que programas de computador intencionalmente desenvolvidos, em geral, com intenções maliciosas, de causar dano a um grupo específico de computadores ou à rede em geral" [214].

Observa-se que o advento da rede de internet está aliado à facilidade em diferentes formas, permitindo a conexão à distância e troca de informações, porém, pode ser favorável e voltada também para o acometimento de danos a outrem, a título de exemplo referido, a utilização de programas de computador como o vírus, intencionados ardilosamente, representando a área dos crimes de natureza informática, assim dizendo, os cibercrimes. É importante ressaltar que "os Estados Unidos, país que originou a internet, foi o primeiro também em se manifestar a respeito da importância dessas ameaças tecnológicas, tipificando pela primeira vez em 1978 crimes de natureza informática"[215].

Com o aumento dos casos desses ilícitos praticados pela internet, a importância desse novo segmento de crimes foi evidenciada. Contudo, não se pode olvidar que esse meio de acesso propiciou de certa forma o surgimento, bem como o próprio aumento de uma série de crimes cibernéticos. E, apesar do conhecimento contemporâneo sobre essas actividades criminosas e "da indispensabilidade e urgência de investida contra tais actos, é necessário categorizar, isto é, reflexionar seu ponto inicial e conceitualizar"[216] .

2.6.2. O Direito Penal Digital

Os delitos cometidos por meio de tecnologias da informação demandam um conjunto de normas e princípios que regulam as condutas criminosas praticadas no meio digital. O termo

---

[213] ibidem, pp. 2-3.
[214] SOUZA, Henry Leones De. VOLPE, Luiz Fernando Cassilhas, ***Da ausência de legislação específica para os crimes virtuais.*** Disponível em: https://egov.ufsc.br/portal/conteudo/daaus%C3%AAncia-de-legisla%C3%A7%C3%A3oespec%C3%ADfica-para-os-crimes-virtuais. Acesso em: 08 abr. 2021. Apud SOBRINHO, Jéssica Rafaela Nunes; et.al, ***ob. cit.***, p. 3.
[215] Ibidem, p. 3.
[216] SOBRINHO, Jéssica Rafaela Nunes; et.al, ob. cit. p. 3.

"digital", por sua vez, refere-se a tudo que está relacionado à tecnologia da informação e da comunicação, englobando a Internet, os dispositivos electrónicos, os *softwares*, entre outros [217]. Assim, podemos definir ***o Direito Penal Digital*** como um ramo emergente do direito que regula o exercício do poder punitivo do Estado tendo como pressuposto de acção os crimes cibernéticos e como consequência as penas.

Uma parte da doutrina defende que o Direito Penal Digital não chega a ser um ramo de Direito. É uma releitura do Direito Penal face ao impacto da internet na sociedade e caracteriza-se por criação de leis para regulamentar conduta on-line e estabelecer novos tipos penais ocorridos no ambiente virtual. De acordo com PIRANI[218], o Direito Penal Digital não implica a criação de um novo Direito Penal, mas sim na importância de que o Direito Penal tradicional se adapte às novas tecnologias e desafios do ciberespaço. Além disso, encarar o Direito Penal Digital como uma extensão do Direito Penal Tradicional permite uma maior consistência e continuidade jurídica. Isso pode ajudar a evitar a criação de leis e regulamentos isolados, que podem levar a confusões e conflitos.

Outra parte da doutrina defende uma visão do Direito Penal Digital como uma nova esfera jurídica. Um dos principais é que a natureza única das questões digitais requer uma abordagem jurídica própria. Por exemplo, a velocidade e a escala com que a informação é disseminada on-line, a facilidade com que os dados pessoais podem ser colectados e usados, e a capacidade de cometer crimes de qualquer lugar do mundo são aspectos que não têm paralelo no mundo físico. Portanto, pode ser necessário desenvolver novos princípios e normas jurídicas para lidar com esses desafios ([219]).

Seguindo de perto Silva (2021),[220] podemos afirmar que o Direito Penal Digital é uma área que necessita de regulamentações próprias e autonomia, uma vez que vivemos em uma sociedade cada vez mais imersa no ambiente virtual, não apenas em termos tecnológicos, mas também psicológicos e sociais. Portanto, o Direito Penal Digital é uma nova esfera jurídica que

---

[217] Cfr. THOMPSON, Marco Aurélio. Direito digital: uma nova esfera jurídica ou uma extensão inevitável do direito tradicional? In: https://jus.com.br/artigos/104612/direito-digital-uma-nova-esfera-juridica-ou-uma-extensao-inevitavel-do-direito-tradicional – acesso- 01-10-2024.

[218] PIRANI, Mateus Catalani. O direito digital aplicado ao consumo sustentável: internet das coisas e sustentabilidade. Tese (doutorado) - Universidade Católica de Santos, Programa de Pós-Graduação stricto sensu em Direito Ambiental Internacional, 2021.

[219] No mesmo sentido, THOMPSON, Marco Aurélio. Direito digital: uma nova esfera jurídica ou uma extensão inevitável do direito tradicional? In: https://jus.com.br/artigos/104612/direito-digital-uma-nova-esfera-juridica-ou-uma-extensao-inevitavel-do-direito-tradicional _acesso 01-10-2024.

[220] SILVA, Kevin Rick Matias; apud. THOMPSON, Marco Aurélio. Direito digital: uma nova esfera jurídica ou uma extensão inevitável do direito tradicional? In: https://jus.com.br/artigos/104612/direito-digital-uma-nova-esfera-juridica-ou-uma-extensao-inevitavel-do-direito-tradicional _acesso 01-10-2024.

se apresenta como um desafio para o Direito Penal Tradicional, exigindo novas abordagens e soluções para proteger a privacidade, os direitos individuais e outros bens jurídicos no ambiente virtual.

Por fim, importa referir que o Direito Penal Digital enfrenta uma série de desafios e questões emergentes. Um dos principais é a velocidade com que a tecnologia evolui, que muitas vezes supera a capacidade do Direito de se adaptar. Isso pode levar a lacunas na legislação e na jurisprudência, deixando os usuários de tecnologia sem protecção adequada. Outro desafio importante é a questão da jurisdição em um mundo cada vez mais globalizado e conectado. *Crimes cibernéticos* podem ser cometidos de qualquer lugar do mundo, tornando difícil determinar qual lei se aplica e como fazer valer a justiça ([221]).

([221]) Cfr. THOMPSON, Marco Aurélio. Direito digital: uma nova esfera jurídica ou uma extensão inevitável do direito tradicional? In: https://jus.com.br/artigos/104612/direito-digital-uma-nova-esfera-juridica-ou-uma-extensao-inevitavel-do-direito-tradicional _acesso 01-10-2024.

CAPÍTULO III: CRIMES CIBERNÉTICOS

3.1. Do Crime em Geral

A criminalidade é um problema que atinge toda a sociedade moçambicana e tem-se acentuado nos últimos anos.[222] Nesse contexto, o debate sobre o combate a criminalidade e a melhor forma de realizá-la é recorrente nas discussões entre os formadores de políticas públicas e pela sociedade em geral.

O fenómeno da criminalidade consiste num problema social, económico e político de extrema importância. No entanto, a acção do criminoso é precedida de uma avaliação de risco. O criminoso decide agir quando conclui que o benefício de sua acção delituosa será maior que o risco que terá de correr. De forma geral, na literatura do crime, são considerados como possíveis determinantes das taxas de crime algumas variáveis relativas às condições económicas, sociais, demográficas e de política pública.[223]

O aumento nas taxas da criminalidade, os elevados custos a elas associados e a crescente importância dada ao assunto em pesquisas de opinião têm levado os governos e a sociedade civil a encarar o problema da violência como um dos mais sérios obstáculos ao desenvolvimento económico e social.[224] Estudos internacionais demonstram que ocorre maior incidência de crimes em contextos de desorganização social, desemprego, baixos salários, desigualdade educacional e principalmente em cenários compostos por jovens.[225]

A África é um dos continentes onde a barbárie se apresenta de forma mais intensa, o que vem se tornando um empecilho ao desenvolvimento económico de todos os países Africanos, dentre eles o Moçambique, constituindo então num desafio de formular e implementar políticas que permitam prevenir e reduzir o crime e a violência.[226]

Para tanto, é de fundamental importância o desenvolvimento de pesquisas que permitam avançar na compreensão das causas desses fenómenos, assim como a geração de bases de dados que permitam monitorar e melhorar a compreensão das tendências espaciais e temporais da criminalidade.[227]

---

[222] MUBARAK, Rizuane. ***Ob. Cit.*** p. 448.
[223] MUBARAK, Rizuane. ***Ob. Cit.*** p p. 448.
[224] Ibidem, p.448.
[225] FERNANDES, Valter. ***Ob. Cit.*** p. 378
[226] MUBARAK, Rizuane. ***Ob. Cit.*** p.449.
[227] Ibidem, ob. cit, p.449.

3.1.1. Noção do Crime em Geral

Para dar conceito de crime, antes porém, importa referir que a doutrina[228] apresenta conceito formal, assim como o conceito material do crime, entretanto, neste trabalho, vamos apresentar cada um desses conceitos.

3.1.1.1. Crime em Sentido Formal

Formalmente pode se definir o crime como sendo a desobediência à lei criminal. Por um caminho lógico categorial (que determina os conceitos pela enumeração dos seus elementos e explica as coisas decompondo a nos seus elementos mais simples) pode aliás procurar dar-se, e tem-se procurado dar, uma definição de crime pela enumeração dos elementos que o compõem.

Assim, o crime, como preceito de espécie que é, supõe uma série hierarquizada de conceitos que, de degrau a degrau, se vão obtendo pela sucessiva abstracção dos seus diversos elementos.[229] Assim sendo, em sentido formal, o crime vai ser uma acção típica, ilícita e culposa que seja passível de pena por lei.[230]

3.1.1.2. Crime em Sentido Material

Em termos materiais, o crime vai ser toda conduta que o Código Penal (CP) já prevê como crime e no caso do ordenamento jurídico moçambicano, vai ser crime toda conduta que se encontra descrita na parte especial do CP, que se encontra concretamente no art. 159º e seguintes.

3.1.2. Distinção entre Crimes e Contravenções

Sobre o assunto em questão - a diferença entre os crimes e contravenções - há uma série de teorias que se dedicam ao estudo deste assunto. No entanto, se todas juntas ou comparadas uma da outra, as ideias que as separavam eram seguintes: por um lado, diz-se que as contravenções não implicam para quem as pratique um prejuízo de censura, um juízo ético, como implica em princípio, a prática de um crime.[231] Esta é a ideia que aparece, a propósito das

---

[228] BELEZA, Teresa Pizarro, ***Direito Penal***, Vol. I, 2ª ed. Revista e actualizada, Associação Académica da Faculdade de Direito Lisboa, Lisboa, 1998, p. 22.
[229] CORREIA, Eduardo, ***Direito Criminal***, Vol. I S/Ed. Reimpressão, Almedina, Coimbra, 2001, p. 198.
[230] BELEZA, Teresa Pizarro, ***Direito Penal***, ob. cit., p. 22.
[231] BELEZA, Teresa Pizarro. ob. cit. pp. 101-103.

contravenções e não só, frequentemente a concepção dita ético-social do Direito Penal. Ou seja, um crime implica um juízo de censura especial sobre o seu agente, a contravenção não.

Por outro lado, diz-se que a protecção dos bens jurídicos através de incriminação de condutas é uma protecção directa e imediata; a protecção dos bens jurídicos através da criação de contravenções é uma protecção indirecta, longínqua, mediata. Veja-se por exemplo, na incriminação por homicídio protege-se directa e imediatamente a vida das pessoas.

Na punição de contravenção que, por exemplo, consiste em conduzir em excesso de velocidade, só de uma maneira muito geral, muito mediata e muito longínqua é que se esta a proteger a vida das pessoas que poderiam ser atropeladas por aquele individuo que vai em excesso de velocidade. Só que esta concepção não satisfaz muito pelo facto de existirem crimes que consistem apenas num certo perigo e que este perigo vai ser abstracto. Aponta-se, como exemplo, a falsificação da moeda, mesmo que esta moeda não venha a entrar em circulação, é um crime previsto e punível nos termos do art. 326º do CP mesmo que esta moeda não venha a entrar em circulação. Por outro lado, uma ideia que existe de que as contravenções correspondem mais a actos de desobediência em relação à Administração, também é um pouco colocada em causa pelo facto de existirem também crimes de desobediência como é o caso do art. 353º do CP.

3.1.3. Tipos de Crimes

Vários são os critérios que são usados para a classificação de crimes, neste trabalho iremo-nos focar, essencialmente, em três critérios apenas, nomeadamente: critérios quanto ao autor, quanto a conduta, quanto ao bem jurídico.[232]

3.1.3.1.Quanto ao Autor

O autor de um crime pode ser, em regra, qualquer pessoa, quando pode ser cometido por qualquer um, estamos neste caso, perante os chamados crimes comuns. Por vezes, a lei leva a cabo nesta matéria, uma especialização, no sentido de que certos crimes só podem ser cometidos por determinadas pessoas as quais pertence uma certa qualidade ou sobre as quais recai um dever especial, deparamos ai com os chamados crimes específicos.[233] No ordenamento jurídico moçambicano, podemos citar o crime de homicídio como crime comum, ou seja, pode este ser cometido por qualquer pessoa, nos termos do artigo 159º do CP; Como um crime

[232] DIAS, Figueiredo Dias, ***Direito Penal***, Tomo II, 2ª Ed. Coimbra Editora, Coimbra, 2012, pp. 303-304.
[233] COSTA, José de Faria, ***Noções Fundamentais de Direito Penal***, 3ª Ed. Coimbra Editora, 2012, p. 227.

especial, pode-se chamar a colação o art 222º do CP que penaliza ao profissional da saúde com pena de prisão de dois meses a um ano e multa por recusar o auxílio da sua profissão em caso de perigo para a vida ou de perigo grave para a integridade física de outra pessoa que não possa ser removido de outra maneira.

3.1.3.2.Quanto a Conduta

Se pelo contrário o tipo incriminador se preenche pela má execução de um determinado comportamento, estaremos em face de crimes de mera actividade. É de resto no fundo, essencialmente a mesma distinção que se leva a cabo quando se distinguem crimes formais (cuja tipificação é indiferente a realização de resultados) e crimes materiais (cuja tipicidade interessa o resultado).[234]

3.1.3.3. Quanto ao Bem Jurídico

Atendemos a forma como o bem jurídico é posto em causa pela actuação do agente. Nos crimes de dano a realização do tipo incriminador tem como consequência uma lesão efectiva do bem jurídico. Nos crimes de perigo, a realização do tipo não pressupõe a lesão, mas antes se basta com a mera colocação em perigo do bem jurídico.[235]

São exemplos de crimes de dano previstos no Código Penal moçambicano, o crime de violação previsto no art. 201º do CP. E para exemplificar um crime de perigo, podemos citar a questão de venda ou exposição de substâncias venenosas ou abortivas, que se encontra regulado pelo art. 223º do CP.

3.1.4. Formas de Aparecimento de Crime

De acordo com o nosso Código Penal actual, no seu art. 15º, o crime pode aparecer sob forma de "consumação e sob forma de tentativa"[236]. É nossa tarefa, explicar como se caracteriza cada uma dessas formas que o crime pode revestir, isso facilitara de certo modo a compreensão do tema que pretendemos fazer o estudo.[237]

[234] DIAS, Figueiredo Dias. ob. cit. p. 306.
[235] Ibidem, pp. 308-309.
[236] Cfr. Art. 15 do CP.
[237] COSTA, José de Faria. **ob. cit**. 2012, p. 231.

3.1.4.1. Consumação

A consumação caracteriza-se pela execução completa da actividade criminosa e da verificação do resultado, ou seja, o agente vai levar a cabo todo acto que julga necessário para efectivação da acção criminosa e, consequentemente, vai ocorrer o resultado por este idealizado.[238]

3.1.4.2. Tentativa

Há tentativa quando o agente praticar actos de execução de um crime que decidiu cometer, sem que este chegue a consumar-se. Ou seja, o agente vai dar início a execução da actividade criminosa e vai se interromper por circunstâncias alheias a sua vontade, a percepção actual é que tanto sendo interrompido, assim como tendo efectuado a actividade criminosa, desde que não se verifique o resultado por este idealizado, estaremos perante uma tentativa.[239]

A tentativa é punível, "quando o crime que se pretendia cometer, segundo o ordenamento jurídico moçambicano, quando consumado, seja punível com uma pena superior a dois anos, isso significa que, para que um crime seja susceptível duma tentativa, a sua moldura penal deve passar dos dois anos de prisão"[240], são exemplos de casos como: homicídio voluntário simples, homicídio agravado, entre outros; casos contrários a estes e não passíveis de tentativa são: as ofensas corporais simples e o aborto. Importa referir que, quando a tentativa for das puníveis, ao agente será aplicado a mesma pena que caberia ao crime que se tentou, se tivesse consumado. E a "tentativa não vai ser punível se o meio usado para tentar o crime não se mostrar adequado para efectivação do mesmo ou quando o objecto desejado inexiste"[241].

3.1.4.3. Elementos do Crime

A teoria geral da infracção penal, que também se designa teoria geral do crime, doutrina geral do crime ou teoria geral do facto punível, trata dos pressupostos gerais das condutas penalmente puníveis, independentemente das particularidades de cada tipo legal de crime.[242] Enquanto a parte especial do Direito Penal versa sobre os elementos que diferenciam os diversos tipos de crime o homicídio, a burla, o furto, a ofensa à integridade física, entre muitos

[238] BELEZA, Teresa Pizarro. **ob.cit**. p. 112.
[239] DIAS, Figueiredo Dias. **ob. cit**. p. 310.
[240] Cfr., os nºs 1 e 2 do art. 18 dio CP.
[241] Cfr., nº 3 do art. 18 do CP.
[242] MUBARAK, Rizuane, ***Direito Penal e Criminalística: Da teoria universal a realidade nacional***, S/Ed, p. 171.

outros, a teoria geral da infracção, ou do facto punível que lhe dá origem, ocupa-se dos princípios e elementos que são comuns a todos eles e que constituem as categorias que integram a noção geral de crime:

- Acção;
- Tipicidade;
- Ilicitude;
- Culpabilidade; e
- Punibilidade.

A principal função da teoria geral da infracção é a de servir de instrumento à decisão penal justa do caso concreto, constituindo factor de certeza e segurança jurídicas, na medida em que permite que se evite a incerteza da mera intuição, a improvisação casuística ou mesmo a arbitrariedade, permitindo ainda a igualdade no tratamento de casos idênticos e economia na análise dos casos práticos pela coerência metodológica.[243]

3.1.4.3.1. A Acção

As graves objecções que podem formular-se contra a generalidade dos conceitos de acção historicamente desenvolvidos, deram lugar ao entendimento crescente que há que abandonar um conceito de acção anterior à tipicidade e com validade geral e que, em seu lugar, há que corrigir a tipicidade em conceito fundamental do sistema de direito penal.[244]

Não indo tão longe, nomeadamente porque sempre há-de falar-se numa acção típica ou numa conduta típica, entendem autores como Roxin e Conceição Valdágua que a acção há-de conceber-se como exteriorização da personalidade, devendo entender-se como acção relevante para o direito penal, o comportamento humano, dominado ou dominável pela vontade, com reflexos no mundo exterior. Daqui resulta que do ponto de vista jurídico-penal não constituem acções e, portanto, não podem consubstanciar a prática de um facto típico, os factos resultantes de forças da natureza, os simples pensamentos, os movimentos reflexos (por exemplo convulsões) e os actos realizados em estado de hipnose ou sonambulismo, sobre os quais não há qualquer domínio da vontade. Em todos estes casos não existe uma conduta dominada ou dominável pela vontade, pelo que não se lhe aplicam as proibições e comandos jurídico-penais,

[243] COSTA, José de Faria. ob. cit. p. 238.
[244] DIAS, Figueiredo Dias. ob. cit. p. 244.

porquanto estes não podem ir além da capacidade de intervenção do Homem com a sua acção, no decurso dos acontecimentos.[245]

Desta forma, independentemente de reconhecer-se ou não outras funções ao conceito de acção, na dogmática jurídico-penal há-de reconhecer-se-lhe pelo menos esta função delimitadora dos comportamentos, quer por se entender que assim já não podem vir a ser considerados típicos, assentando-se num conceito geral de acção, previamente dado ao tipo (Roxin), quer entendendo que o que está em causa são antes vários conceitos de acção tipicamente conformados, enquanto elemento integrante do cerne dos tipos de ilícito, a par de outros, como defende o Prof. F. Dias, reconhecendo a centralidade que assume actualmente a realização do tipo de ilícito.[246]

3.1.4.3.2. Tipicidade

A tipicidade constitui elemento essencial do crime, pois qualquer conduta só poderá ter relevância penal, do ponto de vista da sua incriminação, se for típica, ou seja, quando preencha os elementos constitutivos de um dado tipo penal.[247]

Uma das funções desempenhadas pelo tipo é precisamente a função jurídico-política de garantia, enquanto decorrência do princípio da legalidade, como vimos *nullum crimen nulla poena sine lege* intimamente ligada à sua função sistemática, segundo a qual o tipo compreende o conjunto de elementos que permitem saber de que crime se trata.[248]

Do ponto de vista da natureza dos seus elementos ou conteúdo, o tipo penal é composto por elementos objectivos e elementos subjectivos. Os primeiros são os dados descritivos ou normativos (que carecem de ser complementados com outras normas de cariz jurídico ou social para serem compreendidos) exteriores à psique do agente. Os elementos subjectivos são os que respeitam a factos de natureza psicológica que traduzem a necessária relação que deve existir entre a consciência e a vontade do agente e os elementos objectivos do tipo.

3.1.4.3.2.1. Tipo Objectivo

Integram o tipo objectivo ou constituem elementos objectivos do tipo, consoante os diferentes crimes a considerar:[249]

---

[245] MUBARAK, Rizuane. ***ob. cit***. p. 173.
[246] DIAS, Figueiredo. ***ob. cit.*** p. 245.
[247] Ibidem, p. 245.
[248] FERREIRA, Manuel. ***Ob.cit***. p. 214.
[249] MUBARAK, Rizuane. ***Ob. cit***. p. 180.

- O objecto da acção (p. ex. a pessoa no crime de homicídio ou a coisa alheia nos crimes de furto);
- As várias modalidades de acção, como sucedem com a venda, troca, cedência compra no crime de tráfico de estupefacientes;
- As qualidades especiais do agente nos crimes específicos (em que só podem praticar o crime pessoas com determinados atributos, como seja o de empregado público nos crimes de peculato ou concussão, ou de médico no crime de recusa de facultativo.[250] Integram ainda o tipo objectivo, nos crimes de resultado, ou seja, naqueles em que à conduta se segue necessariamente uma consequência, que pode separar-se espacial e temporalmente daquela:
- O resultado, como seja a morte da vítima, no crime de homicídio;
- O nexo de causalidade entre a acção (ou a omissão) e o resultado;
- A imputação objectiva do resultado à conduta do agente (elemento não escrito dos crimes de resultado diferentes do nexo de causalidade).[251]

3.1.4.3.2.2. Tipo Subjectivo

O dolo é o elemento subjectivo comum a todos os tipos (dolosos) e consiste na representação e vontade psicológica de realização do facto, enquanto conjunto dos elementos objectivos do tipo legal (objecto, resultado, etc.).[252] Em alguns tipos de crime, existem ainda elementos subjectivos específicos, como sejam a intenção de apropriação da coisa no crime de furto. Do ponto de vista da sua estrutura, o dolo compõe-se de dois elementos: volitivo ou emocional e intelectual ou cognitivo.[253]

a) **O elemento intelectual ou cognitivo:** traduz-se no conhecimento de todos os elementos objectivos do tipo.

Com interesse directo para a matéria do erro, alguns aspectos da caracterização do elemento intelectual do dolo que, pela sua pertinência neste trabalho, seguimos de perto:

> 1º: Para que se considere haver dolo, não são exigidos quaisquer actos de consciência ou vontade reflexivos ou secundários, ou seja, actos de consciência ou de vontade pelos quais o agente reflicta sobre os seus dados psíquicos primários, duplicando-os,

[250] DIAS, Figueiredo Dias. ***ob. cit***. p. 247.
[251] Ibidem, p. 247.
[252] FERREIRA, Manuel Cavaleiro de. ***ob. cit***. p. 214.
[253] ibidem, p. 216

intensificando-se. Não é preciso saber que se sabe, não é preciso pensar que se está a pensar, não é preciso querer. É irrelevante que o agente não se tenha apercebido que manteve o propósito de matar por mais de 24h, ou que actuava com frieza de ânimo, por exemplo.

2º: Não é necessária a chamada consciência focal ou a consciência clara ou de atenção. Não é necessário que, no momento do facto, a atenção do agente incida clara e precisamente sobre o elemento da situação considerado. Bastam a consciência marginal, a consciência liminar ou difusa, a consciência ou saber de situação. É suficiente para o dolo que se possa dizer que o agente dispõe da informação correspondente.[254]

3º: Para se verificar o dolo, relativamente aos elementos normativos do tipo, não se exigem conhecimentos técnico-jurídicos (coisa alheia, documento, coisa móvel), bastando o conhecimento do cidadão comum.

b) Elemento volitivo do dolo: traduz-se na vontade de realização dos elementos objectivos do tipo, como supra aludido. Em função da diversidade de atitudes psicológico-volitivas do agente e, portanto, com referência ao seu elemento volitivo ou emocional, o dolo pode revestir três espécies, formas ou modalidades: dolo directo, necessário e eventual.[255]

Com o elemento intelectual do dolo relaciona-se a matéria do erro pertinente à tipicidade, que veremos infra; a propósito do seu elemento volitivo veríamos agora um pouco melhor cada uma das referidas modalidades que pode revestir.[256]

3.1.4.3.3. Espécies de Dolo

Dolo directo ou dolo directo do 1º grau verifica-se quando a vontade do agente se dirige directamente, como objectivo imediato da acção, à realização do facto típico que representou. Independentemente da sua motivação, o agente tem como objectivo único a realização do facto típico ou toma este como objectivo intermédio, mas em todo o caso directo. O arguido A quer matar B porque quer vingar-se dele, por exemplo:

a) **Dolo necessário ou dolo directo do 2º grau -** nestes casos, a realização do facto típico não é o objectivo imediato da sua conduta, mas o agente representa-a como

[254] DIAS, Figueiredo Dias. ob. cit. p. 248.
[255] FERREIRA, Manuel Cavaleiro de. ob. cit., p. 213.
[256] Ibidem, p. 214.

consequência certa ou necessária da sua conduta e, portanto, quer a realização do tipo. Por exemplo, A atira o seu automóvel contra o automóvel de B para danificar o veículo e atingi-lo fisicamente a ele, mas sabe que atingirá necessariamente outras pessoas que seguem no veículo visado, pelo que quer igualmente este último resultado, o qual não constitui o objectivo imediato ou directo de 1º grau do seu comportamento.[257]

b) **Dolo eventual -** Verifica-se quando o facto típico é representado pelo agente como consequência possível da sua conduta e este actua conformando-se com a realização do facto. Por exemplo, A) ao acelerar com a sua viatura numa rua estreita e movimentada admite a hipótese de poder atingir algum transeunte, mas mantém o seu comportamento aceitando aquele facto se o mesmo vier a ocorrer.[258]

3.1.4.3.4. O Erro com Incidência nos Elementos do Tipo

Concluída esta primeira abordagem sobre o conteúdo e estrutura do tipo, cumpre agora abordar a problemática do erro com incidência directa no elemento intelectual ou cognoscitivo do tipo subjectivo. A parte restante do erro tem a sua relevância em sede de culpa como veremos.[259]

a) Erro sobre o Objecto

O elemento intelectual do dolo, a que aludimos, pressupõe o conhecimento de todas as circunstâncias objectivas do crime. Assim, no crime de homicídio o agente deve saber que o objecto da sua acção é um ser humano e que aquela é apta a provocar-lhe a morte. Do mesmo modo na violação de domicílio, o agente deve ter consciência, deve ter conhecimento, que está: a introduzir-se numa habitação, que se trata de habitação de outra pessoa e que não está autorizado a fazê-lo, pois estes três elementos descritivos do correspondem a outras tantas circunstâncias objectivas do tipo.[260]

Se o agente actua desconhecendo algum destes elementos estará em erro sobre as circunstâncias do facto (ou erro sobre o facto típico). Este erro sobre as circunstâncias pode consistir no chamado erro sobre o objecto (ou, na expressão latina, *error in persona vel objecto*).[261] Este erro verifica-se quando o agente atinge com a sua acção um objecto típico diferente daquele que representou. É o que sucede quando um caçador dispara sobre um vulto,

[257] FERREIRA, Manuel Cavaleiro de. ***ob. cit***. p. 214.
[258] DIAS, Figueiredo Dias. ***ob. cit.*** p. 249.
[259] Ibdem.
[260] BELEZA, Teresa Pizarro. **ob. cit**. p. 118.
[261] DIAS, Figueiredo Dias. ***ob. cit***. p. 249

que vê mexer atrás de uns arbusto supondo ser uma peça de caça quando, na realidade, se trata de uma pessoa. Sendo elemento típico objectivo do crime de homicídio a morte de uma pessoa, para que se cometa o respectivo crime impõe-se que o agente saiba que está a atingir uma pessoa (ainda que não seja quem ele pensa,), o que corresponde ao elemento intelectual do dolo.[262]

b) Erro sobre a Identidade do Objecto

Situações semelhantes às anteriores mas delas diferentes num aspecto essencial são os casos de erro sobre a identidade do objecto, que agora veremos: *error in persona* engana-se na qualidade ou identidade da pessoa ou *error in objecto*, quando se engana no objecto concreto: quantidade ou qualidade do mesmo.[263] Este erro verifica-se quando o agente se representa correctamente a existência de um objecto, que corresponde às características exigidas pelo tipo legal, mas erra sobre a sua identidade, em concreto: A. quer matar a mulher de B. mas mata a mulher de C. por confundi-la com aquela; A. pretende danificar o carro do vizinho mas danifica o automóvel de um parente deste que o visitara, por confundir ambas as viaturas. Em ambas situações é irrelevante o erro sobre a identidade, não eximindo de responsabilidade criminal.

3.1.4.3.5. A Imputação Objectiva do Resultado à Conduta – o Nexo de Causalidade

Em primeiro lugar, importa relembrar a distinção entre crimes formais ou de mera actividade e crimes materiais ou de resultado, pois só a propósito deste último suscita a questão da imputação objectiva do resultado e do nexo de causalidade.[264]

Nos crimes formais ou de mera actividade, o tipo objectivo, ou seja, o conjunto dos elementos que descrevem o facto objectivamente ilícito, consiste numa mera acção, numa dada conduta, que se preenche com a sua verificação, independentemente de dar origem a qualquer outro evento ou consequência. O crime consuma-se independentemente da verificação de um resultado separável da conduta. É o caso da omissão de auxílio, da violação de domicílio, devassa da vida privada ou devassa por meio de informática, entre muitos outros; basta-se a lei penal com a prática desses actos, independentemente de daí advirem quaisquer desvantagens ou prejuízos concretos para as pessoas que os sofrem.[265]

São crimes materiais ou de resultado, aqueles em que o tipo incriminador apenas se realiza com a verificação de um resultado típico, espaço-temporalmente desligado, distinto, da

[262] FERREIRA, Manuel Cavaleiro de**.** ***ob. cit***. p. 216.
[263] Ibidem, p. 216.
[264] BELEZA, Teresa Pizarro. ***Ob. cit***. p. 120.
[265] BELEZA, Teresa Pizarro. ***Ob. cit***. p. 120.

própria conduta do agente. É o caso do homicídio em que para além da prática de determinados actos idóneos disparar um projéctil, atingir com objectos, ministrar substâncias, etc., se exige que a tal conduta sobrevenha a morte, pois só com esta se consuma o crime. A morte é o evento material ou resultado que acresce à conduta do agente, seja esta dolosa ou negligente. Também nas ofensas corporais, no fogo posto, no aborto, se exige a verificação de um resultado para se terem por praticados ou consumados os respectivos crimes.[266]

O problema da imputação objectiva do resultado à conduta (incluindo a verificação do nexo de causalidade) só se coloca nos crimes de resultado, como vimos, e pode equacionar-se assim: quando é que pode dizer-se que o resultado deve atribuir-se à conduta? Ou seja, como explica o Prof. Dias: exigindo-se para o preenchimento integral de um tipo de ilícito a produção de um resultado, importa verificar não apenas se esse resultado se produziu, mas também se ele pode ser atribuído, imputado, à conduta.[267]

A exigência mínima que tem de fazer-se relativamente à conexão entre o comportamento humano e o evento é a da causalidade, o que justificou que durante muito tempo toda esta problemática tivesse sido tratada sob a designação de nexo de causalidade.[268]

Na verdade, a teoria do nexo causal é (pelo menos nos delitos omissivos) o fundamento de toda a imputação objectiva, pois o primeiro pressuposto do preenchimento do tipo é que o autor tenha causado o resultado. No entanto, concluindo-se pela causalidade da conduta não se realiza sempre o tipo, como antes se acreditava, ainda que concorram os restantes elementos típicos objectivos. Assim, por exemplo, pode não haver imputação objectiva, mesmo que o autor tenha causado o resultado, porque tal ficou a dever-se a mera casualidade ou a outras causas que podem excluir a imputação objectiva. A imputação objectiva há-de pois verificar-se e analisar-se em dois momentos sucessivos: o do nexo ou relação causal e o dos restantes pressupostos da imputação. Nem sempre, porém, se operou esta distinção, como veremos da exposição das teorias sobre esta problemática.[269]

3.1.4.4. Ilicitude

Sem ignorar as objecções que do ponto de vista científico-dogmático pode suscitar a chamada concepção tripartida do crime, continuaremos a segui-la na exposição, tendo sobretudo em conta que corresponde a um correcto procedimento prático de análise dos casos

[266] FERREIRA, Manuel Cavaleiro de. ***ob. cit***. p. 219.
[267] DIAS, Figueiredo Dias. ***ob. cit***. p. 250.
[268] Ibidem, p. 250.
[269]DIAS, Figueiredo Dias. ***ob. cit***. p. 250.

penais, pelo que tomado o tipo como o primeiro degrau e autónomo qualificativo da acção (acção típica), cabe agora cuidar das causas de justificação, enquanto factor de negação da ilicitude (2º degrau).[270]

Como vimos, a verificação de uma causa de justificação tem como efeito o afastamento ou exclusão da ilicitude de um dado facto típico. As causas de justificação não têm que ter natureza penal, antes podem emanar de um outro ramo do direito, pois é entendimento dominante e mesmo positivado na lei penal que o facto não é punível quando a sua ilicitude for excluída pela ordem jurídica considerada na sua totalidade.[271]

Não são taxativas as causas de justificação previstas na lei, dado precisamente o apelo à totalidade ou unidade da ordem jurídica, podendo resultar outras causas de justificação dos restantes ramos de direito, para além da analogia que, por ser *bona partem,* é admitida.

Principais causas de justificação ou exclusão da ilicitude:

- Legítima defesa;
- Direito de necessidade;
- Conflito de deveres;
- Consentimento expresso ou presumido.[272]

3.1.4.5. Culpa

No que diz respeito ao princípio da culpa, é hoje unanimemente considerado que não há responsabilidade sem culpa, pelo que não é suficiente a afirmação da ilicitude da sua conduta para que o mesmo possa ser sancionado com uma pena. É necessário ainda que a sua conduta seja culposa. Neste sentido se refere a culpa enquanto elemento do crime ou infracção penal. No entanto, tanto no que respeita ao conceito de culpa, como ao seu fundamento e mesmo à sua relação com a matéria da determinação concreta da pena, são várias as posições doutrinárias e delas não cuidaremos aqui, limitando-nos ao essencial, na perspectiva judiciária.

Tomamos, pois, como conceito operacional, a concepção normativa da culpa, de acordo com a qual a culpa traduz-se num juízo de censurabilidade sobre uma certa conduta típica e

[270] FERREIRA, Manuel Cavaleiro de. ***ob. cit.*** p. 221.
[271] DIAS, Figueiredo Dias. ***ob. cit***. p. 250.
[272] Ibidem, p. 250.
[272]Ibidem, p. 251.

ilícita resultante da imputação a alguém desse mesmo comportamento, atribuído à sua vontade, ao seu discernimento e capacidade, relativamente ao qual lhe era exigível que tivesse actuado de modo diverso, de modo conforme ao Direito.[273]

Na perspectiva da aplicação prática do direito, podem agrupar-se em três categorias as causas que podem levar à não punição do agente pela ausência de um juízo de culpa:

- Inimputabilidade;
- Inexigibilidade; e
- Falta de consciência da ilicitude não censurável.[274]

3.1.4.6. Punibilidade

A categoria da punibilidade, enquanto elemento do crime, é em si mesma controversa, opondo-se à sua autonomização autores como, na doutrina penal portuguesa, o Prof. Taipa de Carvalho, para quem os chamados pressupostos adicionais da punibilidade não justificam que se crie uma nova categoria dogmática do crime, pois aqui devem incluir-se apenas os elementos que respeitem a todo e qualquer crime.[275]

Como condições de punibilidade costumam considerar-se distinguindo entre condições positivas e negativas um conjunto de pressupostos que, se bem que não se liguem à ilicitude nem à culpa, todavia decidem da punibilidade do facto, nomeadamente a consumação ou a tentativa no crime de auxílio ao suicídio, o facto de o agente ser encontrado no território nacional para ser aí julgado e punido, a desistência da tentativa, ou o arrependimento activo, o pagamento do valor de cheque.

Neste contexto, fica, porém, a ideia de que, independentemente da autonomização, ou não, da punibilidade como elementos da teoria geral do crime, as chamadas condições de punibilidade que não devam, considerar-se meros pressupostos processuais ou condições de procedibilidade (a apresentação de queixa ou que o agente se encontre no território nacional), devem a sua relevância a constituírem casos de falta de dignidade penal do facto ou de não verificação da necessidade penal. Isto é, a situações em que o legislador por razões político-criminais relacionadas exclusivamente com os fins das penas e com o objectivo da preservação do bem jurídico (desistência da tentativa) ou da reparação do dano causado pela conduta ilícita

[273] FERREIRA, Manuel Cavaleiro de. ***ob. cit.*** p. 222.
[274] DIAS, Figueiredo Dias. **ob. cit**. p. 252.
[275] Ibidem, p. 253.

e culposa (pagamento do valor do cheque), entende atribuir a essas condutas (posteriores à conduta ilícita e culposa) o efeito de exclusão (não aplicação) da pena.[276]

3.2. Cibercrime ou Crimes Cibernéticos

3.2.1. Conceito de Crimes Cibernéticos

Os crimes cibernéticos emergem com o surgimento da internet e o avanço diário da tecnologia. "O cibercrime[277] demonstrou seus primeiros indícios na década de 1960, momento em que se ouviu falar e passou a ser discutido sobre os diversos crimes envolvidos com a nova tecnologia"[278]. Todavia, "não existe consenso geral ou uma definição clara sobre o que é um cibercrime, tendo em vista que os crimes que recorrem moderadamente à tecnologia e aos aparelhos digitais são estabelecidos nesta categoria"[279].

Ainda se discute ao nível da doutrina sobre as denominações para a mesma modalidade do crime. Com efeito, são várias as expressões utilizadas para designar crimes da internet: "cibercrime; crime digital; crime informático; crime informático-digital. Portanto não há consenso quanto à expressão, à definição, nem quanto à tipologia e classificação destes crimes"[280]. Nesse contexto, persiste a inexistência de um conceito de "criminalidade informática" expressamente consagrado na legislação, ou uniformemente sedimentada na doutrina e jurisprudência. Nesse paradigma, Ramos alude que:

> "a prática de crimes na internet assume várias denominações, entre elas, crime digital, crime informático, crime informático-digital, high technology crimes, computer related crime. Não existe consenso quanto à expressão, quanto à definição, nem mesmo quanto à tipologia e classificação destes crimes, contudo, atendendo aos

[276] DIAS, Figueiredo Dias. ob. cit. p. 253.
[277] A expressão "ciber" exprime a noção de Internet ou de comunicação entre redes de computadores.
[278] NASCIMENTO, Samir de Paula, ***Cibercrime: conceitos, modalidades e aspectos jurídicos-penais***. Disponível em: https://ambitojuridico.com.br/cadernos/internet-einformatica/cibercrime-conceitosmodalidades-e-aspectosjuridicos-penais/. Apud SOBRINHO, Jéssica Rafaela Nunes; et.al, ***ob. cit.*** p. 3.
[279] FRANÇA, Leandro Ayres; QUEVEDO, Jéssica Veleda; FONTES, Jean de Andrade; SEGATTO, Anderson José da Silva; ABREU, Carlos Adalberto Ferreira de; SANTOS, Diego da Rosa dos; VIEIRA, Luana Ramos, "***Projeto Vazou: pesquisa sobre o vazamento não consentido de imagens íntimas no Brasil"***. Revista Brasileira de Ciências Criminais, v. 169, ano 28. p. 231-270. São Paulo: RT, jul. 2020. ISSN 1415-5400. Apud SOBRINHO, Jéssica Rafael Nunes; et.al, ***ibidem,*** p. 3
[280] SILVA RODRIGUES, ***Direito Penal Especial, Direito Penal Informático-Digital***, Coimbra, 2009, p.168-194; SOFIA CASIMIRO, ***A responsabilidade civil pelo conteúdo da informação transmitida pela Internet,*** Coimbra, Almedina, 2000, p. 19. Apud DIAS, Vera Elisa Marques – A problemática da investigação do Cibercrime. p. 65, disponível em http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf, consultado em 29-01-2014 42 VENÂNCIO, Pedro Dias, ***- Lei do Cibercrime - anotada e comentada***, p. 16 Apud RIBEIRO, Maria da Conceição Fernandes, ***ob. cit.*** p.14.

> diversos instrumentos legislativos, consideramos ser de especial interesse utilizar a denominação de cibercrime"[281]

De acordo com a Comissão Europeia, Cibercrime

> "são os actos criminosos praticados com recurso a redes de comunicação electrónicas e sistemas de informação ou contra este tipo de redes e sistemas". Esta realidade consegue abarcar as formas tradicionais de crime, publicação de conteúdos ilícitos em meios de comunicação electrónicos, e crimes exclusivos das redes electrónicas, isto é, ataques contra sistemas de informação, bloqueio de serviços e pirataria. Sendo que "os crimes podem ser praticados em grande escala e pode ser muito grande a distância entre o acto criminoso e os seus efeitos"[282].

Decorrente da discussão conceptual, apresentamos aqui diversas definições do cibercrime existentes no nosso mundo académico. Neste sentido, Garcia Marques e Lourenço Martins alertam para o facto de inexistir uma definição concreta de "criminalidade informática", e acrescentam que "é frequente encarar a criminalidade informática como todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é alvo simbólico desse acto ou em que o computador é objecto do crime"[283].

Por seu turno, na Convenção sobre o cibercrime, na alínea a) do artigo 1.º é-nos apresentado o conceito de sistema informático, tendo "(...) como elemento fulcral um ou mais computadores podendo ser constituídos por dispositivos de qualquer tipo, desde que estejam interconectados ou relacionados e processem dados de forma automática, através de utilização de um programa".

Por sua vez, Casabona define Cibercrime como:

> *"el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual"[284].*

Para Verdelho, o termo "Cibercrime" define de forma genérica uma panóplia de crimes praticados com recurso a novas tecnologias de informação e de comunicação, ou seja, cabem naquele conceito actuações criminais clássicas, mas também novos crimes. Deve distinguir-se

---

[281] RAMOS, Alícia Castro; et al, *A Fragilidade do Ordenamento Jurídico Quanto ao Cibercrime: criminosos por trás de uma tela, Vítimas expostas em suas vidas*.Revista da Humanidade, Ciências e Educação – REASE, São Paulo (SP), p.8.n.11. nov. 2022. ISSN-2675 – 3375. p. 1494.

[282] Conforme Boletim da Ordem dos Advogados, mensal n.º 65, Abril 2010. CIBERCRIME "pode ser muito grande a distância entre o acto criminoso e os seus efeitos". p.36, disponível em http://www.oa.pt/upl/%7B3d49f105- 1ff4-426f-8c50-ddaee1b8acbb%7D.pdf, consultado em 26-11-2013. Apud RIBEIRO, Maria da Conceição Fernandes, ***ob.cit***. *p*.14 .

[283] In GARCIA MARQUES E LOURENÇO MARTINS, *Direito da informática*, 2.ª ed., Almedina, Coimbra, 2006, pp. 639 e ss. APUD VENÂNCIO, Pedro Dias, LEI DO CIBERCRIME, ANOTADA E COMENTADA, 1.ª ed., Coimbra Editora, p. 16. Apud RIBEIRO, Maria da Conceição Fernandes, ***ob. cit***. p.14.

[284] DÍAZ, Leyre Hernández, ***Aproximación a un concepto de derecho penal informático***, in DERECHO PENAL INFORMÁTICO, Primera edición, 2010, Civitas, Editorial Aranzadi, ISBN 978-84-470-3429- 1, p.44. Apud RIBEIRO, Maria da C. Fernandes, ***ob. cit.*** p.15.

a "criminalidade informática" (a informática é alvo do crime) da "criminalidade praticada com recurso a meios informáticos" (a informática é meio de execução do crime)"[285].

Segundo Dias, "os crimes de sabotagem informática, crime de dano relativo a dados ou programas informáticos, e o crime de intercepção ilegítima, são "crimes informáticos técnicos", que se podem definir como "as condutas criminalmente desvaliosas, simultaneamente praticadas com a utilização técnica de estruturas e sistemas informáticos e em que estes bens constituem o objecto da acção, lesando o bem jurídico segurança dos sistemas informáticos"[286]. O mesmo autor refere-se à criminalidade informática como sendo criminalidade levitacional ("a criminalidade informática é levitacional por oposição à criminalidade tradicional")[287], sendo os tipos levitacionais de cariz técnico a sabotagem informática, o acesso ilegítimo e a intercepção ilegítima[288].

A cibercriminalidade consiste num facto praticado com recurso às tecnologias de informação[289] e pode abarcar inúmeras condutas ilícitas,

> "*desde el delito económico, como el fraude informática, el robo, la falsificación, el computer hacking, el espionaje informático, el sabotaje, la extorsión informática, la piratería comercial y otros crímenes contra la propiedad intelectual, la invasión de la intimidad, la distribución de contenidos ilegales y dañosos, la incitación a la prostitución y otros crímenes contra la moralidad, y el crimen organizado (Rodríguez Bernal, 2007: 9). Pero a diferencia de otros tipos de delitos, el cibercrimen se vale del ciberespacio para realizar sus actividades delictivas."*[290].

Neste contexto, Cassanti afirma que "toda actividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa actividade são: crime informático, crimes electrónicos, crime virtual ou crime digital"[291].

---

[285] VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes – ***Leis do Cibercrime***, Vol. 1, pp. 27-28, disponível em http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdoCibercrime1.pdf, consultado em 22-12-2013. Apud RIBEIRO, Maria da Conceição Fernandes, ibidem. p.15.

[286] DIAS, Pedro Simões, ***O "Hacking" enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo direit***, in Direito da Sociedade da Informação, vol. VIII, Coord. Prof. Doutor José de Oliveira Ascenção, Coimbra Editora, 2009. ISBN 978-972-32-1710-0,p. 232. Apud RIBEIRO, Maria da C. Fernandes, ***ibidem***. p.16.

[287] ibidem.

[288]ibidem.

[289] SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos, CYBERWAR: ***O fenómeno, as tecnologias e os actores, p. 5.*** Apud Ribeiro, Ibidem**,** p.16.

[290] MEDERO, Gema Sánchez. Cibercrimen, ***Ciberterrorismo y Ciberguerra: Los Nuevos Desafíos Del s. XXI. 239- 267***. Revista Cenipec. 31.2012. Enero- Diciembre. ISSN: 0798-9202. pág 244, disponível em http://www.saber.ula.ve/bitstream/123456789/36770/1/articulo9.pdf, consultado em 25-08-2014. Apud Ribeiro…Ibidem. p.16.

[291]CASSANTI, M, ***Redes de indignação e esperança: Movimentos sociais na era da internet.*** Rio de Janeiro: Jorge Zahar, 2014. p.3. Apud RAMOS, Alícia Castro; et al, ***A Fragilidade do Ordenamento Jurídico Quanto ao***

A criminalidade informática apresenta dois sentidos: sentido amplo e sentido estrito. Nessa perspectiva, Silva dissertando sobre este assunto afirma que "Em sentido amplo, a criminalidade informática engloba toda actividade criminosa realizada por computadores ou meios de tecnologia da informação"[292]. "Em sentido estrito, a criminalidade de informação engloba os crimes, de acordo com Simas "quem que o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital". Dessa forma, Simas definiu o cibercrime como sendo "as infracções penais praticadas no âmbito digital ou que estejam envolvidos com a informação digital, mediante as condutas atentatórias à direitos fundamentais, de pessoas físicas e pessoas jurídicas através dos mais diversos meios e dispositivos conectados à internet, tais como computadores, celulares e outro"[293].

No nosso entendimento, a informática pode ser um instrumento de práticas de crimes tradicionais, isto é, que não necessitam de suporte informacional para serem realizados, nem mesmo sendo parte legal. Nesse corolário, podemos citar crimes cometidos a honra e a dignidade da pessoa humana, que podem ser cometidos com recurso em meio informático para divulgação (e-mail, whatsap e outros). Outros casos que se podem inferir são situações em que a informática surge como "elemento integrador, isto é, podendo o bem jurídico protegido não ser unicamente com a informática, como é o caso de crimes contra *softwares* em que o bem jurídico protegido é autoral. Nisso, ilidimos que Cibercrimes são os delitos penais cometidos por meio digital ou que estejam envolvidos com a informação digital.

Verdelho[294] reconhece três grupos distintos naquilo que vulgarmente se vê referido como cibercrime: os crimes que recorrem a meios informáticos (abrange infracções descritas no Código Penal e, portanto, sistematicamente não autonomizadas, tais como a devassa por meio da informática e o crime de burla informática e nas comunicações); os crimes referentes à protecção de dados pessoais de que se prevê ilícitos criminais específicos; e os crimes informáticos propriamente ditos.

Cibercrime: criminosos por trás de uma tela, Vítimas expostas em suas vidas. Revista da Humanidade, Ciências e Educação – REASE, São Paulo (SP), p.8. n.11. nov. 2022. ISSN-2675 – 3375. p. 1494.

[292] SILVA, Paulo Quintiliano da, ***Dos Crimes Cibernéticos e seus efeitos internacionais***. Procedings of the Firts International Conference on Forensic Computer Science Inv estigation (ICoFCS´2006)/ Departamento de Polícia Federal (ed.) Brasília, Brazil, 2006,124 pp.- ISSN 19180-1114. Apud SOBRINHO, Jéssica R. Nunes; et.al, ob. cit. p. 3.

[293] SIMAS, Diana Viveiros de, ***O cibercrime***. 2014. 168f. Dissertação (Mestrado em Ciências Jurídicoob.citForenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa, 2014. Disponível em: http://hdl.handle.net/10437/5815. Acesso em: 18 maio 2021. Apud SOBRINHO ….. ibidem, p. 3

[294] VERDELHO, Pedro, "Cibercrime***", in Direito da Sociedade da Informação*** (IV), pp. 356-368. Apud RIBEIRO, Maria da C. Fernandes, ob. cit. p.17.

Martins ensina-nos que são muitos, e os mais variados "modus operandi" neste tipo de criminalidade, mencionamos de seguida alguns dos mais conhecidos:

> A "técnica do salame", onde o autor retira pequeníssimas importâncias de várias contas (cêntimos) de terceiros, com pouca alteração dos saldos, movimentando-as para uma conta em seu nome ou de um cúmplice54. A "bomba lógica" ou "programa-crash", que consiste em instruções clandestinas para actuação em determinado momento, logo que verificada certa condição ou evento. O "Vírus", que é um conjunto de instruções que se podem reproduzir rapidamente, e que levam à inutilização de dados, ficheiros e programas, ou mesmo à paralisação de um sistema informático. O "Phishing"[295], que em linguagem de computação, "(...) é uma forma de fraude electrónica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos; senhas, dados financeiros como número de cartões de crédito e outros dados pessoais. O acto consiste em um fraudador se fazer passar por uma pessoa ou empresa confiável enviando uma comunicação electrónica oficial. Isto ocorre de várias maneiras, principalmente por e-mail, mensagem instantânea, SMS, dentre outros. Como o nome propõe (Phishing), é uma tentativa de um fraudador tentar "pescar" informações pessoais de usuários desavisados ou inexperientes"[296].

Para além dos "*modus operandi"* apresentados por Martins, temos o "Pharming", através de *spam* do correio electrónico, envia ficheiros ocultos, que se auto-instalam nos computadores ou sistemas informáticos das vítimas e que uma vez instalados, alteram de modo oculto e automático, os arquivos do sistema. Desde logo ficheiros que contém os favoritos e o registo de cookies[297]. O objectivo final visa que quando o utilizador acede a um determinado *site*, o sistema reencaminha-o para um outro *site* semelhante, mas falso[298] de forma muito semelhante ao Phishing;

Outro *"modus operandi*" é "Keylogger" é um programa que, uma vez instalado no computador, passa a identificar todas as nossas batidas no teclado e, assim, quando escrevemos

---

[295] "Esta actividade é facticamente complexa e traduz-se, antes de mais, na remessa massiva de mensagens de correio electrónico (utiliza portanto a técnica do spam). Tais mensagens incluem um link para uma página na WWW. Esta página será normalmente a reprodução aproximada de uma outra (esta autêntica), por exemplo de um banco ou de uma entidade emissora de cartões de crédito. Conterá elementos identificadores da entidade autêntica e imagens a ele referentes. Porém, será falsa, por ser construída e gerida por terceiros, sem autorização da entidade cujos sinais pretende imitar. Se a vítima usar o link para aceder à página falsa, deparar-se-à com uma página parecida com a do seu banco, ou da entidade gestora do seu cartão de crédito. Desta forma, os criminosos obtêm dados confidênciais que lhes permitirão aceder às contas bancárias das vítimas, transferindo o dinheiro que aí houver para contas suas. Ou utilizar os respectivos cartões de crédito, em seu proveito." VERDELHO, Pedro, ***ob. cit***, p. 413. Apud RIBEIRO…….., ***ob. cit.*** p.17

[296] MARTINS, A. G. Lourenço, ***Criminalidade Informática, Direito da Sociedade da Informação***, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, pp.13-14. Apud RIBEIRO…ibidem.. p.17.

[297] É "um pedaço de informação que um site da web pode colocar no disco rígido do seu computador, para (por exemplo) "reconhecê-lo" num futuro acesso. Um cookie pode ser utilizado para manter um rastreio das suas visitas num site. Normalmente, é necessárioautorizar a gravação de cookies, mas isso depende da configuração de cada browser. MATOS, José A. ***de, dicionário de informática e novas tecnologiaspp.95-96***. Apud RIBEIRO, ,,ibidem p.18)

[298] RIBEIRO,…..ob. cit. p.18.

um endereço electrónico (link) no nosso browser, ele envia essa informação ao seu detentor ou criador, que pode estar em qualquer parte do mundo[299] .

Por último, ataques do tipo Distributed Denial of Service ou DDoS são capazes de levar a que *websites* e redes fiquem indisponíveis[300].

Desta forma, é do nosso entendimento, partindo dos pressupostos referenciados nos parágrafos anteriores, que os ataques na internet podem ocorrer com o emprego de técnicas diversificadas, visando alvos diferentes e por inúmeros objectivos, pois a internet não só cria a oportunidade para o cometimento de novos delitos, como também potencializa os crimes já existentes.

As razões que motivam os cibercriminosos a esses ataques, consoante a Gisele[301], variam de uma mera diversão até a concretização de actos criminosos, como é exposto a seguir:

a) **Demonstração de poder:** mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente.

b) **Prestígio:** vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar *sites* considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo.

c) **Motivações financeiras:** colectar e utilizar informações confidenciais de usuários para aplicar golpes.

d) **Motivações ideológicas:** tornar inacessível ou invadir *sites* que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia.

e) **Motivações comerciais:** tornar inacessível ou invadir *sites* e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas.

---

[299] GLENNY, Misha, DARK MARKET, ***Como os hackers se tornaram a nova máfia, do autor do bestseller*** McMÁFIA, traduzido por Michelle Hapetian, ***civilização*** Editora, 2012, ISBN 978-972-26-3443-4, p. 49. Apud RIBEIRO,... ibidem, p.18.

[300] ibidem

[301] PACHECO, Gisele Freitas, ***Crimes virtuais e a legislação penal brasileira***/ COSTA, Renato Lopes. Revista Electrónica de Ciências Jurídicas. 2018. p. 16.

Assim sendo, para chegar ao fim almejado, os cibercriminosos usufruem de tácticas como, exploração de vulnerabilidade[302], varredura em redes[303], falsificação de correio electrónico[304], interceptação de tráfego, força bruta[305], desfiguração de página[306], negação de serviço[307], dentre outras formas.

Nesta mesma perspectiva, é sabido que legislar sobre o Direito Electrónico é muito delicado, uma vez que se não houver uma devida redacção do tipo penal é bem provável que possa punir uma pessoa inocente. Além disso, sabe-se que as testemunhas dos crimes digitais são as próprias máquinas e elas não sabem diferenciar um crime praticado com dolo de um praticado com culpa, em outras palavras, os computadores não sabem informar sobre o contexto da situação. Este facto acaba levando a punição indevida do agente.

3.2.2. O Bem Jurídico Protegido pelos Crimes Cibernéticos

A natureza do Direito Penal está intrinsecamente ligada à existência de violência e de excessos que gravemente ofendem o convívio em sociedade. Nesse corolário, no entendimento do Bittencourt[308], "modernamente a criminalidade é um fenómeno social normal, que não ocorre somente na maioria das sociedades de uma ou outra espécie, mas, sim, em todas aquelas constituídas por seres humanos". Utilizando-se dos ensinamentos de Durkheim, considerado um dos pais da Sociologia, o autor explica que: (...)

> "o delito não só é um fenómeno social normal, como também cumpre outra função importante, qual seja, a de manter aberto o canal de transformações de que a sociedade precisa. Sob um outro prisma, pode-se concordar, pelo menos em parte, com Durkheim: as relações humanas são contaminadas pela violência, necessitando de normas que as regulem. E o fato social que contrariar o ordenamento jurídico constitui

[302] É definida pelo CERT como uma condição que, quando explorada por um cibercriminoso, pode resultar em uma violação de segurança.
[303] Varredura em redes ou scan, conforme o CERT, é uma técnica que consiste em efectuar buscas minuciosas em redes, com o objectivo de identificar computadores activos e colectar informações sobre eles.
[304] Segundo CERT, a Falsificação de e-mail, ou e-mail spoofing, é uma técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.
[305] Conforme CERT, um ataque de força bruta, ou brute force, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.
[306] Desfiguração de página, defacement ou pichação, conforme definição do CERT, é uma técnica que consiste em alterar o conteúdo da página Web de um site.
[307] Negação de serviço, ou DoS (Denial of Service), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Conforme definição do CERT.
[308] BITTENCOURT, Cezar. Roberto, ***Tratado de Direito Penal***: Parte Geral, 1. São Paulo: Saraiva, 2011, p. 46. Apud SALES, Marcos Levy Gondim, ***A comprovação da materialidade e da autoria nos crimes virtuais.*** Monografia apresentada na Faculdade de Direito da Universidade Federal do Ceará, Fortaleza, 2013, p. 15.

> ilícito jurídico, cuja modalidade mais grave é o ilícito penal, que lesa os bens mais importantes dos membros da sociedade"[309].

Dos ensinamentos dos dois autores, subjaz a ideia de que é fundamental a identificação das condutas humanas cuja gravidade atente contra a ordem social como um todo, cominando, as sanções correspondentes à execução do acto criminoso. Essa tarefa é atribuída ao Direito Penal como "parte do direito público com as penas cominadas para factos que atentem contra a ordem, infracções e as sanções punitivas que lhes correspondem; direito criminal"[310]. De tal modo, busca-se a prevenção da ocorrência de novos delitos e a repressão directa contra o infractor, confluindo ao anseio da sociedade de ver o transgressor da lei respondendo devidamente pela prática de actos, cuja ilicitude recai sobre os bens tidos como os mais valorosos para o ordenamento jurídico[311]. De facto, "em cada situação histórica e social de um grupo humano os pressupostos imprescindíveis para uma existência em comum se concretizam numa série de condições valiosas como, por exemplo, a vida, a integridade física, a liberdade de actuação ou a propriedade, as quais todo o mundo conhece; numa palavra os chamados bens jurídicos; e o direito penal tem que assegurar esses bens jurídicos, punindo a sua violação em determinadas condições"[312].

Por sua vez, Muñoz Conde[313] conceptua "os bens jurídicos como sendo os pressupostos de que a pessoa necessita para sua auto-realização na vida social". A par das diversas definições jurídicas existentes, o que parece ser evidente é que não são todos os "bens" que serão considerados jurídicos, assim como não são todos os bens jurídicos que são tutelados pelo Direito Penal, por força dos princípios da subsidiariedade[314] e da

---

[309] SALES, Marcos Levy Gondim, ***A comprovação da materialidade e da autoria nos crimes virtuais***. Monografia apresentada na Faculdade de Direito da Universidade Federal do Ceará, Fortaleza, 2013, pp. 15-16.
[310] GUIMARÃES, Deocleciano Torrieri,…. Apud SALES, ob., Cit., p.16.
[311] Ibidem, p. 16.
[312] ROXIN, Claus, ***Problemas Fundamentais de Direito Penal.*** Tradução de Ana Paula dos Santos Luís Natscheradetz. 3ª ed. Vegas: Lisboa, 1998. p. 27/28. Apud Apud VIANA, Lucas Freitas, ***Segurança Jurídica como um bem jurídico-penal***. Disponivel no https://www.jusbrasil.com.br/artigos/a-seguranca-informatica-como-um-bem-juridico-penal/1661329789. Acessado no dia 26 de Dezembro de 2023
[313] PRADO, Luiz Regis, ***Bem Jurídico-penal e Constituição***. 8 ed. Rio de Janeiro: Forense, 2019, p. 22. Apud VIANA, Lucas Freitas, ***ibidem.***
[314] O princípio da subsidiariedade, impõe a utilização do Direito Penal em ultima ratio. Será legítima a intervenção estatal penal apenas quando outras formas de controlo social – sejam jurídicas ou não – se revelarem inaptas e insuficientes. O Direito penal, por ser a intervenção estatal mais invasiva e danosa, deve ser, sempre e necessariamente, o último recurso a se recorrer. (DANIEL, Rogério de Carvalho Veiga; et al, ***Função Simbólica do Direito Penal e o Princípio da Intervenção Mínima***. Programa de Apoio à Iniciação Científica - PAIC 2013-2014. In cadernopaic.fae.edu. p.440)

fragmentariedade[315]. Tais fundamentos derivam do princípio da intervenção mínima[316], que conforme lição de Junqueira e Vanzolini,

> o Direito Penal deve ser o último recurso ao qual o Estado recorre para proteger determinados bens jurídicos e somente quando outras formas de controlo não forem suficientes para alcançar tal resultado, de maneira que, só se justifica a acção de tal área quando as demais se mostrarem insuficientes (princípio da subsidiariedade) e somente os bens jurídicos seleccionados serão tutelados pelo Direito Penal (fragmentariedade) [317].

É importante destacar que segundo Luiz Regis Prado[318], "em um Estado Democrático e social de Direito, não pode ser dissociada a tutela penal de um pressuposto bem jurídico, sendo que somente será considerada legítima, sob a óptica constitucional, quando for socialmente necessária, ou seja, quando imprescindível para assegurar as condições de vida, desenvolvimento e paz social, haja vista o fundamento maior da liberdade e da dignidade da pessoa humana.

Há que demarcar fronteiras entre os bens jurídicos tutelados pelo Direito Penal e os tutelados por outros ramos do Direito. Este posicionamento advém do facto de a resposta penal para as violações dos bens jurídicos tutelados ser, em regra, sempre mais severa, pois a área criminal lida com a liberdade do indivíduo, com medidas invasivas, às vezes utilizando-se a força pública, dentre outras, nessa conjectura.

Partindo do pressuposto levantado no parágrafo anterior, importa discorrer se as condutas violadoras de bens jurídicos informáticos merecem ter a protecção jurídica do Direito Penal pois, conforme afirma Crespo[319], "não há como deixar de se questionar se há

---

[315] O princípio da fragmentariedade determina que o Direito penal não deve atuar de modo indiscriminado e generalizado, mas selecionar bens jurídicos para ser objeto de tutela. Tal seleção deverá considerar a importância dos bens jurídicos para o desenvolvimento da vida em sociedade; portanto, somente os valores essenciais em termos sociais é que são dignos de tutela penal. (DANIEL, Rogério de Carvalho Veiga; et al. Função Simbólica do Direito Penal e o Princípio da Intervenção Minima. Programa de Apoio à Iniciação Científica - PAIC 2013-2014. In cadernopaic.fae.edu. p. 440).

[316] O princípio da intervenção mínima é também conhecido pela sugestiva nomenclatura de "ultima ratio". Assim, orienta o poder punitivo estatal a ficar restrito a casos de significativa importância e, mais, de extrema necessidade, sob pena de soar abusivo – e ilegal (DANIEL, Rogério de Carvalho Veiga; et al, ***Função Simbólica do Direito Penal e o Princípio da Intervenção Minima***. Programa de Apoio à Iniciação Científica - PAIC 2013-2014. In cadernopaic.fae.edu. p. 430. "Em um Estado social e democrático de Direito, a obediência ao princípio de intervenção mínima constitui um de seus limites. O Direito penal, como mecanismo de controle social, só deve atuar quando se produzem lesões ou perigos de lesão intoleráveis contra os bens jurídicos essenciais ao desenvolvimento do ser humano em sociedade (BUSATO, 2012, p. 280). Apud DANIEL, Rogério de Carvalho Veiga; et al, ***Função Simbólica do Direito Penal e o Princípio da Intervenção Minima***. Programa de Apoio à Iniciação Científica - PAIC 2013-2014. In cadernopaic.fae.edu. p. 431).

[317] JUNQUEIRA, Gustavo; VANZOLINI, Patrícia, ***Manual de Direito Penal: Parte Geral***. 7 ed. – São Paulo: Saraiva Educação, 2021, p. 45. Apud VIANA, Lucas Freitas, Segurança Jurídica como um bem jurídico-penal. Disponivel no https://www.jusbrasil.com.br/artigos/a-seguranca-informatica-como-um-bem-juridico-penal/1661329789. Acessado no dia 26 de Dezembro de 2023.

[318] PRADO, Luiz Regis, p. 55. Apud VIANA, Lucas Freitas, ***ob. cit.***.

[319] VIANA, Lucas Freitas….Ibidem

novos bens jurídicos referentes ao avanço tecnológico e, além disso, se é o caso de serem plenamente tutelados".

Certamente, as novas tecnologias proporcionaram inúmeros avanços à colectividade, sendo que as pessoas estão cada vez mais conectadas nas "redes" e as informações em geral passaram a ser mais valiosas, tanto para o indivíduo, quanto para as empresas e entidades governamentais. Contudo, noutra perspectiva, verifica-se que, em grande proporção, a informática passou a ser utilizada como um meio para o cometimento de crimes, além de fazer surgir novas condutas, relacionadas com a invasão de dispositivos electrónicos o que, em tese, implicam a violação de bens jurídicos individuais ou colectivos. É nesse âmbito que a segurança informática tem sido um tema tão relevante, não só na sociedade contemporânea, mas também no mundo corporativo que, segundo uma projecção feita pela Gartner, "empresa de consultoria executiva de referência internacional, seriam gastos apenas no ano de 2021, o montante de u$150,4 bilhões com tecnologia e serviços de segurança da informação e gerenciamento de risco, sobretudo por empresas e órgãos governamentais, o que demonstra a magnitude da temática"[320].

Na doutrina penal, é unânime a necessidade de tutelar os bens jurídicos informáticos para que haja protecção jurídica do Direito Penal. Na senda dessa reflexão, Rogério Greco[321] preceitua que a finalidade do Direito Penal é proteger os bens mais importantes para a própria sobrevivência da sociedade, nesse âmbito, Luiz Régis Prado[322] diz que "o pensamento jurídico moderno reconhece que o escopo imediato e primordial do Direito Penal radica na protecção de bens jurídicos – essenciais ao indivíduo e à comunidade". O termo bem jurídico é entendido como uma limitação ao poder punitivo do Estado.

Apesar de haver diversas definições para o conceito Bem Jurídico, de modo geral, vai haver sempre uma relação entre o Bem Jurídico e a limitação punitiva do Estado. É o que se extrai da reflexão de Francisco de Assis Toledo[323].

> Bem jurídico é aquele que esteja a exigir uma protecção especial, no âmbito das normas de direito penal, por se revelarem insuficientes, em relação a ele, as garantias oferecidas pelo ordenamento jurídico, em outras áreas extrapenais. Não se deve, entretanto, supor que essa especial protecção penal deva ser abrangente de todos os tipos de lesão possíveis. Mesmo em relação aos bens jurídico-penalmente protegidos,

---

[320] MOORE, Susan, ***Gartner prevê que gastos mundiais com segurança e gerenciamento de riscos excederão US $150 bilhões em 2021 (tradução livre).*** Gartner Group, 17/05/2021. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwidesecurity-a.... Acesso em 03 Disponivel no https://www.jusbrasil.com.br/artigos/a-seguranca-informatica-como-um-bem-juridico-penal/1661329789. Acessado no dia 26 de Dezembro de 2023.

[321] PADILHA, Palma, ***ob. cit.*** p. 16.

[322] ibidem, p.16.

[323] Ibidem, p. 16.

> restringe o direito penal sua tutela a certas espécies e formas de lesão, real ou potencial.

Ainda sobre o bem jurídico protegido pelos crimes cibernéticos, Luiz Regis Prado[324] destaca que todo delito deve lesar ou expor a perigo de lesão certo bem jurídico e se refere a este último como um ente (dado ou valor social) material ou imaterial haurido do contexto social, de titularidade individual ou meta individual reputado como essencial para a coexistência e o desenvolvimento do homem, e, por isso, jurídico-penalmente protegido. Como visto, entende-se que a função do Direito Penal, sob uma perspectiva individual, é a protecção de bens jurídicos, que são aqueles valores que devem receber maior protecção estatal.

Assim sendo, é importante entender o que são bens jurídicos e a função do Direito Penal, para que se possa aplicar e distingui-los às condutas, e, por conseguinte, defendê-las como criminosas ou não-criminosas no meio informatizado, uma vez que, a evolução cibernética trouxe novas ideias quanto a bens jurídicos e isso influencia uma possível classificação sobre o que sejam crimes cibernéticos. Sendo assim, cabe questionar se há novos bens jurídicos referentes ao avanço tecnológico, porque se houver novos bens jurídicos, os crimes digitais não se limitarão somente aos bens jurídicos tradicionalmente tutelados. Haverá a possibilidade de lesão a outros bens jurídicos, que surgem de condutas ilícitas praticadas por meio da informática. Isso quer dizer que as condutas não serão restritas aos valores que são juridicamente protegidos, como a vida, a integridade física, o património, a fé pública, mas também, a outros valores como segurança de sistemas, informações armazenadas, redes de telecomunicações, etc. A informação, que antes era comercializada apenas em papel (jornal, revistas, etc), hoje, já recebe tratamento de "mercadoria" propriamente dita, pois, actualmente é comercializada com facilidade e é valorizada como se de mercadoria se tratasse, em meio digital e composta por dados.

Ainda na questão dos novos bens jurídicos afectados pela criminalidade cibernética, Wilson Gomes e Lucas Reis[325] questionam se seriam a informação ou os dados, ou ainda os sistemas informáticos? Além disso, se a informação for considerada como bem jurídico novo a ser tutelado, ainda resta analisar o grau do prejuízo causado para que se possa tipificar as condutas. Essas questões ainda são complexas e ainda há muito o que discutir, para se chegar a um consenso doutrinário. É dessa feita, que nos ocorre continuar a busca de um entendimento em relação a matéria em debate - o bem jurídico protegido nos crimes cibernéticos.

[324] Ibidem, p. 17.
[325] PADILHA, Palma, ***ob. cit.*** p. 17.

Ainda na conceptualização do Bem Jurídico protegido, Guilherme de Souza Nucci[326], afirma que "o bem jurídico é o valor para o qual se outorga protecção jurídico-penal no caso concreto. É o escopo do Direito Penal, ao menos para criar normas incriminadoras." Desta forma, o bem jurídico apresenta-se como critério para o legislador, para valoração, no acto de criação ou eliminação de tipos penais, além de sua função primária como objecto protegido.

Na sua obra "*Die Normen und ihre Übertretung*"[327], publicada em 1872, Binding apresenta um conceito diferente de bem jurídico e a sua relação com a dogmática penal, apresentando o delito como sendo a "lesão a um direito subjectivo do Estado, havendo, contudo, total correlação entre a norma e o bem jurídico – a primeira sendo a única e definitiva fonte de revelação deste"[328].

Partindo da visão do Binding, acreditamos que ele desenvolve, portanto, uma concepção na qual a partir da norma penal o bem se revela no ambiente jurídico e que ao ser contrariada, constituía-se num injusto. Segundo a exposição de Santos,[329] acerca da relação entre a vontade da lei e a actividade do indivíduo que, para Binding, correm de maneira divergente, sendo que "toda proibição tem o mesmo objectivo: impedir que certas mudanças no mundo jurídico sejam precipitadas mediante acções humanas". É nessa perspectiva que Binding apresenta uma divisão dessas proibições em três categorias para se alcançar uma concretização do objectivo supracitado, que são desenvolvidos por Santos nos seguintes termos:

> "O primeiro formado pela proibição de resultado indesejável por si mesmo. O segundo, pela proibição da colocação em perigo de bens protegidos antes da ocorrência de sua violação geralmente possível. O terceiro, pela proibição de ações que não consideram resultados reais, mas apenas o cuidado com a sua possibilidade, ou seja, a proibição da desobediência não por ela causar um estado de contrariedade a um interesse e sim pela própria desobediência. Binding afirma que a comparação dessas três espécies de ações proibidas com o seu conteúdo, a proibição de realização, permite observar que o interesse do direito é contrariado pelo estado produzido pela ação proibida, enquanto o estado prévio à ação corresponde a esse interesse. Isso significa que todos esses estados que não devem ser suplantados por meio de sua modificação têm um valor para o direito e podem ser denominados de "bens jurídicos".[330]

Na visão de Santos, os bens jurídicos podem ser entendidos como sendo o interesse do direito enquanto não ofendido por alguma das acções alvo dos grupos de proibição, mantendo-

---

[326] NUCCI, Guilherme de Souza, ***Curso de Direito Penal: Parte Geral.*** 3. ed. rev. atual. e aum. Rio de Janeiro: Forense, 2019. 1397 p. v. 1. ISBN 978-85-309-8311-6. Apud MIRANDA, Bruno Silvão, ***Os bens jurídicos Tutelados pelos Crimes Informáticos na Legislação Brasileira***, Centro Universitário FG – Artigo Científico, Guanambi, BA, Brasil, 2021. p.8.

[327] "normas e sua infração"

[328] MIRANDA, Bruno Silvão, ***ob. cit.*** p.10.

[329]MIRANDA, Bruno Silvão, ***ob.cit.***. p.10.

[330] Ibidem, p.10.

se nesse estado prévio. Justifica-se, portanto, a sua protecção, visto que caso ocorra lesão a um direito subjectivo do Estado, estará configurado o delito na concepção de Binding.

A perspectiva acentuada por Binding, no parágrafo anterior, encontra uma conexão profunda no pensamento do Prado, na medida em que um "Estado Democrático e social de Direito não pode ser dissociada a tutela penal de um pressuposto bem jurídico, sendo que somente será considerada legítima, sob a óptica constitucional, quando for socialmente necessária, ou seja, quando imprescindível para assegurar as condições de vida, desenvolvimento e paz social, haja vista o fundamento maior da liberdade e da dignidade da pessoa humana".[331]

Assim sendo, os crimes informáticos reflectem novos interesses, essencialmente no âmbito social a serem protegidos pelo Estado. Nessa perspectiva, há toda uma necessidade pela tutela penal de bens jurídicos emergentes, oriundos de avanços tecnológicos. Por isso, este nosso entendimento pode ser harmonizado com o enfoque de Viana, quando alude que "as novas tecnologias proporcionaram inúmeros avanços à colectividade, sendo que as pessoas estão cada vez mais conectadas nas "redes" e as informações em geral passaram a ser mais valiosas, tanto para o indivíduo, quanto para as empresas e entidades governamentais. Contudo, noutra perspectiva, verifica-se que, em grande proporção, a informática passou a ser utilizada como um meio ao cometimento de crimes, além de fazer surgir novas condutas relacionadas à invasão de dispositivos electrónicos o que, em tese, implicam em violação de bens jurídicos individuais ou colectivos" [332].

É certo que o bem jurídico em questão é a segurança informática. Em uma abordagem constitucional da segurança informática, é possível vislumbrar que há uma preocupação com "a protecção de dados pessoais constantes de registos informáticos, as condições de acesso aos bancos de dados, de constituição e utilização por autoridades públicas e entidades privadas destes bancos de dados ou de suportes informáticos"[333]. Nota-se um interesse, em todos os âmbitos, sejam eles sociais, económicos, culturais entre outros, a serem protegidos pelo Estado, quando o legislador legiferante "proíbe a utilização de meios informáticos para registo e tratamento de dados, individualmente identificáveis relativos às convicções políticas, filosóficas ou ideológicas, à fé religiosa, à filiação partidária ou sindical e à vida privada"[334].

[331] VIANA, Lucas Freitas, ***ob. cit***…
[332] VIANA, Lucas Freitas, .
[333] Cfr., nº 2 do art. 71 da CRM.
[334] Cfr., nº 1 do art. 71 da CRM.

Na perspectiva da norma constitucional em alusão, há toda necessidade da tutela penal de bens jurídicos emergentes, oriundos de avanços tecnológicos.

Dentro da abordagem constitucional, o Estado estabelece o direito à protecção dos dados pessoais, inclusive nos meios digitais, quando dispõe que "não é permitido o acesso a arquivos, ficheiros e registos informáticos ou de banco de dados pessoais de um para outro ficheiro informático pertencente a distintos serviços ou instituições, salvo nos casos estabelecidos na lei ou por decisão judicial".[335]

Em âmbito internacional, a Convenção de Budapeste (Convenção Sobre o Cibercrime)[336], que é um instrumento de cooperação internacional, aprimoramento legislativo, entre outras acções para o combate ao cibercriminalidade, de modo que, prevê no seu preâmbulo que a aludida convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, sendo que tais elementos sintetizam, conforme Sydow[337], o bem jurídico "segurança informática" e dizem respeito a:

> A) Integridade: os sistemas (operacionais e de redes sociais, por exemplo) e os dados produzidos pelos usuários, como documentos, mensagens, fotografias, filmes, criações intelectuais e assim por diante são património individual, original, e que, por isso, merecem ser protéticos em sua incolumidade. Apenas ao usuário autorizado cabe dispor sobre a inteireza de seus arquivos e suas modificações. Ataques às tais integridades informáticas, pois, são violações que fazem com que tais dados percam suas características originais, podendo levar prejuízos dos mais diversos.
> B) Confidencialidade: assim como há sigilo bancário e de comunicações, deve haver também sigilo acerca de dados. Afora situações de publicidade e transparência obrigatórias, se um usuário decide por não publicitar uma informação particular e de sua titularidade, esta deve permanecer protegida até que o titular dela disponha sobre tal e permita o acesso.
> C) Disponibilidade: além de sigilosos e deverem permanecer íntegros, há também a necessidade de que o usuário titular dos dados, sistemas e redes possa acessá-los livremente e no momento que desejar e precisar. Um usuário não autorizado não pode, portanto, impedir que o legítimo detentor dos direitos dos arquivos o acesso sob risco de frustrar a utilidade do arquivo, mesmo que integro e sigiloso."

As previsões constitucionais referenciadas no art. 71 da CRM servem apenas para ilustrar que existe certamente uma preocupação constitucional com os aspectos elementares nos quais a segurança informática objectiva proteger; ainda que não trate explicitamente da questão em debate - o bem jurídico protegido pelos crimes cibernéticos. Nesse corolário, há necessidade de a segurança informática ser tutela como o bem jurídico protegido pelos crimes

[335] Cfr., nº 3 do art. 71 da CRM.
[336] Conselho da Europa, ***Convenção sobre o Cibercrime***. Budapeste, 23 de de Novembro de 2001, disponível em: https://rm.coe.int/16802fa428. acessado nos dias 17 de Dezembro de 2023.
[337] VIANA, Lucas Freitas, ***ob. cit***.

cibernéticos e, consequentemente, exigir a intervenção do direito penal para que seja de carácter subsidiário e fragmentário. Outrossim no panorama internacional, partindo da Convenção de Budapeste, a preocupação assenta também na segurança informática como um bem jurídico, exigindo-se a necessidade de prosseguir com carácter prioritário uma política criminal comum, cujo objectivo circunscreve-se na protecção da sociedade contra a criminalidade no ciberespaço, por meio da adopção de legislação adequada e do aperfeiçoamento da cooperação internacional.

3.2.3. Classificação dos Crimes Cibernéticos

O progresso tecnológico reduziu distâncias, aproximou o mundo, através da possibilidade de comunicação instantânea com qualquer pessoa que esteja conectada a essa rede mundial interligada. Concordando com Padilha, "é facilmente perceptível que a sociedade digital está se tornando cada vez mais interligada com o mundo, e tornando estreitas as relações comerciais, económicas, políticas e sociais, fruto da evolução tecnológica"[338]. Nessa senda, apesar desta sensação de proximidade entre as sociedades, entre as pessoas, entre os mercados, percebe-se uma grande tendência da sociedade de ficar mais solitária, uma vez que podem-se pagar as contas e fazer compras *on-line*, sem ir ao banco etc.

Certamente a eficiência da tecnologia, velocidade no acesso e a disseminação da informação acrescentaram algumas peculiaridades no tratamento dos crimes virtuais. Estes tipos de crimes são caracterizados pela velocidade e novidade que, quando consideradas juntamente com a ofensa a um Bem Jurídico especial, exigem conhecimentos específicos para que se possa chegar aos indícios de autoria e materialidade da infracção penal. Actualmente, a internet tornou-se um ambiente para o cometimento de novos delitos e também como um novo meio para a prática de condutas ilícitas. Esses delitos cometidos no âmbito digital, muitas vezes são chamados por crimes cibernéticos, crimes digitais, crimes electrónicos, crimes da informática, crimes cometidos na internet, *cybercrimes*, fraudes electrónicas, delitos computacionais, dentre outros, mas todos eles referem-se à prática delituosa cometida no meio digital.

Assim, surge a necessidade de classificar os diversos tipos de crimes cometidos no meio ambiente digital. Nesse corolário, apresentamos as diversas classificações doutrinárias amplamente discutidos e apontados por diversos autores.

[338] PADILHA, Palma, ***ob. cit.*** p. 11.

Para Wendt et al[339], existem as acções prejudicais atípicas e os crimes cibernéticos. Na mesma referência, o autor disserta afirmando que as acções prejudiciais atípicas são aquelas condutas que causam prejuízo ou transtorno para vítima através da rede mundial de computadores, mas não são tipificados em lei.

No seu ensinamento, Wendt afirma que os crimes cibernéticos dividem-se em:

> "crimes cibernéticos abertos" e "crimes exclusivamente cibernéticos". Os "crimes exclusivamente cibernéticos" são aqueles que necessariamente precisam do meio da informatica para cometer tal crime (como é o caso do crime de invasão de dispositivo informático. Portanto os crimes cibernéticos abertos são aqueles que podem ou não ser praticados pelo meio informatico, como é o caso dos crimes de violação de direito do autor, pode ser praticado tanto no ambiente virtual como no analógico"[340].

Ainda no âmbito da discussão sobre a classificação dos crimes cibernéticos a outra parte da doutrina, encabeçada por Pinheiro, é apologista em estudar os crimes cibernéticos, levando em consideração o papel desempenhado pelo computador no contexto da prática do acto ilícito. Nesse sentido, conforme esclarece o autor:

> "(...) 1) quando o computador é o alvo – p. Ex.: crime de invasão, contaminação por vírus, sabotagem do sistema, destruição ou modificação de conteúdo do banco de dados, furto de informação, furto de propriedade intelectual, vandalismo cibernético, acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo por fora da empresa; 2) quando computador é o instrumento para o crime – ex.: crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores ou alterações de saldos e fraude de telecomunicações, divulgação ou exploração de pornografia; 3) quando o computador é incidental para outro crime – ex.: crimes contra honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis, registo de actividades do crime organizado; 4) quando o crime está associado com computador – p. Ex.: pirataria de software, falsificações de programas, divulgação, utilização ou reprodução ilícita de dados e programas de comércio ilegal de equipamentos e programas"[341]

Outra doutrina aponta que existem três tipos de classificações os puros, mistos e comuns. Assim explica Teixeira que "os primeiros são aqueles em que o sujeito visam especialmente o sistema de informática; as acções materializam-se, por exemplo, por actos de vandalismo contra a integridade do sistema ou pelo acesso desautorizado ao computador. O crime informático misto consubstancia-se nas acções em que o agente visa o bem

---

[339] WENDT, Emerson; et al, ***Crimes cibernéticos: ameaças e procedimentos de investigação***. Rio de Janeiro: Brasport, 2012. Apud TATEOK, Victor Augusto, ***Classificação dos Crimes Cibernéticos***. Artigo publicado no Jusbrasil, 2017. Disponível A https://www.jusbrasil.com.br/artigos/classificacao-dos-crimes-digitais/307254758. Acessado em 10 de Janeiro de 2024.

[340] Ibidem.

[341] PINHEIRO, Patrícia Peck, ***Direito digital***. 5. Ed. São Paulo: Saraiva, 2013. Apud TATEOK, Victor Augusto**,** ***Classificação dos Crimes Cibernéticos***. Artigo publicado no Jusbrasil, 2017. Disponível A https://www.jusbrasil.com.br/artigos/classificacao-dos-crimes-digitais/307254758. Acessado em 10 de Janeiro de 2024.

juridicamente protegido diverso da informática, porém o sistema de informática é ferramenta imprescindível. E os crimes de informática comum são condutas em que agente utiliza o sistema de informática como mera ferramenta, não essencial à consumação do delito".

Para Viana et al[342], existem quatro tipos de classificações de crimes digitais, nas quais, segundo os autores o principal Bem Jurídico a ser protegido pela Lei Penal nesses casos é a inviolabilidade da informação automatizada (dados). Nessa tipologia, os autores apontam como primeira classificação os crimes informáticos próprios: aqueles que o computador é usado como meio para executar o crime, mas não existe a inviolabilidade da informação automatizada (exemplos: ameaça, incitação ao crime e etc), os crimes informáticos próprios são aqueles em que o bem jurídico protegido pela lei penal é inviolabilidade de dados (Como é o caso do crime de invasão de dispositivo informático, inserção de dados falsos em sistema de informações e modificação e alteração não autorizada de sistema de informações. A segunda categoria na classificação, são os crimes mistos, aqueles que além de proteger a inviolabilidade de dados, a legislação visa proteger o bem jurídico de natureza diversa (crime eleitoral) e, por fim, o crime informático mediato ou directo é aquele considerado o delito fim não informático que herdou a característica do meio para consumar o crime.

Para outros autores como Crespo et al[343], existem duas modalidades: na primeira, fala-se de actos dirigidos contra o sistema da informática. Essa modalidade, para os autores, estes são os chamados de "crimes informáticos próprios", praticados por meio da informática, sem a informática o crime não ocorrerá (como é o caso do crime de inserção de dados falsos em sistema de informações. A segunda modalidade, portanto, são "crimes informáticos impróprios", podem ser praticados de várias formas, sendo ela por meio da informática ou não, como são os casos os crimes contra a honra e violação direitos do autor, estelionato, pornografia infantil dentre outros[344].

---

[342] VIANA, Tulio; MACHADO, Felipe, ***Crimes informáticos***. Belo Horizonte: Fórum, 2013, Apud TATEOK, Victor Augusto, ***Classificação dos Crimes Cibernéticos***. Artigo publicado no Jusbrasil, 2017. Disponível A https://www.jusbrasil.com.br/artigos/classificacao-dos-crimes-digitais/307254758. Acessado em 10 de Janeiro de 2024.

[343] CRESPO, Marcelo Xavier de Freitas, ***Crimes Digitais***. São Paulo: Saraiva, 2011. Apud TATEOK, Victor Augusto***, Classificação dos Crimes Cibernéticos***. Artigo publicado no Jusbrasil, 2017. Disponível A https://www.jusbrasil.com.br/artigos/classificacao-dos-crimes-digitais/307254758. Acessado em 10 de Janeiro de 2024.

[344] Castro alinha na mesma classificação em crimes cibernéticos próprios e impróprios, porém enquadra no âmbito do modus operandi. Nisso, os crimes digitais são classificados em próprios e impróprios. Segundo Castro[344], crimes digitais próprios são aqueles praticados exclusivamente através de sistemas informáticos, pois somente através desta, é que torna-se possível a execução e consequentemente a consumação do delito. Entretanto, tais crimes são tipos novos, que agridem sistemas de informática como bem juridicamente protegido, e, diante da

Nesta perspectiva, Crespo[345] fundamenta ainda aludido que os crimes digitais próprios também podem ser chamados de risco informático. Essa categoria de crimes digitais (próprios ou puros) são "condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra sistemas informáticos e os dados". Enquanto os impróprios com base exclusiva na categoria do bem jurídico referenciado pela norma, são "condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra bens jurídicos que não sejam tecnológicos, já tradicionais e protegidos pela legislação, como a vida, a liberdade, o património, etc.)".

Ressalta-nos afirmar que a classificação apresentada, distinguindo os delitos virtuais, foi com base na espécie de bem jurídico referenciado pela norma. Nesse corolário, os crimes digitais próprios seriam aqueles cujos bem jurídicos de referência são os "dados armazenados electronicamente", o que, conforme analisado, ressalta os problemas históricos de gradual espiritualização do conceito de bem jurídico e perda de seu rendimento na protecção ao acusado/investigado. Vale destacar que todas as etapas do processo de imputação devem estar sujeitas à possibilidade de refutação, em atendimento aos princípios do contraditório e da ampla defesa.

Do entendimento da dissertação de Crespo, nos reserva ainda aludir que os crimes digitais impróprios podem ser praticados de todo modo e ainda através de sistemas de informática. Desta forma, o agente que comete o delito, utiliza, esporadicamente, a informática. O computador funciona como um instrumento para a execução do crime. Estes são delitos que violam bens já protegidos por nossa legislação, como o património, a honra, a ameaça, como configurados no nosso Código Penal.

No caso dos crimes digitais próprios, segundo os argumentos do Crespo, "o que muda é o modo como se pratica a acção delitiva, pois só podem ser praticados através da informática, sendo não necessários conhecimentos técnicos específicos. Já os ilícitos digitais impróprios são aqueles que dependem de conhecimento técnico próprio do âmbito da computação. Enquadram-se nestes, os *hackers*, os *cracker*s, justamente por deterem maior conhecimento informático"[346].

escassez de legislação existente neste âmbito, alguns fatos não podem ser punidos por serem atípicos. (CASTRO, Carla Rodrigues Araújo de Crimes ***de Informática e Seus Aspectos Processuais***. Rio de Janeiro, Lumen Júris, 2003.). Apud PADILHA, Palma, ***Crimes.*** p.18

[345] CRESPO, Marcelo Xavier de Freitas, ***Crimes Digitais.*** São Paulo: Saraiva, 2011. Apud ESCÓSSIA, Radael de. Problemas genéricos de discurso jurídico-penal na [e sobre a] internet e outros ciberespaços: Uma revisão narrativa de literatura sobre crimes digitais. 2020. p.27. In ROCHA, Lilian; et al [org], ***Caderno de Pós´-Graduação em Direito: Crimes Digitais***. Instituto CEUB de Pesquisa e Desenvolvimento, Brasília, 2020. Disponível : https://www.repositório.uniceub.br. Acessado no dia 8 de Janeiro de 2024.

[346] PADILHA, Palma, **ob.cit**. p.18.

Há um aspecto a importante a reter no âmbito dos crimes digitais próprios, em que só poderá ser punido o agente que praticou o delito virtual, onde a informática é o meio e o fim desejado, havendo legislação específica, caso contrário, não será possível puni-lo pelas condutas ilícitas praticadas pelo computador. O que implica a observância do princípio da tipicidade no âmbito do direito penal.

Para Damásio Jesus[347], "os crimes electrónicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço 'real', ameaçando ou lesando outros bens, não-computacionais ou diversos da informática".

A doutrina costuma distinguir ainda os crimes quanto aos efeitos da conduta. Partindo desse pressuposto, classificam-se os crimes cibernéticos entre os chamados "crimes materiais" (ou de resultado), "formais" ou de "mera conduta". Essa diferença "corresponde à relação entre a acção e a modificação do mundo exterior, de tal sorte que se possa proceder a uma delimitação naturalística" entre as categoriais. Enquanto nos crimes materiais seria possível distinguir entre a acção e seus efeitos sensíveis "no mundo" (resultado naturalístico); nos outros a lei prescindiria da indicação de tais efeitos"[348].

Corroborando com Costa[349], essa distinção entre crimes próprios e impróprios é muito importante, porque através desta análise é que será possível concluir se a conduta ilícita é realmente criminosa ou mesmo discutir acerca da questão, com a finalidade de tipificar e punir tais condutas. Quanto aos crimes digitais impróprios, a semelhança entre este e o crime comum encontra-se no bem jurídico tutelado. Uma injúria, por exemplo, sempre atingirá a honra subjectiva da vítima, mesmo que praticada por meio do computador. O nosso ordenamento jurídico adoptou um modelo misto (próprios e impróprios).

3.2.4. Sujeitos dos Crimes Cibernéticos

3.2.4.1. Aspectos Preliminares

Segundo os ensinamentos do Nascimento, com o surgimento da internet e o avanço diário da tecnologia, a população não viveu apenas dos benefícios advindos da mesma, surgindo também os crimes cibernéticos. O cibercrime demonstrou seus primeiros indícios na década de 1960, momento em que se ouviu falar e passou a ser discutido sobre os diversos crimes

[347] Em: ALMEIDA, Maria Paula Castro,Apud ESCÓSSIA, Radael de, ob. cit.. p.27.
[348] TAVARES, Juarez, **…….** Apud ESCÓSSIA, Radael de, **ob. cit**. . p.27.
[349] COSTA, Fernando José da,... Apud PADILHA, ***Palma,….ob. cit.*** p.19

envolvidos com a nova tecnologia[350]. Todavia, não existe consenso geral ou uma definição clara sobre o que é um cibercrime, tendo em vista que os crimes que recorrem moderadamente à tecnologia e aos aparelhos digitais são estabelecidos nesta categoria[351] .

Como ainda se discutia as abundantes denominações para a mesma modalidade do crime, inúmeros doutrinadores definiram um conceito para o Cibercrime, assim,

> "Observou-se uma subdivisão, estabelecidas como espécies de cibercrimes, aqueles praticados por meio do computador, ao mesmo tempo que outros comportam apenas aqueles que alcançam directamente o computador. Logo, são diversos os nomes dados para definir uma infracção penal cometida através de um dispositivo ligado à rede de internet, entre eles, crime digital, crime informático digital, crime informático, crimes cibernéticos, criminalidade informática, high technology crimes, computer related crime, dentre outros. Não há um consenso quanto à sua denominação, quanto à sua definição, quanto à tipologia e nem classificação, porém, consideramos utilizar a denominação cibercrime[352]

Diante disso, de acordo com Barbai[353],

> "com a nomenclatura utilizada para denominar o presente trabalho, o termo cibercrime, originou-se na França, na cidade de Lyon. Durante a reunião de um subgrupo das nações do G8, que seria composto pelos países mais ricos e industrializados do mundo, que discutiu sobre os crimes praticados por dispositivos electrónicos conectados à internet, objectivando analisar os problemas relacionados à criminalidade em razão da ampliação desta rede".

Utilizando o termo cibercrime, Roque[354] afirma que se trata de "toda conduta, definida pela lei como crime, e que o computador tiver sido utilizado como instrumento de sua perpetração". O sujeito activo emprega, como forma de execução de sua infracção, ferramentas específicas da rede de computadores, valendo-se das habilidades tecnológicas voltadas para o uso desses dipositivos, não sendo especificamente um computador, uma vez que se trata de um sentido amplo, pois "a rede de computadores é um conjunto de diversos equipamentos com recursos facilitadores de comunicação"[355].

Em sentido lato, os crimes cibernéticos "englobam toda actividade criminosa através de computadores, entre outros meios de tecnologia"[356]. Já em sentido *stricto*, a criminalidade de informação "engloba os crimes, de acordo com" Simas[357], "quem que o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital". Dessa forma, definiu o cibercrime como sendo as infracções penais praticadas no âmbito digital ou

---

350 SOBRINHO, Jéssica Rafaela Nunes; et.al, ***ob. cit***. p. 3.
351 Ibidem, p. 3.
352 SIMAS, Diana Viveiros de,***O cibercrime***. 2014. 168f. Dissertação (Mestrado em Ciências Jurídico Forenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa, 2014. Disponível em: http://hdl.handle.net/1.p. 3.
529 SOBRINHO, Jéssica Rafaela Nunes; et.al. ***ob. cit***.p. 3.
354 Ibidem, p. 3.
355 SOBRINHO, Jéssica; et. al, ***ob., cit*** p.3.
356 Ibidem, p.3.
357 Ibidem, p.3.

que estejam envolvidos com a informação digital, mediante às condutas atentatórias aos direitos fundamentais, de pessoas físicas e pessoas jurídicas através dos mais diversos meios e dispositivos conectados à internet, tais como computadores, celulares e outros.

De acordo com a Comissão Europeia[358], "inclui-se no cibercrime três tipos de actividades criminosas, os crimes tradicionais cometidos com a assistência do computador e redes de informática, os crimes relativos ao conteúdo, com a publicação de conteúdos ilícitos por meios de comunicação electrónica, e os crimes exclusivos das redes de informação, que são cometidos exclusivamente por meio informático".

Na sua totalidade, as condutas ilícitas no meio virtual podem ser divididas em duas: acções ilícitas atípicas e crimes virtuais. Na primeira, não há previsão legal, ou seja, não sendo regida pelo código penal, podendo o causador ser responsabilizado apenas na esfera cível"[359]. No segundo, "esses crimes podem ser realizados de forma tradicional, isto é, por meio de computadores como é o caso dos crimes contra a honra, ou também, podem ser praticados com a utilização do computador ou alguma outra fonte com acesso à internet, por exemplo, no caso de clonagem de cartões por meio da internet"[360].

Assim sendo, trata-se de uma modalidade de crimes amplos, tanto como inúmeras denominações e, tal como, diversas especificidades, sejam elas, os tipos de actividades ilícitas, as divisões pelas espécies de crimes e como estão distribuídas no ordenamento jurídico. Sabendo-se que foi em 1960 em que se verificaram os primeiros indícios sobre essa modalidade de crimes. Repare-se que apresentava maiores incidências em casos de manipulação e sabotagem de sistemas de computadores [361]. Entretanto, foi apenas na década de 70 que os sujeitos activos dessas infracções penais ganharam destaque e ficaram conhecidos, naquele momento, como Hackers [362].

O termo *Hackers* foi usado de forma errónea, para referir-se à esses indivíduos que praticavam esses crimes tinham o conhecimento de informática ou melhores conhecimentos de programação de computadores para acessar as informações de qualquer usuário que esteja conectado na rede mundial de computadores. Mesmo com esses conhecimentos não deixaram de ser identificados como criminosos. "Já em 1980, houve um maior crescimento de outros tipos de crimes, não apenas envolvendo vírus e softwares, como exemplo o da pirataria e

[358] Ibidem, p.3.
[359] Ibidem, p.3.
[360] Ibidem, p.3.
[361] Ibidem, p.3.
[362] SOBRINHO, Jéssica; et. al, ob., cit p.3.

pedofilia online, gerando assim, certa preocupação com a segurança virtual" [363]. Todavia, foram os *Crackers* que deram início ao uso do computador para fins ilícitos, com uma nova modalidade de crimes, começando, assim, a burlar as leis e criar novos meios de agir contra outras pessoas, com a vantagem de não serem vistos, agindo anonimamente[364].

Evidencia-se, portanto, que as definições do cibercrime são extensas, bem como, sua origem foi percebida precedentemente, conquanto se trata de uma prática extremamente ampla, vez que o meio tecnológico permite infinitas possibilidades. Assim, é imperioso destacar a figura do sujeito que investe na prática do cibercrime, valendo-se dos conhecimentos tecnológicos e da desinformação dos ofendidos que são imensuráveis, tal como da sociedade em geral.

Para discutir a essência desses crimes, no ordenamento jurídico-penal, é essencial ter em conta alguns elementos do próprio crime: autoria e materialização do próprio acto delituoso e a questão das provas.

3.2.4.2. Sujeitos Activos ou Autoria dos Crimes Cibernéticos

Os crimes praticados no ambiente virtual diferem dos demais tipos de crime em razão do distanciamento físico entre o agressor e o ofendido; de facto, ao invés de uma acção física movida directamente à pessoa do ofendido, os criminosos cibernéticos utilizam-se de dispositivos electrónicos para emanar ordens de quebra de senhas, transferências de arquivos, dados, valores monetários etc., ou códigos criptografados que são convertidos em mensagens, tudo com o intuito de perpetrar o acto ilícito.

Em princípio, qualquer pessoa pode ser um sujeito activo dos crimes cibernéticos. Entretanto, para praticar um crime com um computador através da internet, é preciso ter algum conhecimento de informática por parte do infractor, pois, para invadir outro computador e ter acesso a arquivos e dados ou mesmo causar algum estrago, é preciso compreender o funcionamento daquele sistema informático que vai ser invadido, conseguir de alguma forma as senhas de acesso, e no mínimo, saber qual o conteúdo dos arquivos que se busca. Um agente invasor com este perfil é o sujeito activo do delito digital. Entende-se por sujeito activo o autor da infracção penal, a pessoa que, de forma directa ou indirecta, pratica a conduta descrita pelo tipo penal[365].

[363] Ibidem, p.3.
[364] Ibidem, p.3.
[365] NUCCI, Guilherme de Souza, ***Manual de direito penal***. 10. ed. rev., atual. e ampl. Rio de Janeiro: Forense, 2014.

Em relação ao sujeito activo, é um crime comum, quanto ao agente estes podem ter diversos níveis de gravidade, pode ser uma pessoa comum sem relevantes conhecimentos técnicos, tal como programação e internet, conquanto, pode ser uma pessoa com conhecimento técnico aprofundado. Como ensina Sobrinho *et al*, "Independente ainda de sua identificação, o sujeito activo do cibercrime é aquele que desfruta de sua inteligência e acessa os dispositivos com intuito de cometer delitos, inclusive, sem conhecimento tão robusto"[366].

Neste contexto, há que distinguir dois tipos de sujeitos nos crimes cibernéticos: "o agente activo com conhecimento superior de informação quanto à internet e seus sistemas, utilizando-o para praticar o crime típico causando prejuízos aos sujeitos passivos, para obter vantagem a si própria ou terceiros". Esses sujeitos activos apenas são conhecidos por dois termos: o *hacker* e o *cracker"*[367].

1. Hacker

O hacker não é propriamente o sujeito activo dos crimes cibernéticos. Mas é conhecido, pela maioria da população, como criminosos. Pois eles possuem conhecimento de informática e computação, são empenhados em desenvolver e modificar *softwares e hardwares* de computadores, trabalhando na área de informática e não necessariamente para cometer algum tipo de cibercrime.

A definição do termo *hacker* é controversa na doutrina, mas entendê-lo como uma pessoa com grande conhecimento na área de informática. É nessa linha de pensamento que, segundo Plantullo[368], "é uma pessoa física que detém, como objecto, a investigação da integridade e da segurança de um sistema qualquer de computador. Utiliza-se de técnicas avançadas para invadir sistemas e detectar suas respectivas falhas". Segundo este parafraseado, os *hackers* não são criminosos propriamente ditos, ou melhor como se pretende mostrar no seio da sociedade. Nessa perspectiva Bach nos ensina que os *hackers*

> "orientam seu potencial para construir, seu objectivo é compreender mais, não se utilizando do objectivo de destruir ou roubar dados deliberadamente, eles compartilham informações deixando impressões para que administradores de rede realizem correcções, pois os verdadeiros hackers são autodidactas, conhecem excessivamente hardware, redes, linguagens de programação, diversos sistemas operacionais, e exactamente os protocolos necessários "[369].

Assim, subjaz o entendimento de que os hackers não devem ser classificados como os criminosos perigosos no âmbito dos crimes cibernéticos. Mas olhar como sujeitos que

[366] SOBRINHO, Jéssica Rafaela Nunes; et.al, ***ob, cit.*** p. 4.
[367] Ibidem, p. 4.
[368] SALES, Marcos Levy Gondim, ***ob. cit.***, p. 40.
[369] SOBRINHO, Jéssica Rafaela Nunes; et al. ob. cit. p. 4.

empreendem o papel da evolução da informática, pelas suas capacidades intelectuais, pois, beneficiam todo o meio digital, descobrindo falhas de segurança nos softwares e auxiliam na reparação. Por isso, concordamos com os vários autores que afirmam que denominar como hackers aqueles que cometem os crimes cibernéticos, demonstra-se de forma bastante equivocada. Os hackers são pessoas que detêm largos conhecimentos na área da informática, sendo capazes de inventar ou modificar mecanismos tecnológicos.

2. Cracker

O *Cracker*, a seu turno, conforme definição apresentada pelo website da TechTarget[370], "é aquele que se especializa em invadir computadores de outras pessoas, normalmente por meio de acesso à mesma rede à qual pertence o alvo". O autor avança mais apontando que os Crackers "Podem burlar senhas ou licenças necessárias para a utilização de softwares pagos ou, em outra linha, invadem e superam a segurança de dispositivos electrónicos alheios". A finalidade do ataque de um cracker varia bastante, podendo ser ela delitiva, altruística ou pelo simples "prazer" de vencer o desafio".

Do entendimento da definição do Target, podemos exemplicar como casos de ataques de Crackers, envio de um programa malicioso, por *spam*, à caixa de e-mails de uma pessoa, que seja alvo escolhido do criminoso, que, após o download da pessoa, fica exposta à invasão do cracker, posteriormente, faz o uso de todos os dados constantes do seu computador. Neste exemplo, demonstra-se claramente que as acções dos Crackers visam, essencialmente, a obtenção de lucro de forma ilícita.

Como apregoa Rezende, o termo cracker foi criado por volta de 1985 pelos próprios Hackers, porque a imprensa empregava o termo "hacker" de forma equivocada para divulgar as acções criminosas realizadas por meio tecnológico[371]. Assim, o termo "cracker apareceu para designar um grupo de usuários que usaram seu rico conhecimento em informática para violar o sistema de segurança, códigos de criptografia e senhas de acesso à rede, com a intenção de invadir e sabotar para fins criminosos[372]. Destacam-se algumas designações para cada tipo de delito cibernético, isto é, a forma que utilizaram cometendo esses ilícitos, geralmente derivadas da língua inglesa, com tradução aproximadamente fiel à acção, conforme definições de Coriolano Aurélio de Almeida Camargo Santos – Director de Crimes de Alta Tecnologia da OAB:

---

[370] SALES, Marcos Levy Gondim, ***ob. cit.***, p. 41.
[371] SOBRINHO, Jéssica Rafaela Nunes;et al. ***ob. cit.*** p. 5.
[372] Ibidem, p. 5.

> "Dentre os novos delitos penais cometidos no mundo virtual, os chamados cibercrimes, destacam-se e nomeiam-se alguns a seguir. O "cracking" ou quebra de um sistema de segurança, de forma ilegal e sem ética, por um cracker. O "phishing scam", técnica que permite que piratas virtuais roubem informações de uma máquina com o objectivo principal de burlar transacções financeiras. Os actos de "gray hat" e de "black hat". A cor do chapéu define que tipo de acções o hacker pratica. Aquele de "chapéu branco" é um hacker ético. O "black hat" (chapéu preto) é o hacker antiético, também denominado cracker. O hacker "gray hat" (chapéu cinza) é aquele penetra um sistema sem, no entanto, lesá-lo, ferir sua confidencialidade ou praticar vandalismo […][373].

Os *Crackers* usam vários métodos para cometer os cibercrimes. Esses métodos estão relacionados aos tipos penais, como sejam de invasão de sistema de segurança de forma antiética, roubando informações importantes, e principalmente o que acontece com frequência no momento presente, que são os delitos envolvidos em transacções financeiras, dado que o meio tecnológico apresenta como o mais usual para a sua prática.

3.*Warez e Wannabe*

Para além dos *hackers e crackers*, são também conhecidos na arena dos cibercrimes os *Warez e Wannabe*. *Warez* - trata-se de "um indivíduo que aplica os conhecimentos informáticos para copiar programas de forma ilegal e para fins comerciais, algumas de suas actividades são compreendidas nas vendas de programas piratas"[374]. E tal como, o termo *Wannabe*, este é "quem sabe combinar algumas técnicas de ataques prontas e invadir sistemas frágeis. Como também, o termo Larva, que se refere àquele que consegue desenvolver suas próprias técnicas de ataque e penetrar em sistemas de nível de segurança médio. Eles estão considerados na fase de transição entre o *wannabe e o hacker*"[375].

4. Praeker e Lammer

Ainda no âmbito das denominações para acções delituosas específicas, existem outros termos, como *Preaker*, que designa aqueles que "burlam os sistemas de telefonia"[376], bem como o termo *Lammer,* aplicado para "as pessoas que não detêm o conhecimento necessário para desenvolverem suas próprias ferramentas e utilizam ferramentas desenvolvidas por outros para realizarem seus ataques, actualmente conhecido também como "script kiddie" e foi o termo depreciativo mais frequentemente usado no final dos anos 1980 e 1990"[377].

---

[373] Ibidem, p. 5.
[374] Ibidem, p. 5.
[375] SOBRINHO, Jéssica Rafaela Nunes;et al. ***ob. cit.*** p. 5.
[376] ibidem., p.5.
[377]Ibidem, p.5.

No nosso entendimento, *Preaker* são pessoas fraudulentas que invadem os meios de comunicação telefónica, para proveito próprio sem o pagamento devido, instalando escutas a fim de facilitar o acesso externo, visando o ataque a sistemas. Por sua vez os "*Lammers* são aqueles que possuem algum conhecimento querem se tornar um *hacker* e, dessa maneira, ficam invadindo e perturbando os sites, em outras podem ser denominados de iniciantes"[378].

5. Defacers e Carders

Ainda neste contexto dos perfis dos criminosos, encontramos os *Defacers*, esta designação é oriunda do inglês (defacing) e é utilizada para caracterizar aqueles que desfiguram sites ou perfil de redes sociais. "Os defacers são semelhantes a pichadores, no entanto, suas actividades são realizadas em sites"[379] .

Ainda neste mesmo contexto, temos os *Carders*, que são especialistas em fraudes por meio de cartões de crédito, os *Scammers*, que são aqueles que se aproveitam de mensagens enganosas e propagandas falsas levando o sujeito passivo a fornecer informações sigilosas ou instalar *softwares* de espionagem[380]. Como se pode depreender, há várias designações específicas apontadas dos sujeitos activos dos crimes cibernéticos. Essas designações são empregues de acordo com as terminologias usadas no ambiente virtual, evidenciando suas características, habilidades e quanto aos delitos praticados, posto que a sociedade está em constantes transformações e nisso, a área da informação decorre de grande actualização regular, sendo necessária devida actuação legislativa para responsabilizá-los.

Frente à classificação de perfis de criminosos, temos uma ideia de quem eles são, o que querem, de uma forma genérica, e como agem. Mas a questão de fundo é: como identificá-los antes mesmo de eles cometerem condutas ilícitas que os identifiquem? Já que quando falamos em sujeito activo sabemos que realmente os dados obtidos para identificação do sujeito é o endereço da máquina que envia as informações, ou seja, o IP, seu *login* e senha, portando com a possibilidade de camuflagem dos dados e a utilização de dados falsos dificilmente há uma rápida identificação do sujeito activo na prática.

A imputação objectiva do autor do crime e sua comprovação é extremamente difícil frente à ausência física do sujeito activo. Assim, ocorre que, frente à importância da identificação do autor do crime e a dificuldade desta identificação, surgiu a necessidade de se

[378] Ibidem, p.5.
[379] Ibidem.p.5.
[380] ibidem, p.5

traçar um perfil denominando grupos que praticam determinados crimes virtuais, dentre essas denominações temos a figura do *hacker*.

Entretanto, a imputação objectiva ao autor do crime e sua comprovação é extremamente difícil frente à ausência física do sujeito activo. Assim, diante da importância da identificação do autor do crime e a dificuldade desta, surgiu a necessidade de se traçar um perfil denominando grupos que praticam determinados cibercrimes. Decorrente disso, o primeiro problema a ser enfrentado nos crimes cibernéticos é a determinação da autoria. Muito dificilmente a pessoa que pretende cometer uma infracção penal utiliza sua identificação pessoal real[381]. Há casos em que o criminoso, em conformidade com Zacarias, faz-se passar por outra pessoa, mediante o uso indevido de suas senhas pessoais. Por conseguinte, nas redes de computadores, não é possível identificar o usuário visualmente ou através de documentos, mas é possível identificar o endereço da máquina que envia as informações à rede, isto é, o IP da máquina[382].

O autor em referência avança mais apontando que:

> "a quebra do sigilo dos dados de conexão de usuário, trata-se somente da disponibilização por parte das empresas, em um primeiro momento, de qual teria sido o IP utilizado e o horário (incluindo informações de fuso horário) de determinada acção criminosa realizada em um serviço de Internet, como redes sociais, contas de e-mail, programas de mensagens instantâneas, dentre outros e em um segundo momento das informações do usuário que efectivamente utilizou aquele IP de determinado provedor, ou seja, qual teria sido, supostamente, o endereço físico no "mundo real" em que o computador ou outro equipamento informático com acesso à Internet estaria instalado no momento da conduta criminosa"[383].

Ainda na análise da questão da autoria, Greco questiona "Como identificar o agente? Para termos uma ideia das dificuldades e da complexidade que o tema dos controlos assume, por exemplo, na Internet, basta mencionar que podem existir serviços que poderiam ser denominados de "serviço de máscara"[384]. Para o autor, a questão tem a ver com o problema de armazenamento dos *logs* de acesso. Visitando a nossa legislação Penal, podemos conferir que não existe nenhuma previsão de por quanto tempo os servidores devem armazenar essas informações.

---

[381] ZACCARIAS, Inellas Gabriel Cesar de, ***Crimes na Internet***. 2ª edição, 2009, p. 25. Disponível em https://www.estantevirtual.com.br/gabrielcesar-zaccaria-de-inellas/crimes-na internet/1750000007, acessado no dia 19 de Dezembro de 2023.
[382] Ibidem.
[383] ZACCARIAS, Inellas Gabriel Cesar de, ob. cit., p. 25.
[384] INELAS, Gabriel Cesar Zaccarias de. ob., cit.

3.2.4.3. Os Métodos e Meios Utilizados pelos Criminosos nos Cibercrimes

A ideia de que a internet é o meio pelo qual os criminosos executam os cibercrimes é sobejamente consensual. Assim, instruída a persecução penal, mediante a investigação do cibercrime cometido, é imprescindível a identificação imediata do meio pelo qual o crime foi praticado, para nortear a acção do órgão investigativo, à medida que serão distintas as técnicas utilizadas para obtenção da autoria e materialidade do crime[385]. Um dos problemas mais complexos é a prova de autoria do delito na investigação dos crimes cibernéticos, em virtude do anonimato do usuário da rede, pois raramente o sujeito-activo utiliza sua identidade legítima. Isso é o que torna

> "os logs, os eventos que são praticados em determinado acesso e são registados no sistema computacional, permitindo a verificação dos actos praticados naquele momento e o endereço IP (internet protocol), que refere-se ao registo criado toda vez que uma conexão é feita, essas são as evidências de maior relevância na investigação, além de serem as provas que irão conduzi-las, todavia, obter esses dados é um processo árduo, devido as exigências legais que devem ser respeitadas rigorosamente"[386].

Na mesma perspectiva, Sales apregoa que "os criminosos, utilizando-se de variados métodos, obtém informações ou arquivos pessoais da vítima para a realização de diversos crimes, a depender do nível de interesse em relação ao objecto do crime, conhecimento técnico e de periculosidade do infractor". A afirmação de Sales evidencia, ainda de forma enfática, que a utilização da tecnologia pode constituir meio para a prática de outras figuras típicas que não estão vinculadas à informática e que de outro modo poderiam ser perpetradas, amoldando-se à classificação supra exposta dos chamados crimes informáticos impróprios, mistos ou mediatos, de acordo com o caso[387]. Nisso, as informações e os arquivos pessoais obtidos são utilizadas para realizar transacções comerciais ilícitas, transferências financeiras, extorquir a vítima etc., podendo os delinquentes responderem pelos diversos crimes, dependendo do acto nele praticado.

Entretanto, afere-se igualmente a configuração de crimes cibernéticos propriamente ditos[388] que estão previstos na nossa legislação penal, aqueles em que o bem jurídico protegido

[385] SOBRINHO, Jéssica; et al. Ob., Cit. p. 5.
[386] Ibidem. p.5.
[387] SALES, Marcos Levy Gondim, ***A comprovação da materialidade e da autoria nos crimes virtuais***. Monografia apresentada na Faculdade de Direito da Universidade Federal do Ceará, Fortaleza, 2013, p. 43.
[388] Os crimes propriamente ditos – designados também de crimes virtuais ou cibernéticos/informáticos próprios ou puros. Como foi abordado nesta dissertaçáo, são aqueles em que o sujeito activo utiloza o sistema informático do sujeito passivo, no qual o computador como sistema usado como objecto e meio para a execução do crime.

pela norma penal é a inviolabilidade das informações automatizadas (dados), devendo ser aferido o tipo penal incorrido pelo agente, no caso concreto, de acordo com a via por ele eleita para a obtenção das informações e dos arquivos pessoais.

Assim, para a obtenção dos dados, uma das principais formas de invasão a dispositivos electrónicos, utilizada por *hackers* mal-intencionados[389], é infectando-os com *malwares* (softwares maliciosos), que, de acordo com Abhisek Singh[390], "são programas feitos para causar danos e/ou interromper a máquina infectada e outras máquinas ligadas a ela em rede, podendo também fazer o furto de informações pessoais de usuários do dispositivo infectado, seja este móvel (computadores de bolso, como smartphones, tablets e laptops) ou não".

Na mesma perspectiva, e tal como Singh ensina:

> "os malwares podem ser classificados em 4 tipos: worms, trojans, vírus e, por fim, spywares e adwares. Os worms são softwares maliciosos que são programados automaticamente para se espalharem de uma máquina para outra com finalidades diversas. Enquanto os Mass-Mailing Worms, por exemplo, espalham-se por meio do envio em massa de mensagens para vários endereços de e-mail que são coletados da máquina da vítima, resultando na famosa prática de Spam. Uma espécie desse tipo de worm, citado pelo autor, trata-se do mass-mailing worm W32.Assarm@mm, que envia mensagens respondendo a todas as mensagens não lidas que estão na caixa de entrada do software Microsoft Outlook"[391].

O problema é que, normalmente, as ditas mensagens vêm acompanhadas de outros tipos de *malwares*, que acabam entrando despercebidamente na máquina do usuário e resultam em graves consequências. A seu turno, "os trojans", ou "cavalos de Tróia" como são popularmente conhecidos, são programas que se disfarçam de softwares bons e enganam o usuário a executá-los, existindo actualmente uma infinidade de *trojans* criados por hackers maldosos. Uma vez executados, os *trojans* podem, dentre outras tarefas, enviar e-mails"[392] (como no caso dos mass-

---

"Nessa categoria de crimes está, não só a invasão de dados não autorizados, mas toda a interferência em dados informatizados como, por exemplo, invasão de dados armazenados em computador seja no intuito de modificar, alterar, inserir dados falsos, ou seja, que atinjam diretamente o software ou hardware do computador e só podem ser concretizados pelo computador ou contra ele e seus periféricos". (ALMEIDA, Jéssica de Jesus; et. al. Crimes Cibernéticos, In Caderno de Graduaçáo, Ciências Humanas e Sociais Unit | Aracaju | v. 2 | n.3 | p. 215-236 | Março 2015 | periodicos.set.edu.br. p.224).

[389] Tendo em atenção os diferentes sujeitos activos nos cibercrimes, somos de entendimento que os Hackers mal-intencionados são os crackers. Visto haver uma diferença entre os hackers e os crackers: geralmente são muito parecidos em relação ao vasto conhecimento aprofundado em informática, sendo que a principal distinção, pelo menos na maioria da doutrina, é a finalidade que suas práticas resultam, posto que os hackers realizam actividades positivas, não criminosas, enquanto a motivação dos crackers é criminosa em sua essência, agindo, normalmente e premeditadamente, com objectivo criminoso de obter vantagens ilícitas.

[390] SALES, Marcos Levy Gondim. ob. cit. p. 43.

[391] Ibidemm p.43.

[392] Texto na íntegra: ***"Malware stands for Malicious Software***. Malicious softwares are programs, which are designed to damage and/or disrupt the infected machine and/or other networked machines. It can be classified into four types". SINGH, Abhishek. SINGH, Baibhav. JOSEPH, Hirosh, ***Vulnerability Analysis and Defense for the Internet.*** Nova Iorque: Springer Science+Business Media, p. 169, 2008. 34 No original, aduz o autor: "For

mailing worms), destruir dados da máquina, fazer o *download* de arquivos, fornecer acesso remoto do computador infectado ao hacker que programou o *malware* etc.

Especialmente, existem os chamados *Password-Stealing* (PSW) *Trojans*, que, segundo Abhishek Singh[393]

> "roubam senhas e/ou informações (de cartões de crédito, contas de e-mail etc) directamente do computador da vítima e mandam para o autor do vírus por e-mail ou por arquivo para uma unidade de armazenamento remoto. É o caso do clássico Trojan-IM. Win-32, que rouba senhas de programas de mensagens instantâneas como o ICQ e o Msn Messenger. Por sua vez, o vírus trata-se de um código executável (programa) que pode se replicar de um lugar para outro, repetidas vezes, e atingir a sua finalidade no sistema, seja ela benigna ou maligna".

Diferenciando-se do *trojan*, basicamente, em razão de o vírus ser potencialmente ofensivo à operacionalidade do dispositivo infectado como um todo (por exemplo, ele pode impedir que um computador inicialize o sistema operacional, tornar defeituoso o funcionamento do *mouse*, do teclado etc), enquanto o outro, disfarçado como um software bom para a máquina, busca na verdade criar uma porta dos fundos no sistema para que o autor do *malware* possa utilizar a máquina infectada como se fosse administrador desta, devassando o conteúdo ali contido, enviando mensagens em nome do proprietário etc[394].

Por fim, encontramos "os *spywares* e os *adwares*, *softwares* que, uma vez introduzidos secretamente na máquina invadida, ajudam o seu autor a juntar informações sobre o usuário ou sobre uma organização sem que estes tenham conhecimento, tais como os horários de funcionamento da máquina, quais as páginas mais acessadas, que tipo de propagandas da *web* são logo cortadas pelo usuário etc"[395].

Segundo as lições do Singh[396] os *malwares* enquadram-se tanto como instrumentos de violação de mecanismo de segurança para a obtenção de dados ou informações do titular do dispositivo, como também se tratam de vulnerabilidades para a obtenção de vantagem ilícita.

De igual modo, não se pode perder de vista o phishing, termo utilizado pelos hackers para se referir à palavra inglesa *fishing* que, traduzindo para o português, significa "pescaria".

---

example, W32.Assarm@mm is a mass-mailing worm that sends messages in reply to all unread messages in the Microsoft Outlook Mailbox", ibid, p. 170. 44. Apud SALES, Marcos Levy Gondim. ob. cit. p. 43.

[393] SALES, Marcos Levy Gondim. ob. cit. p. 43.

[394] Ibidem, p.43.

[395] Ibidem, p.43.

[396] Ibidem, p. 44.

Nesta actuação,

> "o phishing realmente na "pesca" de informações e dados pessoais da vítima, que pode ser feita por métodos mais ou menos tecnológicos, mas sempre induzindo a vítima em erro. Nos ataques mais primitivos, o phishing é feito mediante o envio de uma mensagem falsa para a vítima por e-mail, em que o criminoso se faz passar por uma empresa ou um órgão os quais possuem credibilidade notória, tais como bancos ou até mesmo órgãos do poder judiciário, e alega a necessidade de a vítima realizar alguma medida de urgência". De outro modo, "a vítima pode ser levada a acreditar que está diante de uma grande oportunidade financeira por um anúncio publicitário, enquanto navega na internet. Diante de tais situações, a vítima é induzida a urgentemente preencher cadastros, fornecendo endereço, número de cartão de crédito, dados pessoais, como o número da carteira de identidade e da sua inscrição no cadastro de pessoas físicas etc., que são utilizados pelos criminosos para a realização de empréstimos bancários, transações financeiras indevidas a partir da conta da vítima ou para a aplicação de outras fraudes"[397].

Nestas condições, pensamos na existência da ocorrência de uma figura delitiva própria do direito penal de Burla, previsto nos termos do art. 287 do CP. Entretanto, pelos meios que o infractor usa para atingir as suas pretensões maliciosas, afere-se, na verdade, a consumação do crime de burla informática, prevista nos termos do art. 289 do CPM, nos termos em que o acto praticado pelo criminoso, serve-se do computador como principal meio para atingir o objectivo pretendido pelo criminoso ou objecto do crime; criminalidade gerada através do computador enquanto instrumento de trabalho.

Neste acto, há uma intenção de obter para si ou terceiros, enriquecimento ilegítimo, causando a outra pessoa prejuízos patrimoniais. Note-se que o bem jurídico protegido é, não só o património como em outros crimes, mas também os programas informáticos e os respectivos processamentos e os dados, quanto à sua aplicabilidade e segurança. Infelizmente essa protecção restringe-se aos casos de burla em que o agente do acto tem a intenção de obter um enriquecimento ilegítimo que causa a outra pessoa prejuízo patrimonial.

Como se pode aferir pela norma do art. 289 do CP, as práticas mais comuns caracterizadas como burla são: interferência no resultado de tratamento de dados; causar prejuízo patrimonial a outrem com intenção de enriquecimento ilegítimo; utilização de dados sem autorização ou de forma incorrecta; estruturar programas informáticos incorrectamente...

Ademais, o crime *phishing* pode envolver o emprego de meios mais avançados de tecnologia, como o d*efacement* e a efectiva utilização de malwares. Com efeito, o *defacement*, conforme noticiado pela Revista Consultor Jurídico, consiste em "alterar um *site* visualmente o que equivale a uma pichação na internet. *Sites* de instituições públicas são alvos constantes

[397] SALES, Marcos Levy Gondim. ob. cit. p. 44.

desse tipo de invasão, utilizada por grupos hackers para fazer protestos de cunho político"[398]. Desse modo, os hackers criminosos utilizam-se da técnica para maquiar um website e enganar a vítima que, por exemplo, acreditando estar realmente navegando do sítio electrónico do seu banco, uma vez que digitou correctamente o endereço electrónico daquele, inscreve os dados referentes à sua conta bancária nos campos ali demonstrados, os quais serão todos encaminhados, entretanto, para o(s) autor(es) do acto malicioso.

Há casos em que, por um lado o sítio electrónico da empresa almejada possui uma defesa superior à técnica de invasão do *hacker*. Nessas situações há um caminho a ser percorrido pelos criminosos que visa a:

> "criação de um website em moldes muitos parecidos ao da instituição original. Desse modo, o criminoso envia mensagens alertando as vítimas sobre a necessidade de actualização de dados, ou alguma outra estória para ludibriá-la, juntamente com o link do website por ele criado para que a vítima forneça seus dados supondo estar no endereço eletrónico correcto, e, da mesma forma acima descrita, as informações acabam parando nas mãos dos criminosos"[399].

Por outro lado, o *phishing* pode ser ainda mais nocivo à vítima, quando ela, além de ter sido ludibriada pela estória dos delinquentes faz o download de malwares para o seu dispositivo ao verificar o anexo da mensagem ou efectivamente visitar o link enviado pelos autores dessa. Neste caso, independentemente do fornecimento voluntário da vítima, dos seus dados e informações pessoais, os infractores invadem a máquina dela e, deste modo, estão aptos a realizar as diversas finalidades já estudadas por meio dos malwares maliciosos[400].

De acordo com o que até este ponto foi visto, para que o usuário se conecte à rede mundial, ele necessita dos serviços de uma provedora de internet, a qual lhe fornecerá um número de IP que o identificará durante todo o tempo em que ele permanecer conectado. Toda transmissão de dados realizadas por ele, bem como o acto de sua conexão, serão identificados pelo seu IP em conjunto com a data, hora e o fuso horário GMT do dispositivo utilizado para a navegação. Trata-se do número de IP do principal meio de rastreamento do infractor que pratica crimes no âmbito virtual, existindo actualmente diversos programas[401] que permitem a exacta

---

[398] ibidem, p.47.
[399] SALES, Marcos Levy Gondim. ob. cit. p. 47.
[400] bidem, p.47.
[401] "LocalizaIP- LocalizaIP fornece a localização do usuário através da digitação de seu endereço IP. Além dessa funcionalidade, a ferramenta ainda permite a geolocalização. O GeoIP faz o rastreamento IP pelo mapa de um computador. Isso é possível tanto em computadores com IPv4 quanto em máquinas IPv6. WhoisO Whois é um protocolo de perguntas e respostas sobre DNS, que são os domínios de site Ele ajuda na proteção da rede de computadores e, na busca por rastrear IP, auxilia na descoberta de quem é a pessoa detentora do IP. Network Connections O aplicativo do Network Connections permite que o usuário visualize todas as conexões IP que foram feitas através do smartphone. As informações são completas incluindo a quantidade de dados enviados e recebidos por cada IP. Isso ajuda bastante na hora de saber quais os aplicativos estão utilizando mais a internet Fing –

localização geográfica da máquina utilizada pelo usuário. De igual modo, em posse dessa informação, pode o provedor ser accionado, directamente ou por intermédio do Poder Judiciário, para fornecer os dados do usuário vinculado ao IP e todas as informações acerca da conexão, sendo mister a preservação desses de modo a se comprovar a existência de elo entre a conexão à rede e a ocorrência do acto infraccional.

3.2.4.4. Sujeito Passivo dos Crimes Cibernéticos

Quando falamos de um crime específico, logo sabemos quem é o sujeito activo e passivo da conduta, quem realizou e em quem recaiu a acção ou omissão. Contudo, nos crimes virtuais, de forma generalizada, a única afirmação cabível é que será sempre uma pessoa física caso ou jurídica ou uma entidade titular seja pública ou privada, titular do bem jurídico tutelado, sempre haverá o sujeito passivo, ou seja, alguém que está sendo lesado, enfim o que sofre a acção. Nesta perspectiva, o sujeito passivo da infracção penal pode ser qualquer indivíduo normal, pessoa física, ou até mesmo uma pessoa jurídica, haja vista, poder, por exemplo, ter seus bens desviados, seu património deteriorado ou mesmo ter informações violadas. Ambas informações são capazes de determinar a acção do agente criminoso. Portanto, ocorre que "actualmente muitos dos crimes praticados ainda não são divulgados, seja por conta da não disseminação dessas informações ou pela falta de denúncias, como, por exemplo: grandes empresas evitam a divulgação sobre possíveis ataques virtuais ou mesmo invasões para não demonstrarem fragilidade quanto à segurança e quanto às pessoas físicas vemos que por falta da devida punibilidade"[402] aos infractores e a falta de mecanismos de denúncia, apesar de já existirem, as vítimas acabam não denunciando o que facilita a propagação desses crimes.

Enfatizando a ideia exposta no parágrafo anterior, para Orrigo et al., "o sujeito passivo do crime cibernético pode ser qualquer indivíduo que tenha um bem jurídico lesado ou

Ferramenta de rede ferramenta de rede permite a visualização de dispositivos conectados a uma rede Wi-Fi determinada, aumentando, a proteção contra invasores. Ao rastrear o IP, o Fing analisa o provedor da internet, mede a qualidade de rede e o uso de dados. Isso oferece uma segurança maior, inclusive na hora de diagnosticar problemas e evitar a perda de informações importantes. Hosts Green. O Hosts Green é o primeiro do brasil em Saas a monitorar URL's, links e IP's, tanto os dinâmicos quanto os fixos. Ele também tem diversas integrações com outros sistemas. Ele gera relatórios constantes e envie notificações de alerta. O acompanhamento das operações é constante, apresentando sua base de dados periodicamente. Você pode experimentar a ferramenta de forma gratuita, é só fazer o cadastro. Para rastrear IP, monitorar os endereços e ainda otimizar suas páginas, confira os planos que a HostGreen oferece e comece a ter resultados positivos rapidamente." (ALMEIDA, Abraão, Rastrear IP: 5 Ferramentas que podem ajudar nessa missão. 21 de Maio de 2020. Disponivel no https://blog.hosts.green/rastrear-ip/, acessado no dia 27 de dezembro de 2023.

[402] ALMEIDA, Jéssica de Jesus; et. al, ***Crimes Cibernéticos***, In Caderno de Graduaçáo, Ciências Humanas e Sociais Unit | Aracaju | v. 2 | n.3 | p. 215-236 | Março 2015 | periodicos.set.edu.br. p.227).

ameaçado de lesão por acções realizadas por meio do computador, podendo ser Pessoa Física ou Pessoa Jurídica"[403].

Ressalta-nos corroborar com os autores citados em relação ao sujeito passivo nos crimes cibernéticos que de facto o sujeito passivo pode ser qualquer pessoa que se serve das novas tecnologia de comunicação e informação para fins adversos (profissionais, sociais, financeiros, económicos e outros) e essa pessoa acaba sendo vítima, pois os criminosos utilizam técnicas cada vez mais apuradas de engenharia social, aliadas às tais tecnologias. Nesse contexto, depois de se analisar quem pode ser o sujeito passivo dos cibercrimes é importante analisar o tempo e local do crime, dois aspectos complexos para identificar os criminosos virtuais.

3.2.5. Jurisdição e Competência para Julgar os Crimes Cibernéticos

3.2.5.1. Critérios Gerais de Definição de Competência

A necessidade de evitar confusão na divisão da jurisdição, de modo a determinar, face a um caso concreto, qual o tribunal que, atento sua espécie, o referido caso concreto deve ser entregue e, por acréscimo, dentre os tribunais da mesma espécie, qual em concreto deve ser chamado a conhecer do caso, leva a que seja necessário regulamentar através da lei, de forma geral e abstracta, o âmbito de actuação de cada tribunal, permitindo o diferimento de cada caso de natureza penal a um único tribunal.

É nisso que consiste a determinação da competência em processo penal, que obsta à confusão da divisão da jurisdição e conflitos de competência (positivos ou negativos) entre os tribunais. A determinação da competência por via geral e abstracta, através da lei, permite que a acusação saiba, de antemão qual o tribunal perante partida, permite ao tribunal saber quais os casos relativamente aos quais é acusação possam eventualmente, um aspecto que não deixa de ter relação com o princípio do juiz natural.

A propósito da determinação em concreto do tribunal competente para conhecer e decidir um caso penal, trata-se de uma questão que pressupõe a resposta a três ordens de perguntas que correspondem a igual número, de vertentes de competência, nomeadamente material, territorial e funcional.

[403]ORRIGO, Gabriel Marcos Archanjo; et al, ***Crimes Cinbernéticos: uma abordafem jurídica sobre os crimes realizados no âmbito virtual***.Jus.com.br, 2015. Disponivel em: https//jus.com. br/artigos/4358/crimes-cibernéticos-abordagem jurídica-sobre-os-crimes-realizados-no-ambito-virtual. Acessado no dia 13 de Janero de 2024.

3.2.5.1.1. Competência Funcional (do Tribunal Penal)

> **Competência funcional - "**é aquela fixada em razão de certas atribuições específicas conferidas aos órgãos judiciais em determinados processos. Estão em vários diplomas legais. **Competência funcional** decorre das funções exercidas pelo juiz em determinado processo de acordo com as suas fases, ou seja, funções diferentes desempenhadas no decorrer do procedimento, inclusive quanto ao grau de jurisdição. A **competência hierárquica** é uma espécie de competência funcional por se referir à competência originária para conhecer e decidir a causa bem como à competência recursal, ou seja, para o julgamento de eventual recurso"([404]).

Em uma **perspectiva horizontal**, verificar-se-á competência funcional quando ao nível da primeira instância determinada questão deva ser conhecida ou seja da competência dum tribunal diferente, tendo em conta a fase em que o processo se encontra, como seria o caso de se atribuir competência para decidir questões relacionadas com execução da pena a um tribunal de execução de penas (artigo 22 do CPP), ressalvada a competência para decisão ou prática de actos jurisdicionais que se levantem durante a fase de instrução preparatória que pertence ao juiz de instrução criminal nos termos do artigo 19 do CPP.

Assim, a competência do juiz de instrução criminal decorre de funções exercidas pelo juiz em determinado processo de acordo com as suas fases. Com efeito, *"compete ao juiz de instrução exercer as funções jurisdicionais relativas à instrução, dirigir a audiência preliminar e decidir quanto à pronúncia. Não pode proceder ao julgamento do arguido o juiz que, no processo respectivo, tenha, contra ele, proferido despacho de pronúncia" (Cfr. artigo 19 n°1 e 2 do CPP).*

Fora dos casos de actos jurisdicionais praticados durante a instrução preparatória dos processos-crime, a competência para conhecer de questões do processo-crime que careçam de decisão jurisdicional cabem aos tribunais comuns ou judiciais[405].

Na **perspectiva hierárquica,** como já se referiu, a **competência hierárquica** é uma espécie de competência funcional quando se referente a**o julgamento de eventual recurso**. Com efeito, *"têm competência penal: a) o Tribunal Supremo; b) o Tribunal Superior de Recurso; c) o Tribunal Judicial de Província; d) o Tribunal Judicial de Distrito" (artigo 18 n°2 do CPP).* Ou seja, a competência funcional pode ser por graus, quando permite que as decisões penais, não adquirindo carácter definitivo logo que são proferidas, possam em regra ser sucessivamente reexaminadas por tribunais de Segundo grau, ou de terceiro grau (com competência limitada à matéria de direito) e do grau extraordinário de revisão.

([404]) https://trilhante.com.br/curso/competencia-na-justica-do-trabalho/aula/competencia-funcional-2 - acesso, 28/10/2022.

[405] CUNA, Ribeiro José, ***Lições de Direito Processual Penal,*** Escolar Editora, Maputo, 2004, pag. 224-229.

Portanto, à luz do disposto no artigo 19 n°1 e 2 da LOJ – Lei n° 24/2007, de 20 de Agosto, conjugado com o artigo 18 n°2 do CPP, trata-se da **competência em razão da hierarquia** em que, tendo em atenção a estrutura vertical dos tribunais, temos os de primeira e de segunda instância em matéria de facto, visto ser permitido em regra somente um grau de recurso. Em matéria de direito poderá haver dois graus de recurso, visto que a lei o permite.

Neste sentido, o tribunal competente hierarquicamente, tendo em conta as categorias de tribunais judiciais, nomeadamente o Tribunal Supremo, os Tribunais Superiores de Recurso, os Tribunais Judiciais de Província e Tribunais Judiciais de Distrito, o tribunal de segunda instância será imediatamente o de categoria a seguir, salvo casos de recurso sobre a matéria de direito interpostos nas decisões proferidas pelos tribunais judiciais de Província, em segunda instância, que devem ser interpostos directamente para o Tribunal Supremo por força do artigo 19 n°3 da LOJ – Lei n° 24/2007, de 20 de Agosto, é denominado por recurso *per saltum.*

Outrossim, haverá desvios no que refere a competência na perspectiva vertical (competência em razão da hierarquia), naqueles casos em que o Tribunal Supremo julga funcionando em segunda instância ou em instância única.

3.2.5.1.2. Competência Material (do Tribunal Penal)

A competência material consiste na parcela de jurisdição que é distribuição pelas diferentes espécies de tribunais (Tribunais comum, tribunal laboral, tribunal de menores, tribunal fiscal, tribunal aduaneiro, tribunal administrativo), com base na natureza das causas a resolver, o que permite que tendo em conta as particularidades decisivas na matéria ou na natureza dos assuntos a tratar sejam competentes órgãos jurisdicionais dotados de uma organização e um formalismo que responda aos desafios suscitados pela especificidade da matéria.

Do que se trata, na competência material, é "...fundamentalmente, de repartir as causas penais pelas diferentes espécies de tribunais de 1ª instância"[406], referindo-se Germano Marques da SILVA (2010:183) essencialmente ao facto de competência material em 1ª instancia ser geralmente determinada em função a natureza e gravidade do crime, com o critério quantitativo a atender à gravidade da pena aplicável, e o critério qualificativo à espécie do crime ou à natureza de algum dos seus elementos.

[406] DIAS, Jorge de Figueiredo, ***Direito Processual Penal***, 1° Volume, 1.ª Edição – 1974, Reimpressão, Coimbra, 2004, pág. 332

Para o efeito, existem métodos de determinação da competência material, nomeadamente o método de determinação abstracta da competência e o método de determinação concreta da competência.

- **Método de determinação abstracta da competência** – com base neste método a competência material resulta imediatamente ou incondicionalmente da lei, o que pode ser materializado por duas vias: dando a cada tribunal competência para conhecer e decidir de certos tipos de crime, ou dando "(...) a cada tribunal competência para o conhecimento e decisão de crimes a que corresponda, em abstracto, uma pena até um certo máximo..."[407].
- **Método de determinação concreta da competência** – de acordo com este metido, e contrariamente ao método de determinação abstracta da competência, não se atenda directamente ao tipo de crime ou à pena máxima que lhe seja aplicável, mas ao crime.

À luz do Direito moçambicano vigente, sendo competentes para conhecer a matéria criminal os tribunais judiciais e, por isso, comuns em matéria criminal (artigo 222 n°4 da CRM) uma vez que são atribuídos outros tribunais, resultando daí que são tribunais de competência genérica nesta matéria, segue-se em **regra o método da determinação abstracta da competência material**, o qual segue também a via da gravidade da infracção aferida ou indicada através do máximo da pena aplicável. Note-se que sempre que as circunstâncias o justifiquem podem ser criados tribunais judiciais de competência especializada, de acordo com o estabelecido na lei da organização judiciária (artigo 18 n°3 do CPP).

De acordo com as suas categorias, os tribunais judiciais, do topo à base e conforme a sua hierárquica, são os seguintes: Tribunal Supremo, tribunais Superiores de Recursos; tribunais judiciais de província; e tribunais judiciais de distrito (Cfr. artigo 29 n°1 da Lei de organização judiciária - Lei n° 24/2007 de 20 de Agosto conjugado com o artigo 18 n°2 do CPP). Assim, consoante maior ou menor for o máximo da pena aplicável, o tribunal competente será maior ou menor escalão.

Neste sentido, começando pelos Tribunais Judiciais de Distrito, que constituem a base hierarquia dos tribunais judiciais, funcionando em 1ª instância, compete, *em matéria criminal julgar as infracções criminais cujo conhecimento não seja atribuído a outros tribunais e* ***julgar as infracções a que correspondam pena não superior a (12) doze anos de prisão maior*** (artigo 84º/2, alíneas a) e b) da LOJ - 24/2007 de 20 de Agosto, actualizada pela Lei n° 11/2018, de 3 de Outubro).

[407] Idem, pág. 333.

Importa referir, no entanto, que também a competência dos tribunais judiciais em matéria criminal é repartida entre as diversas categorias dos tribunais judiciais com base na qualidade da pessoa do arguido. Neste sentido, "*ao tribunal judicial de província, funcionando como tribunal da primeira instância, compete, em matéria criminal: (a) julgar as infracções criminais, cujo conhecimento não seja atribuído a outros tribunais; (b)* ***conhecer de processos-crime em que sejam arguidos juízes profissionais dos tribunais judiciais de distrito e magistrados do Ministério público junto dos mesmos*** **(**artigo 73 n°2 alíneas a) e b) da LOJ - 24/2007 de 20 de Agosto).

Aos Tribunais Superiores de Recurso, enquanto tribunais de escalão intermédio entre o Tribunal Supremo e os Tribunais Judiciais de Província, em matéria criminal, compete: (a) *julgar os processos-crime em que sejam arguidos juízes profissionais dos Tribunais judiciais de província e magistrados do Ministério público junto dos mesmos; (b) julgar os processos-crime em que sejam arguidos juízes eleitos dos tribunais judiciais de província, por actos relacionados com o exercício das suas funções; e (c) conhecer dos pedidos de habeas corpus que, nos temos da lei processual, devem ser-lhes remetidos* (Cfr. artigo 63º alíneas a), b) e d) da LOJ- 24/2007 de 20 de Agosto).

Por fim, o Tribunal Supremo, que é o mais alto órgão judicial na hierarquia dos tribunais judiciais, funcionando em plenário e como tribunal de instância única tem competência para: *(a) julgar os processos-crime em que sejam arguidos o Presidente da República, o Presidente da Assembleia da República e o Primeiro-Ministro*; (b) *julgar os processos-crime instaurados contra o Presidente, Vice-Presidente e os juízes conselheiros do Tribunal Supremo, o Presidente e os Juízes Conselheiros do Conselho Constitucional*; *o Presidente e os Juízes Conselheiros do Tribunal Administrativo, o Procurador-Geral da República; Vice-Procurador-Geral da República e o Provedor de Justiça*; (c*) julgar os processos-crime instaurados contra os juízes eleitos do mesmo tribunal, por actos relacionados com o exercício das suas funções*; (Cfr. artigo 46 alíneas a), b), e c) da LOJ - 24/2007 de 20 de Agosto). Verifica-se aqui a atribuição de competências com base na qualidade dos arguidos, que são figuras, grosso modo, entidades titulares de órgãos de soberania.

Às secções do tribunal Supremo, como tribunal de primeira instância compete: *(a) julgar processos-crime em que sejam arguidos deputados da Assembleia da República, membros do Conselho de Ministros, membro do Conselho de Estado e outras entidades nomeadas pelo Presidente da República nos termos da Constituição, e todas as demais entidades que gozam do foro especial nos termos da lei e não estejam abrangidos pelo artigo*

46º, da Lei de organização judiciária, (b) julgar processos-crime em que sejam arguidos juízes profissionais dos Tribunais Superiores de recursos e magistrados do Ministério Público, junto dos mesmos tribunais; (c) julgar os processos-crime instaurados contra os juízes eleitos dos mesmos tribunais, por actos relacionados com o exercício das suas funções; e (d) julgar os processos de extradição (Cfr. artigo 51º alíneas a), b), c), e) da LOJ - 24/2007 de 20 de Agosto).

A determinação da competência material em particular é relevante, uma vez que caso determinada causa esteja pendente perante tribunais incompetente, por carecer de competência em razões da matéria, suscita-se a questão da incompetência material que é uma excepção dilatória (artigo 140 n°1 alínea b) do CPP), tendo legitimidade para deduzi-la o Ministério Público, sobre quem alias recai o dever de o fazer, e ainda tem legitimidade para deduzi-la a parte acusadora e os arguidos uma vez admitidos a intervir no processo, bem como os próprios tribunais a titulo oficioso, portanto, independentemente de ter sido ou não deduzida (artigo 36 conjugado com o artigo 141 ambos do CPP).

Constata-se, pois que todos os sujeitos processuais podem levantar a excepção da incompetência material, em qualquer altura do processo até ao trânsito em julgado da decisão final e, caso seja comprovada e julgada procedente, determina ou tem como efeito a remessa do processo para o tribunal competente (Cfr. artigo 142, corpo, 1ª parte do CPP), devendo este anular "...apenas os actos que se não teria praticado, se perante ele tivesse corrido processo, e os que têm de ser repetidos para ele tomar conhecimento da causa".

3.2.5.1.3. Competência Territorial (do Tribunal Penal)

Determinado o tribunal competente em razão da matéria, segue-se a determinação do tribunal competente dentre os que, sendo da mesma espécie materialmente competente, deve ser chamado a apreciar e decidir o caso concreto. O que está em causa, portanto, é repartição das causas penais pelos diversos tribunais da mesma espécie, no caso do processo penal em que está em causa a matéria penal, os tribunais está relacionada com a necessidade de que, para cada caso penal, seja chamado a conhecer e decidir o tribunal que, dadas as suas ligações com o lugar do crime ou localização do arguido ligações mais ou menos imediatas ou próximas, esteja em melhores condições de julgar o caso, nomeadamente pela facilidade de recolha de elementos de prova, porquanto "a competência territorial delimita a jurisdição dos tribunais da mesma espécie segundo a sua localização no território"([408]).

[408] SILVA, Germano Marques da, ***Curso de Processo Penal I – Noções Gerais, Elementos do Processo Penal***, 6ª Edição, Revista e Actualizada, Verbo, Edição Babel, Lisboa, 2010, pág. 199

Outra razão que se pode referir é que há que permitir que a cada caso corresponda, sempre que possível, um tribunal competente em razão do território. Na abordagem da competência territorial há que distinguir a sua determinação por factos cometidos em território nacional e por factos cometidos no estrangeiro, uma vez que sendo a lei penal substantiva moçambicana aplicável, em regra, a factos cometidos em território nacional (princípio da territorialidade), casos existem em que pode ser aplicada a factos cometidos no estrangeiro.

3.2.5.1.4. Competência Territorial por Factos Cometidos em Território Nacional

Tendo em conta a finalidade da competência territorial¸ o critério da aferição é o do lugar da infracção ou *locus delicti*¸ ou seja, o critério geral que se traduz na conexão entre a infracção e o lugar ou zona geográfica onde o facto que o configura ocorreu, podendo haver critérios subsidiários para aqueles casos em que aquele se revele em concreto inadequado. O referido critério do lugar da infracção vem patente, nos artigos 23 e seguintes do CPP.

Assim, ***"é competente para conhecer de um crime o tribunal em cuja área de jurisdição se tiver verificado a consumação*"** **(Cfr. artigo 23 n°1 do CPP).** Trata-se do critério geral de determinação da competência territorial, que é da consumação da infracção em termos de área em que se consumou a infracção ser considerada em princípio, o *locus delicti*, pelo que para os chamados crimes materiais ou de resultado interessará, para efeitos de consumação da infracção, a produção do evento típico, sendo assim irrelevante o fim do exercício da actividade ou termo da omissão.

Por existirem infracções que se consumam por factos sucessivos ou reiterados, (v.g., furto continuado -artigo 270 n°2 do CP), ou por um só facto que se pode prolongar no tempo e no espaço (v.g rapto – artigo 197 do CP; sequestro- artigo 198 do CP), será competente em razão do território o tribunal do lugar onde se praticou o último facto (sucessivo ou reiterado), ou em que cessou a consumação, conforme prescreve o artigo 23 n°2 do CPP. Ou seja, ***"para conhecer de crime que se consuma por actos sucessivos ou reiterados, ou por um só acto susceptível de se prolongar no tempo, é competente o tribunal em cuja área de jurisdição se tiver praticado o último acto ou tiver cessado a consumação" (Cfr. artigo 23 n°2 do CPP).*** Funciona neste caso, também, o critério da consumação da infracção, com particularidade de se considerar o lugar onde se praticou o último facto ou em que se cessou a consumação.

Relativamente as infracções que se consumam por factos sucessivos ou reiterados, há que não confundir uns e outros (factos sucessivos ou reiterados) "…com a pluralidade de crimes do mesmo agente. Num e noutro trata-se de um só crime com modalidade de execução que

consiste na execução por uma sucessão de factos (=factos sucessivos) ou em que cada um dos factos realiza parcialmente a execução e a produção de um evento parcial do crime (=factos reiterados).

No caso particular de infracções que se consumam por um só facto e se prolonga no tempo e no espaço, "trata-se dos denominados crimes permanentes em que a execução e consumação perduram enquanto não for posto termo à violação permanente do interesse penalmente tutelado. A execução em tais crimes é composta por acção e omissão, e a execução como a consumação só cessam mediante a acção devida que ponha termo à omissão do agente do crime ([409]).

Quanto as infracções praticadas, em parte, em território nacional, vale também o critério da consumação, bem assim se atende ao lugar ou área onde a execução, preparação ou comparticipação do facto se verificou, desde que o mesmo seja punível pela lei moçambicana, e no caso de factos de encobrimento praticados em território nacional é competente o tribunal do lugar onde se praticou o facto que configura encobrimento (artigo 23 n°1 do CPP).

No entanto, porque o resultado da infracção pode não chegar a se consumar e, por conseguinte, não podendo valer o princípio geral da determinação da competência territorial (lugar da infracção), a lei prevê um critério subsidiário e excepcional, do qual resulta que será competente territorialmente em cuja área se praticou ou cometeu o último acto de execução da infracção ou último facto punível. Ou seja, ***"se o crime não tiver chegado a consumar-se, é competente para dele conhecer o tribunal em cuja área de jurisdição se tiver praticado o último acto de execução ou, em caso de punibilidade dos actos preparatórios, o último acto de preparação" (Cfr. artigo 23 n°3 do CPP).***

Estaríamos perante uma infracção que não chegou a se consumar, num caso de tentativa ou frustração, e ainda quando se trate de actos preparatórios que em si configurem crime autónomo e, como tal, punível (artigo 22 n°2 conjugado com o artigo 19 do CP).

Pode suceder que, tendo a infracção sido cometida nos limites de diversos distritos, províncias, haja dúvidas sobre o lugar em que foi. Em tal hipótese de **crimes de localização duvidosa ou desconhecida,** consagra um **princípio de prevenção da jurisdição**, dando competência a qualquer dos tribunais, mas preferindo o que primeiro tomar conhecimento da infracção", ou seja, o tribunal da circunscrição onde primeiro tiver havido notícia do crime, o que obsta a eventual conflito negativo, ou até mesmo positivo, de competências entre tribunais.

[409] FERREIRA, Manuel Cavaleiro de, ***Curso de Processo Penal I***, 1986, pág. 89, citado por SILVA, Germano Marques da, ***Curso de Processo Penal I – Noções Gerais, Elementos do Processo Penal***, 6ª Edição, Revista e Actualizada, Verbo, Edição Babel, Lisboa, 2010, pág 201

Ou seja, ***"se o crime estiver relacionado com áreas de jurisdição diversas e houver dúvidas sobre aquela em que se localiza o elemento relevante para determinação da competência territorial, é competente para dele conhecer o tribunal de qualquer das áreas de jurisdição, preferindo o daquela onde primeiro tiver havido notícia do crime. Se for desconhecida a localização do elemento relevante, é competente o tribunal da área de jurisdição onde primeiro tiver havido notícia do crime" (Cfr. artigo 25 n°1 e 2 do CPP).***

A regra geral de determinação da competência territorial é afastada aplicando-se *normas especiais*, naqueles processos em que sejam ofendidos *juízes de Direito ou magistrados do Ministério Público*, por infracções contra eles cometidas na área territorial sob jurisdição do tribunal a que pertencem, ou em que participem seus *parentes ou cônjuges* que sejam partes ofendidos, pois em tais casos é competente o tribunal *territorialmente mais próximo* e não aquele que, em atenção ao lugar da infracção, seria normalmente competente, o que se explica "…por razões evidentes de imparcialidade e prestígio de julgamento…"([410]).

Por via deste desvio à regra geral assegura-se que os processos em que estejam envolvidos magistrados judiciais e do Ministério Público na qualidade de vitimas, ou em que haja participação dos seus parentes ou cônjuges como partes ou ofendidos, sejam julgados por tribunal diferente daquele em que os magistrados em causa exercem funções, afastando desta forma eventuais factores de influência na imparcialidade do tribunal, visto tratarem-se de processos que directa ou indirectamente respeitam a magistrados.

Nesse sentido determinam as normas especiais constantes no artigo 27 do CPP, segundo o qual "*se num processo for ofendido pessoa com a faculdade de se constituir assistente ou parte civil um magistrado judicial ou do Ministério Público, e para o processo deva ter competência, por força das disposições anteriores, o tribunal onde o magistrado exerce funções, é competente o tribunal da mesma hierarquia ou espécie com sede mais próxima, salvo tratando-se do Tribunal Supremo".*

3.2.5.1.5. Competência Territorial por Factos Criminais Cometidos no Estrangeiro

"Se o crime for cometido no estrangeiro, é competente para dele conhecer o tribunal da área de jurisdição onde o agente tiver sido encontrado ou do seu domicílio. Quando ainda assim não for possível determinar a competência, este pertence ao tribunal da área de jurisdição onde primeiro tiver havido notícia do crime. Se o crime for cometido em parte no estrangeiro, é

[410] DIAS, Jorge de Figueiredo, ***Direito Processual Penal***, 1°. volume, 1.ª Edição – 1974, Reimpressão, Coimbra, 2004, pág. 344

competente para dele conhecer o tribunal da área nacional onde tiver sido praticado o último acto relevante, nos termos das disposições anteriores" (Cfr. artigo 26 do CPP).

3.2.5.1.5.1. Competência Territorial por Factos Criminais Cometidos a Bordo de Navio ou Aeronave

É competente para conhecer de crime cometido a bordo de navio o tribunal da área de jurisdição do porto moçambicano para onde o agente se dirigir ou onde ele desembarcar; e, não se dirigindo o agente para território moçambicano ou nele não desembarcando, ou fazendo parte da tripulação, o tribunal da área de jurisdição da matrícula (Cfr. artigo 24 n°1 do CPP).

Igualmente é competente para conhecer de crime cometido a bordo de aeronave, o tribunal da área de jurisdição do aeroporto moçambicano para onde o agente se dirigir ou onde ele aterrar; e, não se dirigindo o agente para território moçambicano ou nele não aterrando, ou fazendo parte da tripulação, o tribunal da área de jurisdição da matrícula (Cfr. artigo 24 n°2 do CPP).

Nos casos em que não é aplicável o critério do local onde o agente se dirigir, desembarcar, aterrar ou da jurisdição da matrícula, é competente o tribunal da área de jurisdição onde primeiro tiver havido notícia do crime (Cfr. artigo 24 n°3 do CPP).

3.2.5.1.6. Competência (do Tribunal Penal) por Conexão

As regras de determinação da competência material e territorial podem, em alguns casos, sofrer alterações ou excepções, quer porque existem especiais conexões entre diferentes infracções ou verificam-se prorrogações de competência resultantes da lei em certos casos, quer porque surgem conflitos de competência entre vários tribunais.

Assim, entre vários crimes pode haver uma particular relação, ditada pela sua **proximidade material ou objectiva, ou pessoal ou subjectiva**, ou ambas, relação essa de que resulta ser conveniente o seu julgamento conjunto, daí que tal "…relação entre crimes,… determina excepções à regra de que a cada crime corresponde um processo e às regras de competência material, funcional e territorial, definidas em função de um crime e, representa um desvio às regras normais da competência em razão da organização de um único processo para uma pluralidade de crimes ou a apensação de vários processos que hão-de ser apreciados e decididos conjuntamente"([411]).

[411] SILVA, Germano Marques da, ***Curso de Processo Penal I – Noções Gerais, Elementos do Processo Penal***, 6ª Edição, Revista e Actualizada, Verbo, Edição Babel, Lisboa, 2010, pág. 207-208

Em tal caso, o julgamento conjunto deduzirá uma excepção aos princípios determinantes da competência material ou territorial, por tratar-se de competência por conexão, justo focada, acima de tudo, por razões de economia processual e de boa administração da justiça penal (juntando processos conexos será provavelmente mais esgotante a produção probatória e respectiva cognição) e mesmo de prestígio das decisões judiciais, sendo que tal caso o princípio do juiz natural não é posto em causa, porque os critérios de conexão através dos quais irá se determinar o tribunal competente são estabelecidos, previamente, de forma geral e abstracta, por lei anterior.

Assim, para todos os crimes determinantes de uma conexão, organiza-se um só processo. Se tiverem já sido instaurados processos distintos, logo que a conexão for reconhecida procede-se à apensação de todos àquele que respeitar ao crime determinante da competência por conexão (Cfr. artigo 32 do CPP). Oficiosamente, ou a requerimento do Ministério Público, do arguido, do assistente ou do lesado, o tribunal faz cessar a conexão e ordena a separação de algum ou alguns processos, sempre que (artigo 34 do CPP):

a) Houver na separação um interesse ponderoso e atendível de qualquer arguido, nomeadamente no não prolongamento da prisão preventiva;

b) A conexão puder representar um grave risco para a pretensão punitiva do Estado, para o interesse do ofendido ou do lesado;

c) A conexão puder retardar excessivamente o julgamento de qualquer dos arguidos;

d) A audiência de julgamento decorrer na ausência de um ou alguns dos arguidos e o juiz tiver como mais conveniente a separação de processos.

Note-se que a competência determinada pela conexão se mantém: (*a)* mesmo que, relativamente ao crime ou aos crimes determinantes da competência por conexão, seja proferida sentença absolutória ou a responsabilidade penal se extinga antes do julgamento; (*b)* para o conhecimento dos processos separados nos termos já referenciados anteriormente (Cfr. artigo 35 do CPP).

Importa referir que a conexão só opera relativamente aos processos que se encontrarem simultaneamente na fase de instrução, de audiência preliminar ou de julgamento (artigo 28 n°3 do CPP). A conexão não opera entre processos que sejam e processos que não sejam da competência de tribunais de menores e do Tribunal Supremo ou tribunal superior de recurso, sempre que funcionarem em 1.ª instância e se se tratar de hipótese de conexão subjectiva e objectiva nos termos do artigo 32 conjugado com o artigo as alíneas b) e c) do número 1 do artigo 28 ambos do CPP.

3.2.5.1.6.1. Competência (do Tribunal Penal) por Conexão Pessoal ou Subjectiva

Há conexão pessoal ou subjectiva sempre que uma diversidade ou pluralidade de infracções se encontra relacionada ou ligada através da unidade do agente ou a um só agente. Com efeito, "*há conexão de processos quando o **mesmo agente** tiver cometido vários crimes através da mesma acção ou omissão, na mesma ocasião ou lugar, sendo uns causa ou efeito dos outros, ou destinando-se uns a continuar a ocultar os outros; (Cfr. artigo 28 n°1 alínea a) do CPP).*

Ademais*, há conexão de processos quando o mesmo agente tiver cometido vários crimes cujo conhecimento seja da competência de tribunais com sede na mesma área de jurisdição, de acordo com as regras gerais de competência territorial (Cfr. artigo 29 conjugado com o artigo 23 e seguintes ambos do CPP).*

Assim, na conexão pessoal ou subjectiva haverá sempre concurso real de infracções (**varias infracções cometidas pelo mesmo agente**), e porque pelo cometimento de tais infracções deve ser aplicada uma única pena (cúmulo jurídico),

> *o tribunal competente para conhecer de tais infracções será único, concretamente, o da infracção a que couber pena mais grave, e no caso de infracções de igual gravidade, o tribunal a cuja ordem o arguido estiver preso (Cfr. artigo 31 n°1 alínea a) e b) do CPP). Se o arguido não estiver preso (no caso de infracções de igual gravidade), será competente o tribunal da área onde primeiro tiver havido notícia de qualquer dos crimes (Cfr. artigo 31 n°1 alínea c) do CPP). Se o arguido tiver foro especial, é este foro especial ou tribunal de competência especializada, que será competente para de todos conhecer (artigo 31 n°2 do CPP).*

Das regras excepcionais de determinação da competência territorial, resulta que na eventualidade de o mesmo agente ter cometido diversas infracções e tiverem sido instauradas diversos processos, estes deverão ser apensados àquele que respeite a infracção que determinar a competência para o julgamento (artigo 32 do CPP). Como uma das razões justificativas da apensação de diversos processos instaurados contra o mesmo agente aquele que tem por objecto infracção que determinar a competência para o julgamento, conforme referido anteriormente, é de apontar a necessidade de avaliar a personalidade do agente que, sendo de particular relevo em direito penal e de direito processual penal, tem como pressuposto a concentração de processos que lhe digam respeito ([412]).

[412] SANTOS, Gil Moreira dos, ***O Direito Processual Penal***, 1ª Edição, Janeiro de 2003, Edições ASA, pág. 187.

3.2.5.1.6.2. Competência (do Tribunal Penal) por Conexão Material ou Objectiva

A conexão material ou objectiva, pressupondo sempre uma pluralidade de agentes, pode assumir a forma de conexão objectiva por comparticipação criminosa ou conexão objectiva por infracções reciprocas e simultâneas.

Por um lado, será **conexão objectiva por comparticipação criminosa**, quando uma mesma infracção tiver sido levada a cabo por diversos agentes (autores e cúmplices que comparticiparam na mesma infracção). Ou seja, "***há conexão de processos quando o mesmo crime tiver sido cometido por vários agentes em comparticipação (Cfr. artigo 28 n°1 alínea b) do CPP).*** Nesta modalidade de **conexão objectiva (por comparticipação criminosa),** a lei determina que *o tribunal competente para conhecer de tal infracção será único, concretamente, o tribunal competente para conhecer a infracção a que couber pena mais grave, e no caso de infracções de igual gravidade, o tribunal a cuja ordem o maior número dos arguidos estiver preso (Cfr. artigo 31 n°1 alínea a) e b) do CPP). Se não houver arguidos presos ou o seu número for igual, será competente o tribunal da área onde primeiro tiver havido notícia de qualquer dos crimes (Cfr. artigo 31 n°1 alínea c) do CPP). Se algum ou alguns dos agentes comparticipantes tiverem ou tiverem foro especial, é este foro especial ou tribunal de competência especializada, que será competente para de todos conhecer (artigo 31 n°2 do CPP).*

Por outro lado, será **conexão objectiva por infracção reciproca e simultâneas** quando diferentes infracções tenham sido cometidas na mesma ocasião, reciprocamente, ou por várias pessoas reunidas. Ou seja, "*há conexão de processos quando vários agentes tiverem cometido diversos crimes em comparticipação, reciprocamente, na mesma ocasião ou lugar, sendo uns causa ou efeito dos outros, ou destinando-se uns a continuar ou a ocultar os outros" (Cfr. artigo 28 n°1 alínea c) do CPP).* Importa esclarecer que crimes recíprocos são aqueles em que há uma interligação da causa e efeito; e os agentes ofendem-se uns aos outros, na mesma ocasião, aparecendo também com a qualidade de ofendidos ([413]).

Nesta segunda modalidade de conexão objectiva (por infracções reciprocas ou simultâneas), a lei determina igualmente que *o tribunal competente para conhecer de tal infracção será único, concretamente, o tribunal competente para conhecer a infracção a que couber pena mais grave, e no caso de infracções de igual gravidade, o tribunal a cuja ordem*

[413] GONÇALVES, Manuel Lopes Maia, ***Código de Processo Penal, Anotado e Comentado***, 2ª Edição, Edições Almedina, AS, Maio, 2007, pág. 114

o maior número dos arguidos estiver preso (Cfr. artigo 31 n°1 alínea a) e b) do CPP). Se não houver arguidos presos ou o seu número for igual, será competente o tribunal da área onde primeiro tiver havido notícia de qualquer dos crimes (Cfr. artigo 31 n°1 alínea c) do CPP). Se algum ou alguns dos agentes comparticipantes tiverem ou tiverem foro especial, é este foro especial ou tribunal de competência especializada, que será competente para de todos conhecer (artigo 31 n°2 do CPP).

3.2.5.1.6.3. Competência (do Tribunal Penal) por Conexão nas Contravenções e Transgressões.

Podem ser processadas e julgadas conjuntamente as contravenções e transgressões a editais, posturas ou disposições regulamentares que constem do mesmo auto de notícia levantado contra diversos infractores, ainda que não se verifiquem as condições exigidas para a conexão subjectiva ou objectiva (artigo 28 n°2 do CPP).

3.2.5.1.7. Competência Material e Funcional (do Tribunal Penal) Determinada por Conexão

Se os processos conexos devessem ser da competência de tribunais de diferente hierarquia ou espécie, é competente para todo o tribunal de hierarquia ou espécie mais elevada (Cfr. artigo 30 do CPP).

Neste sentido, deve-se tomar em conta as categorias de tribunais judiciais, nomeadamente o Tribunal Supremo, os Tribunais Superiores de Recurso, os Tribunais Judiciais de Província e Tribunais Judiciais de Distrito, (artigo 29 da LOJ – Lei n° 24/2007, de 20 de Agosto).

3.2.4.2. Competência Territorial para Julgar os Crimes Cibernéticos.

Destaca-se que no âmbito dos crimes informáticos é extremamente difícil indicar o exacto momento da prática do acto ilícito, para que seja aplicada a consequente sanção penal. Isto porque, no meio informático existe uma dissociação temporal, pois é possível programar a execução de um crime informático no tempo, ou seja, o acto ilícito pode ser executado meses após a sua programação, devido o facto de todo computador possuir um relógio interno.

O Código Penal Moçambicano adoptou a teoria da actividade para descrever o momento do crime. Assim sendo, a prática de um crime ocorre no momento da acção ou omissão, independentemente do momento do resultado (art. 2 do CP).

Todavia, no mundo virtual não existe um espaço físico predeterminado e tão pouco um espaço geograficamente delimitado. Assim, para a constatação da prática de um determinado crime informático é necessário detectar a localização da informação, pois esta será essencial para proporcionar a ideia de território. Ademais, cumpre esclarecer ainda que o espaço virtual é denominado de "ciberespaço", que indica o local onde ocorre todo fluxo de informações através das redes de comunicações. Desta forma, grande parte dos crimes virtuais supera fronteiras territoriais, pois o mundo está conectado à internet. Com efeito,

> "Um dos maiores problemas com relação à efectiva resolução dos crimes, no âmbito digital, se dá por conta da fixação da jurisdição e da competência. A jurisdição é uma das funções do Estado, onde ele substitui as partes na solução dos conflitos. Embora seja um poder único, é repartido em vários órgãos do Estado, por praticidade. Surge a competência – uma dessas repartições – que é o limite de actuação do juiz em determinado território. Como decidir, então, qual juiz será competente se o crime não é praticado no meio físico?"([414]).

A legislação processual penal moçambicana não responde especificamente sobre a questão do tribunal competente para julgar os crimes cibernéticos, mas a aplicação de alguns princípios do Código Penal de 2019 pode responder à questão. com efeito, para determinar o tribunal competente para julgar os crimes cibernéticos pode se recorrer aos princípios da territorialidade (art. 4 do CP), da extraterritorialidade (art. 5 do CP), da nacionalidade e, defesa dos interesses nacionais (art.2 do CPP) e da representação (art. 7 do CPP).

Como já fizemos referência, em relação à competência territorial¸ o critério da sua aferição será o do lugar da prática do crime cibernético. Num primeiro momento haverá a necessidade de aferir a conexão entre a infracção e o lugar ou zona geográfica onde o facto que o configura ocorreu, podendo haver critérios subsidiários para aqueles casos em que aquele se revele em concreto inadequado. O referido critério do lugar da infracção vem patente, nos artigos 23 e seguintes do CPP conjugado com o artigo 5 do CP. Assim, com as necessárias adaptações podemos afirmar que ***"é competente para conhecer de um crime cibernético o tribunal em cuja área de jurisdição se tiver verificado a consumação*****" (Cfr. artigo 23 n°1 do CPP conjugado com o artigo 5 do CP).** Trata-se do critério geral de determinação da competência territorial que é da consumação da infracção, em termos de área em que se

([414]) COLLI, Jonathan Delli, & BEZERRO, Eduardo Buzetti Eustachio. A tutela jurídico-penal dos crimes digiatais. Colloquium Socialis, Presidente Prudente, v. 01, n. Especial 2, Jul/Dez, 2017, p.139-145.

consumou a infracção ser considerada em princípio, o *locus delicti*, pelo que para os chamados crimes materiais ou de resultado interessará, para efeitos de consumação da infracção, a produção do evento típico, sendo assim irrelevante o fim do exercício da actividade ou termo da omissão.

Quanto as infracções praticadas, em parte, em território nacional, vale também o critério da consumação, bem assim se atende ao lugar ou área onde a execução, preparação ou comparticipação do facto se verificou, desde que o mesmo seja punível pela lei moçambicana, e no caso de factos de encobrimento praticados em território nacional é competente o tribunal do lugar onde se praticou o facto que configura encobrimento (artigo 23 n°1 do CPP).

No entanto, porque o resultado da infracção pode não chegar a se consumar e, por conseguinte, não podendo valer o princípio geral da determinação da competência territorial (lugar da infracção), a lei prevê um critério subsidiário e excepcional, do qual resulta que será competente territorialmente em cuja área se praticou ou cometeu o último acto de execução da infracção ou último facto punível. Ou seja, podemos afirmar com as necessárias adaptações que ***se o crime cibernético não tiver chegado a consumar-se, é competente para dele conhecer o tribunal em cuja área de jurisdição se tiver praticado o último acto de execução ou, em caso de punibilidade dos actos preparatórios, o último acto de preparação" (Cfr. artigo 23 n°3 do CPP).***

Estaríamos perante infracção que não chegou a se consumar num caso de tentativa ou frustração, e ainda quando se trate de actos preparatórios que em si configurem crime autónomo e, como tal, punível (artigo 22 n°2 conjugado com o artigo 19 do CP).

Pode suceder que, tendo a infracção sido cometida nos limites de diversos distritos, províncias, haja dúvidas sobre o lugar em que foi. Em tal hipótese de **crimes de localização duvidosa ou desconhecida,** consagra um **princípio de prevenção da jurisdição**, dando competência a qualquer dos tribunais, mas preferindo o que primeiro tomar conhecimento da infracção", ou seja, o tribunal da circunscrição onde primeiro tiver havido notícia do crime, o que obsta a eventual conflito negativo, ou até mesmo positivo, de competências entre tribunais. Ou seja,

> "se o crime cibernético estiver relacionado com áreas de jurisdição diversas e houver dúvidas sobre aquela em que se localiza o elemento relevante para determinação da competência territorial, é competente para dele conhecer o tribunal de qualquer das áreas de jurisdição, preferindo o daquela onde primeiro tiver havido notícia do crime. Se for desconhecida a localização do elemento relevante, é competente o tribunal da área de jurisdição onde primeiro tiver havido notícia do crime*" (Cfr. artigo 25 n°1 e 2 do CPP).*

A regra geral de determinação da competência territorial é afastada aplicando-se *normas especiais,* naqueles processos em que sejam ofendidos *juízes de Direito ou magistrados do Ministério Público,* por infracções contra eles cometidas na área territorial sob jurisdição do tribunal a que pertencem, ou em que participem seus *parentes ou cônjuges* que sejam partes ofendidos, pois em tais casos é competente o tribunal *territorialmente mais próximo* e não aquele que, em atenção ao lugar da infracção, seria normalmente competente, o que se explica "…por razões evidentes de imparcialidade e prestígio de julgamento…"([415]).

Por via deste desvio à regra geral assegura-se que os processos em que estejam envolvidos magistrados judiciais e do Ministério Público na qualidade de vitimas, ou em que haja participação dos seus parentes ou cônjuges como partes ou ofendidos, sejam julgados por tribunal diferente daquele em que os magistrados em causa exercem funções, afastando desta forma eventuais factores de influência na imparcialidade do tribunal, visto tratarem-se de processos que directa ou indirectamente respeitam a magistrados.

Nesse sentido, determinam as normas especiais constantes no artigo 27 do CPP, segundo o qual "*se num processo for ofendido pessoa com a faculdade de se constituir assistente ou parte civil um magistrado judicial ou do Ministério Público, e para o processo deva ter competência, por força das disposições anteriores, o tribunal onde o magistrado exerce funções, é competente o tribunal da mesma hierarquia ou espécie com sede mais próxima, salvo tratando-se do Tribunal Supremo".*

A partir do entendido, parece-nos defensável afirmar que "se o crime cibernético for cometido no estrangeiro, é competente para dele conhecer o tribunal da área de jurisdição onde o agente tiver sido encontrado ou do seu domicílio. Quando ainda assim não for possível determinar a competência, este pertence ao tribunal da área de jurisdição onde primeiro tiver havido notícia do crime. Se o crime cibernético for cometido em parte no estrangeiro, é competente para dele conhecer o tribunal da área nacional onde tiver sido praticado o último acto relevante, nos termos das disposições anteriores" (Cfr. artigo 26 do CPP conjugado com o artigo 5 do CP).

Tendo em conta a doutrina dominante sobre a competência territorial para julgar os crimes cibernéticos, entendemos que a teoria do resultado com relação ao lugar da prática do crime cibernético, se mostra mais ajustada. Assim, sugere-se que de *iure condendo,* **seja adoptada a teoria do resultado com relação ao lugar da prática do crime cibernético.**

[415] DIAS, Jorge de Figueiredo, ***Direito Processual Penal***, 1°. Volume, 1.ª Edição – 1974, Reimpressão, Coimbra, 2004, pág. 344

Assim, a competência para julgar um crime cibernético, seria o local onde se encontre o computador violado, pois nesse local é onde houve a consumação do crime.

3.3. Meios de Provas nos Crimes Cibernéticos

3.3.1. Provas – conceptualização

Com o surgimento da internet, vários são os benefícios que ela traz para a humanidade. Porém, esse avanço tecnológico está correndo ao lado da utilização ilimitada e indiscriminada desse meio virtual, favorecendo os acontecimentos dos crimes virtuais e, consequentemente, dando alerta a visão jurisdicional na esfera processual penal.

O Processo Penal corresponde a uma sequência de actos juridicamente preordenados e praticados por determinados sujeitos processuais, com legitimidade para o efeito, isto é, autorizados, em ordem à emissão de decisão, na qual apura-se se foi praticado o acto que viola bens jurídicos tutelados pelo direito penal. No Processo Penal, o objectivo das partes que litigam em juízo, circunscrevem-se na "capacidade de convencer o julgador através de uma reconstrução histórica dos factos ocorridos tendo como base o conjunto probatório anexado aos autos[416]. O Processo Penal é um instrumento utilizado para reconstruir determinado facto histórico da forma mais aproximada possível da realidade. Para que seja feita a reconstrução do passado, é fundamental que haja provas, que são meios utilizados para apurar a verdade material. Nesse corolário, a constituição da prova é uma ferramenta que possui grande importância para o Direito.

A prova é um dos pressupostos fundamentais para atingir a verdade, sendo o principal meio para convencer o juiz que deverá promulgar sentença mais justa possível e de acordo com que entender ser a verdade dos factos. Nesse caso, os meios de prova "são todos os instrumentos que se destinam a levar ao processo um elemento, uma informação a ser utilizada pelo juiz para formar uma convicção acerca dos factos alegados pelas partes. Pode ser facto, alegações, documentos, imagens, algum parecer que auxilie directa ou indirectamente um desvendar da verdade dos factos"[417].

Ainda neste contexto, por Prova "Entende-se, assim, no sentido jurídico, a demonstração que se faz, pelos meios legais, da existência ou veracidade de um facto material ou de um acto

[416]TAVORA, Nestor; ALENCAR, Rosmar Rodrigues, ***Curso de Direito Processual Penal***, Jus Podivm, Salvador, 2012. p. 376.

[417] PINTO, Samara Silva, *Dos Crimes Virtuais, da Obtençcão das Provas e as Tendências Jurídicas decorrentes da Evolução Tecnológica*. Instituto Brasileiro de Direito Público - IDP, Brasília-DF. Disponível no https://www.idp.edu.br, acessado no dia 3 de Janeiro de 2024.

jurídico, em virtude da qual se conclui por sua existência ou se afirma a certeza a respeito da existência do facto ou do acto demonstrado"[418].

A prova consiste no "esforço metódico através do qual são demonstrados os factos relevantes para a existência do crime, a punibilidade do arguido e a determinação da pena ou medida de segurança aplicáveis"[419]. As provas têm por função a demonstração da realidade dos factos (341.º do Código Civil) sendo que "constituem objecto da prova todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis"[420]

A doutrina apresenta-nos vários tipos de prova:

> "**a prova perfeita** que leva à conclusão de que o agente praticou ou não o ilícito-típico; a prova imperfeita que carece da conjugação com outras provas para que se chegue a uma conclusão; **a prova directa** dá-se quando incide directamente sobre os factos que se pretendem provar; e **a prova indiciária** que é uma **prova indirecta,** obtida através da indução e de um raciocínio empírico, da ciência ou da técnica verifica-se (induz-se) o facto que se quer provar, parte-se de um facto conhecido (que indicia) para o facto desconhecido que se procura provar, o indício é necessário quando o facto respeite a uma só causa, mas quando possa ser atribuído a várias causas já será um indício provável ou possível; **as provas pessoais** são recolhidas pela declaração da própria pessoa e pelos comportamentos desta quando presta depoimento (expressões), **na prova real ou prova pessoal passiva,** a pessoa é antes objecto de observação, não importando nestas o alcance das declarações"[421].

No nosso ordenamento jurídico, há liberdade de prova, desde que não seja prova proibida por lei[422], o que demonstra a inexistência de um elenco taxativo das provas admissíveis, segundo os ditames do CPP[423]. Com efeito, os meios de prova previstos no nosso CPP são nomeadamente: Testemunhais (art. 159 do CPP), Declarativas (art. 174 do CPP), Acareactivas (180 do CPP), Reconhecimento de pessoa (art, 181 do CPP) e de Objecto (art. 182 do CPP), Reconstitutivas do facto (art. 184 do CPP), Periciais (art. 185 do CPP) e Documentais (art. 199 do CPP).

Como se pode notar, os meios de prova referidos no parágrafo anterior referem-se a um conjunto de acções praticadas pelas partes, juiz ou terceiros, destinadas a comprovar ao juiz a

---

[418] CAGLIARI, José Franciscol, ***Prova em Processo Penal*** – SP, disponível em https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_publicacao_divulgacao/doc_gra_dout_crim/crime%2038.pdf, acessado no 3 de Janeiro de 2024.

[419] MENDES, Paulo de Sousa, ***As proibições de prova no processo penal.*** Apud RIBEIRO, Maria da Conceição Fernandes, ***Cibercrime e a prova digital.*** Dissertação de Mestrado em Ciências Jurídico-Forenses. Instituto Superior Bissaya Barreto, Coimbra, 2015. p.41. disponível no Repositorio Comum: https://comum.rcaap.pt/bitstream/10400.26/28946/1/Cibercrime%20e%20Prova%20Digital.pdf, acessado no dia 29 de dezembro de 2023.p.39.

[420] Cfr., o art. 155 do CP.

[421] RIBEIRO, Maria da Conceição Fernandes, ***ob. cit***., p.42.

[422] Cfr., art. 156 do CPP.

[423] Cfr, art. 157 do CPP.

ocorrência ou não do facto, a veracidade ou não de uma informação, isto é, por via desses meios de prova expressamente configurados na Lei, pretende-se trazer uma percepção cujo objectivo é comprovar a veracidade de uma alegação.

A inexistência de provas idóneas e válidas implica na impossibilidade de uma condenação. Esta só ocorrerá quando houver uma certeza acerca da culpabilidade que não é obtida através de suposições e alegações não comprovadas. Para J. E. Carreira Alvim, a prova pode ser conceituada sob duas acepções distintas: no sentido objectivo e no sentido subjectivo. Objectivamente, as provas correspondem a todos os métodos utilizados para demonstração da existência ou não de um facto jurídico ou aos métodos utilizados com propósito de esclarecimento da ocorrência para que o juiz conheça da verdade dos factos. Subjectivamente, é a "convicção que se forma no espírito do juiz quanto à verdade dos fatos". A prova está intimamente ligada à demonstração da verdade dos factos[424].

3.3.2. Objecto da Prova

Nas reflexões das sessões anteriores, chegamos ao entendimento de que a prova é um elemento instrumental em que as partes fazem uso para convencer, fundadamente, o juiz da sua pretensão num processo. Outrossim, a prova é o meio através do qual o juiz se serve para averiguar os factos em que as partes fundamentam suas alegações. É ela, como resume Moacyr Amaral Santos, "a soma dos factos produtores da convicção, apurados no processo"[425]. Nesses termos, "Objecto da prova, ou *thema probandum*", escreve Frederico Marques, "é a coisa, facto, acontecimento ou circunstância que deva ser demonstrado no processo" (...) "Como o juiz se presume instruído sobre o direito a aplicar, os actos instrutórios só se referem à prova das *quaestiones facti*. O juiz deve conhecer o Direito. Essa obrigação é elementar para o exercício da jurisdição (jura novit curia). Donde se segue que, abstractamente falando, constitui objecto de prova tão-só o que diz respeito às questões de fato surgidas no processo"[426].

Dos conceitos apresentados nas diversas dimensões discursivas, somos de entendimento que o objecto da prova, portanto, são os factos pertinentes ao processo e que suscitam o interesse da parte em demonstrá-los. Porém, se os Factos não pertencem ao litígio e não têm nenhuma relação com o objecto da acusação, consideram-se factos sem pertinência, pelo que devem ser

[424] ALVIM, Carreira, ***Teoria Geral do Processo,*** revista, ampliada e actualizada, Editora Forense, Rio de Janeiro, 2009. p. 260.
[425] CAGLIARI, José Franciscol. ***ob. cit***.
[426] MARQUES, José Frederico, ***"Elementos de Direito Processual Penal".*** Campinas: Bookseller, 1997. Vols. I e II.

excluídos do âmbito da prova em concreto e ter a sua prova recusada pelo juiz, sob pena de se desenvolver actividade inútil. Além de pertinentes, só devem ser objecto de prova "os factos relevantes, por estes" entendendo-se aqueles "que podem influir, em diferentes graus, na decisão da causa"[427].

Outrossim, os factos relevantes e pertinentes devem fundamentar a acção e a defesa capazes de influenciar na decisão do juiz, na responsabilidade penal e na fixação da pena, necessitando, portanto, de adequada comprovação em juízo. Isto é o que se insere no nosso CPP, ao preceituar que são objecto da prova "todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido, e a determinação da pena ou da medida de segurança aplicáveis" (nº 1 do art. 155). A norma em alusão, aponta ainda que "se tiver lugar pedido civil, constitui, igualmente, objecto da prova, os factos relevantes para a determinação da responsabilidade civil" (nº 2 do art. 155). A devida demonstração dos factos em juízo é fundamental para que um processo tenha prosseguimento, e consequentemente possa viabilizar o julgamento.

Entretanto, somente os factos relevantes, relacionados ao litígio, poderão ser considerados objectos da prova. Em respeito ao princípio da economia processual, o juiz deve dirigir o processo de forma a evitar que atrasos em seu curso ocorram em decorrência do requerimento de provas dispensáveis ou simplesmente protelatórias ocasionalmente feito pelas partes. Alguns factos carecem de provas e outros não.

De forma diversa ao que se verifica no processo civil, a falta de controvérsia sobre um facto não dispensa a prova. "No processo penal, não se exclui do objecto da prova o chamado facto incontroverso ou facto admitido. Na investigação criminal – como ensina Fenech – "*el julgador debe llegar a la verdad de los hechos tal como ocurrieran historicamente, y no tal como quieran las partes que aparescan realizados"*[428]. Assim, a confissão, por exemplo, que elimina a controvérsia sobre a autoria, não dispensa a necessidade de outras provas sobre ela e que, aliás, deverão corroborá-la.

Em conformidade com Cagliari, "Os factos evidentes e os notórios dispensam prova, segundo a máxima notória "*vel manifesta non egent probatione"* (o notório e o evidente não precisam de prova). Sem embargo, porém, se tais factos notórios corresponderem a elementares do tipo penal deverão ser objecto de prova. Não é porque a morte de alguém seja facto notório que poderá ser dispensado o exame de corpo de delito"[429].

---

[427] CAGLIARI, José Franciscol, ***ob. cit.***.
[428] Ibidem.
[429] CAGLIARI, José Franciscol, ***ob. cit.***.

Certamente, os factos notórios pela sua natureza não necessitam ser provados. Por isso, uma parte da doutrina chama-se de verdade sabida, pois já são de conhecimento público, já fazem parte da cultura de uma sociedade. Segundo Mossim, "o facto notório é aquele de existência vulgarizada, indicando-se uma verdade irretorquível que deve ser aceita sem discrepância"[430].

Ao lado dos factos notórios, estão as chamadas máximas da experiência ou regras da experiência, que também dispensam prova. São elas as noções e futuros conhecimentos ministrados pela vida prática e os costumes sociais ou, como escreve Santos, "juízos formados na observação do que comummente acontece e que, como tais, podem ser formados em abstracto por qualquer pessoa de cultura média"[431]. Daí que Santos explica:

> "em cada esfera social, da mais letrada à mais humilde, há uma porção de conhecimentos que, tendo passado por uma experiência contínua e prolongada, ou, quando não, pelo crivo da crítica coletiva, fruto da ciência, da arte, da técnica ou dos fatos cotidianos, faz parte de sua communis opinio. É certo, por outro lado, que essa communis opinio pode variar, conforme o lugar, o tempo, o progresso da ciência ou da técnica, as transformações políticas, sociais, religiosas etc., mas não deixa de ser também certo que as afirmações nela fundadas, por qualquer membro da esfera social, em que se formou, adquirem autoridade que a afirmação individual não pode ter, porque aquela traz consigo e resulta da crítica e da apuração coletiva"[432].

Há outra categoria dos factos, que interessam nesta classificação: são as presunções. As presunções legais são factos que a lei presume que tenham ocorrido. O exemplo mais clássico é a inocência do réu. A Lei presume a inocência do réu, portanto, não cabe ao réu provar que é inocente, pois este facto já é presumido. No entanto, este facto é uma presunção relativa, ou seja, pode ser também, absoluta, ou seja, não admitir prova em contrário. Um outro exemplo é a presunção de que o menor de 12 anos não tem condições mentais de consentir na realização de um acto sexual, sendo, portanto, crime contra trato sexual com menores (art. 202 do CP), estamos perante a uma presunção absoluta de incapacidade para consentir, ou presunção iure et de iure). Frise-se que embora o facto presumido independa de prova, o facto que gera a presunção deve ser provado. Assim, embora seja presumida a incapacidade para consentir do menor de 12 anos, a condição de menor de 12 anos deve ser objecto de prova.

[430] Ibidem.
[431] Ibidem.
[432] Ibidem.

3.3.3. Classificação da Prova

Os doutrinadores apresentam inúmeras classificações da prova, segundo diversos critérios. Santos[433], acolhendo o sistema proposto por Malatesta, que classifica as provas segundo três critérios, apresenta-os como sendo: o do objecto, o do sujeito e o da forma.

a) **Objecto da prova**: é o facto a provar-se. Quanto a ele, as provas são directas ou indirectas. Refere-se às primeiras provas, directa e imediatamente ao facto a ser provado. As segundas dizem respeito a outro (s) facto (s) que, por sua vez, se liga (m) ao facto a ser provado. São provas indirectas as presunções e indícios. A prova indirecta é também chamada de circunstancial, assim definida por João Mendes Júnior: "prova circunstancial é, pois, aquela que se deduz da existência de um facto ou de um grupo de factos, que, aplicando-se imediatamente ao facto principal, levam a concluir que este facto existiu"[434].

b) **Sujeito da prova** é a pessoa ou coisa de quem ou de onde dimana a prova; a pessoa ou coisa que afirma ou atesta a existência do facto provando. A Prova pessoal é toda afirmação pessoal consciente, destinada a fazer fé dos factos afirmados, como a testemunha que narra o facto que presenciou. A Prova real de um fato consiste na atestação inconsciente, feita por uma coisa, das modalidades que o facto provado lhe imprimiu. As Provas reais são, por exemplo, o lugar, a arma, o cadáver, a ferida etc. Para estas, Vicente de Azevedo prefere falar em "meios de prova objectivos e meios de prova subjectivos"[435].

c) **Forma da prova** é a modalidade ou maneira pela qual se apresenta em juízo. Em relação à forma, a prova é testemunhal, documental ou material. A Prova testemunhal, em sentido amplo, é a afirmação pessoal oral, compreendendo as produzidas por testemunhas, declarações da vítima e do réu. A Documental é a afirmação escrita ou gravada. Diz-se material a prova consistente em qualquer materialidade que sirva de prova ao facto provado; é a atestação emanada da coisa: o corpo de delito, os exames periciais, os instrumentos do crime etc.

Aos critérios de classificação, acrescenta-se o referido por Moacyr Amaral Santos e por Frederico Marques[436], o qual leva em consideração **a preparação das provas,** dividindo-as em **causais e pré-constituídas**. Por causais, também chamadas de simples consideram-se as provas preparadas no curso da demanda. São causais as provas testemunhais, os exames periciais etc. Pré-constituídas, em sentido amplo, são as provas preparadas preventivamente, em vista de

[433] CAGLIARI, José Franciscol. ***ob. cit.***
[434]ibidem..
[435] Ibidem,
[436] CAGLIARI, José Franciscol. ***ob. cit***.

possível utilização em futura demanda. Em sentido estrito, dizem-se pré-constituídas as provas consistentes em instrumentos públicos ou particulares, representativos de actos jurídicos que pelos mesmos se constituem.

3.3.4. Características das Provas Digitais

As principais características das provas digitais[437] são: o **carácter temporário**, pelo decurso do tempo a prova pode deixar de existir; é fungível, dada a facilidade de substituição dos dados informáticos por outros; é **volátil**, pois facilmente se escondem esses dados, podendo ser ocultados ou suprimidos, do suporte original; por fim, cumpre-nos salientar a **fragilidade da prova,** cujo manuseamento deverá ser cuidadosamente efectuado[438]. Como bem repara Miren Josune Pérez Estrada,

> "(...) *no se puede cuestionar que la evolucíon tecnolólica ha supuesto un incrementode la calidad de vida y un desarrollo en laestructura social y económica. Se habla ya de una nueva civilización caracterizada por la instantaneidad y la desaparicíon de las distâncias, pero tambíen es evidente que este gran avance tecnológico perjudica, en ocasiones, los intereses ajenos. Aparecen nuevos medios para delinquir y ello conlleva la necesidad de investigar dichos delitos através de los, tambíen, nuevos medios tecnológicos*"[439].

Tendo em atenção as características inerentes às provas digitais, ilidimos que a maior dificuldade para apurar um crime informático é a obtenção de provas. Afinal onde estariam essas evidências armazenadas? Por onde começar a procurar? Tendo em consideração que cada Estado possui a sua própria soberania legislativa, como lidar com questões jurídicas que envolvem mais de um Estado com leis diversas ou mesmo um País sem uma legislação específica no âmbito dos crimes cibernéticos?

De facto, há uma clara evidência que as provas virtuais são uma matéria que precisa de ser tratada com maior delicadeza e profundeza, visto serem muito sensíveis, com maior possibilidade de serem destruídas num momento para outro. Por isso, a perda de integridade, por serem provas de cunho sensível, há obstáculos quanto à sua utilização. A dificuldade enfrentada pela maioria dos países é a falta de instrumentos eficientes para recolha de provas pela via virtual.

---

[437] RIBEIRO, Maria da Conceição Fernandes.***ob. cit***. pp. 48-49.
[438] Ibidem, pp. 48-49.
[439]Ibidem, p.49.

Assim sendo, vale a pena ressaltar que, quase todo crime cometido, no qual há um computador relacionado, se as provas digitais não forem recolhidas adequadamente, com uso das ferramentas técnicas apropriadas, pode ser invalidado em possível litígio judicial. As provas digitais são extremamente frágeis, de forma que, se não forem tratadas dentro de padrões técnicos específicos, não deixem rastos para as dúvidas.

A maior crítica dos especialistas em crimes cibernéticos é exactamente a falta de legislação, bem como carência em termos de cooperação internacional que em muito prejudica as investigações de tais delitos. O desejo é um só: que todos os países tenham seu ingresso na Convenção de Budapeste. Com efeito, ocorre que, por se tratar de uma Convenção formalizada pelo Conselho da Europa, é necessário que o mesmo convide todos os países do mundo para sua integração no tratado.

Desta forma, claramente se vê a necessidade de o nosso País priorizar o ingresso e realizar as articulações políticas necessárias para tal, já que nada a respeito até ao momento ocorreu. Se Moçambique ainda não legislou tais crimes, bem como o seu meio de investigação e produção de prova, decerto, não se preocupou de igual modo com a adesão a Tratados Internacionais sobre essa temática.

3.3.5. Princípios Relativos às Provas no Processo Penal

Sobre este assunto, é sobejamente consensual que as normas referentes às provas são normas processuais (natureza jurídica, direito subjectivo), ou seja, de aplicação imediata, sendo demonstradas em consequência dos crimes ocorridos na vigência de uma determinada lei. Nesse corolário, a prova deve ser usada para se referir aos elementos de convicção produzidos, via de regra, para o processo judicial e com a garantia do contraditório e da ampla defesa.

Nesta perspectiva, antes de abordar os princípios relativos às provas, importa classificá-las, segundo Nucci[440] nos seguintes critérios:

> "(i) Quanto ao objecto (relação da prova com o facto a ser provado): a prova dreferese directamente ao facto por si o demonstrando, como por exemplo, a testemunha visual. Já a prova indirecta refere-se a um outro acontecimento que leva ao facto, como por exemplo, o álibi, que de acordo com Nucci "é a alegação feita pelo acusado, como meio de provar a sua inocência, de que estava em local diverso de onde ocorreu o crime, razão pela qual não poderia tê-lo cometido".

[440] NUCCI, Guilherme de Souza, ***Manual de Processo e Execução Penal.*** 11. Ed. Rev., atual e ampl. Rio de Janeiro: Ed. Forense, 2014. Apud BARBOSA, Caroline Ap. Sales, ***Teoria Geral da Prova no Direito Processual penal Brasileiro***. Disponível no https://www.jusbrasil.com.br/artigos/teoria-geral-da-prova-no-direito-processual-penal-brasileiro/337514638, acessado no dia 30 de Dezembro de 2023.

> (ii) Quanto ao efeito ou valor (grau de certeza gerado pela apreciação da prova): a prova plena é aquela necessária para condenação e que imprime no julgador certeza quanto ao facto. Já a prova não plena ou indiciária é a limitada quanto à profundidade, permitindo, por exemplo, a decretação de medidas cautelares.
> (iii) Quanto ao sujeito ou causa: a prova real é aquela que resulta do facto, como por exemplo, as fotografias e pegadas do local do crime. Já a prova pessoal decorre do conhecimento de alguém, como por exemplo, a confissão e testemunha.
> (iv) Quanto a forma ou aparência: a prova testemunhal está relaccionada à afirmação de uma pessoa, independentemente dessa pessoa ser testemunha, com por exemplo, o interrogatório do réu. Já a prova material se trata de qualquer elemento que corporifica a demonstração do facto, com por exemplo, o exame de corpo de delito e os instrumentos do crime. Também há a prova documental".

Nucci diz que "as provas plenas consistem nas provas que possuem valor probatório suficiente para fundamentar por si só a decisão judicial sobre o facto que se pretende provar. Já as provas não plenas são as aquelas que não são idóneas nem suficientes para fundamentar por si só a decisão judicial sobre os factos que se pretende provar, senão que funcionam conjuntamente com outros mananciais probatórios, como um elemento a mais a permitir ao juiz inferir uma hipótese sobre esses factos mediante um procedimento de prova indirecta ou indutiva"[441]. Em razão do exposto, as provas não plenas somente podem coadjuvar a decisão em qualidade de indícios.

Os princípios relativos à prova são as seguintes as categorias:

3.3.5.1. Princípio da Legalidade

Em respeito do princípio da legalidade da prova, consta do art. 4 do CPP, que "São nulas as provas obtidas mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida sua privada e familiar, no domicílio, na correspondência ou nas telecomunicações". Outrossim, o princípio em alusão encontra a sua manifestação no art. 156.º do CPP ao preceituar que "são admissíveis as provas que não forem proibidas por lei"[442]. A nossa Constituição advoga serem nulas "todas as provas obtidas mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada e familiar, no domicílio, na correspondência ou nas telecomunicações"[443].

Tendo em atenção ao princípio da legalidade, concordamos com Gonçalves ao afirmar que "as proibições de prova constituem um limite à descoberta da verdade enquanto as regras de produção de prova visam disciplinar os processos e modos de a alcançar"[444].

---

[441] BARBOSA, Caroline Ap. Sales***, ob. cit***.
[442] Cfr., o nº 1 do art. 156 do CPP.
[443] Cfr., art, 65, no seu nº 3 da CRM
[444] RIBEIRO, Maria da Conceição Fernandes, ***ob. cit***. p.43.

3.3.5.2. Princípio da Livre Apreciação da Prova

Este princípio está consagrado no art. 157 do CPP, segundo o qual, a prova[445] "é apreciada segundo as regras da experiência e a livre convicção da entidade competente, excepto quando há disposição legal em sentido diferente, tal como acontece na prova pericial, segundo o art. 185º do CPP: "A prova pericial tem lugar quando a percepção ou a apreciação dos factos exigirem especiais conhecimentos técnicos, científicos ou artísticos.

A liberdade a que se refere neste artigo, como ensina Castanheira Neves, "não é, nem deve implicar nunca o arbítrio, ou sequer a decisão irracional, puramente impressionista, emocional que se furte, num incondicional subjectivismo, à fundamentação e à comunicação"[446]. A prova surge como fundamento e limite da actividade jurisdicional, fundamento que sem a produção e constatação da mesma não haveria decisão quer condenatória quer absolutória e limite porque o julgador não pode decidir pela condenação sem prova ou contra a prova produzida. Neste contexto, surgem, contudo, limitações a este princípio da livre apreciação da prova, dado o valor probatório atribuído à prova pericial, aos documentos autênticos e autenticados e ao valor do caso julgado[447].

Uma nota importante a reter é que a prova pericial é dos meios probatórios mais utilizados na recolha de prova dos crimes informáticos, na medida em que tem lugar quando a percepção ou apreciação dos factos exigirem especiais conhecimentos técnicos, científicos ou artísticos.

A manifestação deste princípio pode encontrar no art. 198 do CPP, dispondo que " o juízo técnico, científico ou artístico inerente à prova pericial presume-se subtraído à livre apreciação do julgador (nº1). Ainda na mesma norma, sempre que a convicção do julgador divergir ao juízo contido no parecer dos peritos, deve-se aquele fundamentar a divergência (nº 2).

Segundo este princípio o julgador é livre, ao apreciar as provas, embora tal apreciação seja vinculada aos princípios em que se consubstancia nos conceitos e normas que norteiam o

---

[445] "Este modo de valoração da prova resulta da Revolução Francesa de 1789, e a sua implementação deve-se essencialmente à instituição do tribunal de juri, onde aos jurados era permitido uma garantia de imparcialidade face às decisões proferidas pelos magistrados, que julgavam de acordo com as leis emadas pelo monarca "Entendia-se que o critério último da verdade residia na íntima convicção dos jurados, que, despojados das "amarras" legalmente impostas pelo legislador em sede de valoração da prova, assentavam aquela convicção na força da razão, e não na vontade, em última instância, do soberano." Atente-se que deixar nas mãos dos jurados a valoração da prova aumenta a probabilidade de cometimento de erro judiciário". NEVES, Rosa Vieira, A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção (na Decisão Final Penal), Coimbra Editora, 2011, apud cit. RIBEIRO, Maria da Conceição Fernandes, p.43.

[446] ibidem, .p.44.

[447] Ibidem,p.44.

profissional de direito na interpretação das regras inerentes às provas e as normas da experiência comum, da lógica, regras de natureza técnica, científica ou artística, que se devem incluir no âmbito da regulação dos meios de prova, do procedimento probatório e do convencimento judicial a respeito das alegações susceptíveis de prova no processo.

3.3.5.3. Princípio da Verdade Material

Segundo o princípio da investigação ou da verdade material, o tribunal não está limitado pela prova dos factos feitos pela acusação e defesa, pois tem o poder/dever de investigação oficiosa. "Definido o objecto do processo pela acusação e delimitado consequentemente o objecto do julgamento, o tribunal deve procurar a reconstrução histórica dos factos, deve procurar por todos os meios processualmente admissíveis alcançar a verdade histórica, independentemente ou para além da contribuição da acusação e da defesa; contrariamente ao que sucede no processo civil, não existe ónus da prova em processo penal. O tribunal pode e deve ordenar oficiosamente toda a produção de prova que entenda por necessária ou conveniente para a descoberta da verdade."[448].

Como corolários deste princípio, temos o **princípio *in dubio pro reo* e o princípio da imediação**. Segundo o primeiro (*in dubio pro reo),* havendo dúvida, quanto à matéria probatória, a decisão deve ser a mais favorável ao arguido, concretizando assim o princípio da presunção da inocência, o Juiz não pode abster-se de decidir ("non liquet") e as consequências de não se conseguir provar devem ser sofridas por quem tinha obrigação de fazer prova, o Ministério Público e subsidiariamente o Juiz.

No que toca ao princípio da imediação, é-lhe atribuído dois sentidos: "o primeiro consiste na utilização dos meios de prova originais; o segundo pressupõe a oralidade do processo, concretiza-se na relação de proximidade comunicante entre o tribunal e os participantes no processo de modo a existir uma percepção do material (probatório) que levará à decisão. O Princípio da Contraditoriedade certifica-se na estruturação da audiência de julgamento, compreende um debate ou discussão entre a acusação e a defesa, onde são apresentadas as razões de facto e de direito, as provas e é questionado o valor das mesmas, ficando excluída a possibilidade de condenação com base em elementos de prova que não tenham sido discutidos em audiência"[449].

---

[448] RIBEIRO, Maria da Conceição Fernandes, ***ob. cit.***.p.44.

[449] RIBEIRO, Maria da Conceição Fernandes, ***ob. ct.*** .p.46.

Parece-nos importante aludirmos ao princípio "nemo tenetur[450]", como elucida Lara Pinto, no levantamento da questão sobre:

> "se seria admissível a revelação coactiva da password para desencriptação de dados *obtidos em buscas ao domicílio, mas estando os discos rígidos cifrados - teriam os arguidos que entregar as passwords dos computadores apreendidos*[451]? Esta questão surgiu num acórdão inglês[452], onde o tribunal *ad quem* entendeu que sendo os dados cifrados incriminatórios, e o acesso a esses dados dependa da revelação da *password*, então esse conhecimento poderá ser incriminatório. Entendeu ser um caso de possível aplicação do privilégio contra a auto-incriminação, mas como este admite excepções legais, o tribunal invocou o princípio da proporcionalidade, e estando os dados na posse da polícia de forma legal, a revelação da *password* é uma medida proporcional, levando a uma pena de prisão de dois anos a sua não revelação"[453].

Relativamente ao ordenamento jurídico Português, Figueiredo Dias e Costa Andrade alegam ser importante reparar que:

> "não obstante, o princípio *nemo tenetur*, na vertente de direito ao silêncio do arguido, seja na sua dimensão de privilégio contra uma auto-incriminação, não esta consagrado expressamente na Constituição da República Portuguesa, a doutrina e a jurisprudência são unânimes quanto à vigência desse princípio no nosso direito processual penal, ainda quanto à sua natureza constitucional. Desde logo, pela consagração jurídico-constitucional de valores ou direitos fundamentais como a dignidade humana, a liberdade de acção, e a presunção da inocência"[454].

Ainda na mesma senda, a lei processual penal portuguesa, contém normas que asseguram esse princípio, tais como o direito ao silêncio do arguido (artigo 343.º, n.º1, artigo 345.º, n.º1), assim como o dever de esclarecimento ou advertência sobre os direitos decorrentes daquele princípio. No âmbito dos questionamentos anteriormente levados, Sofia Pinto teceu as seguintes conclusões:

> "Já no que toca ao enquadramento deste caso face ao Direito Português, podemos afirmar que estamos no âmbito de aplicação do direito ao silêncio (artigo61.º/1, d) CPP, em virtude de estarmos perante uma declaração do arguido (a revelação da password) que é incriminatória (como resulta do exposto). Ora, no panorama legal português, não há uma previsão legal no sentido de estabelecer uma excepção ao princípio nemo tenetur (direito ao silêncio), ao contrário do que se passa na lei inglesa. Daqui decorre que não será exigível a revelação da password (porquanto constitui uma declaração incriminatória), sob pena de violação do estatuto processual do arguido. Conclui-se, pois, que não é exigível a colaboração do arguido neste caso (i.e. não tem

---

[450] "*nemo tenetur principle: " In criminal law, self- incrimination is the act of exposing oneself generally, by making a statement, "to an accusation or change of crime; to involve oneself or nother person in a criminal prosecution the ganger thereof*". Traduzido de Inglês: No direito penal, auto incriminação é o acto de expor-se geralmente, por meio de declaração, "a uma acusação ou acusação de crime; envolver-se ou outra pessoa em um processo criminal ou no perigo do mesmo".

[451] Nesta análise seguimos de perto o estudo de: PINTO, Lara Sofia, Privilégio contra a auto-incriminação versus colaboração do arguido, in PROVA CRIMINAL E DIREITO DE DEFESA, estudos sobre teoria da prova e garantias de defesa em processo penal, Reimpressão, coord. Teresa Pizarro Beleza e Frederico de Lacerda da Costa Pinto, Almedina, Coimbra, 2011, ISBN 978-972-40-4090-5, pp.91-116. Apud RIBEIRO, Maria da Conceição Fernandes. ob. cit. p.46.

[452] Ibidem, p.46.

[453] Ibidem, p.46.

[454] Ibidem, p.46.

de revelar a password de desencriptação) na medida em que não existe uma disposição legal que imponha essa colaboração em concreto"16 artigos 58.º, n.º2, 61.º, n.º1, alínea h), 141.º, n.º4, alínea a))[455] .

Tendo em atenção ao discurso sobre o princípio *nemo tenetur*, no âmbito do direito processual penal português, ilidimos que o direito ao silêncio do arguido, não está consagrado, expressamente, na nossa Constituição da República. Porém, implicitamente, podemos aferir a sua consagração jurídico-constitucional de valores ou direitos fundamentais como a dignidade humana[456], a liberdade de acção e a presunção da inocência[457].

3.3.5.4. Princípio do Contraditório

O princípio do contraditório está previsto no art. 5 do CPP, e o processo penal subordina-se a esse princípio. No nosso entendimento, o princípio do contraditório pretende estabelecer um equilíbrio da pretensão punitiva do Estado com a presunção de inocência do acusado. Isto demonstra que, por força da lei, para cada alegação feita por uma das partes, existe o direito de manifestação da parte contrária sobre o facto ou a prova apresentada.

O contraditório configura-se como o princípio-garantia[458] do devido processo legal. Porém, o contraditório e a ampla defesa estão umbilicalmente ligados e acabam confundindo-se. Aquele não seria senão a exteriorização desta. Como lecciona Frederico Marques, "ciência bilateral dos actos e termos processuais e possibilidade de contrariá-los, impõe o contraditório que se dê às partes ocasião e possibilidade de intervirem no processo, de modo especial, para cada qual exteriorizar seu pensamento em face das alegações do adversário. Ora, tudo isso está implícito nos meios e recursos essenciais ao direito de defesa"[459].

Em verdade, em conformidade com Grinover et al, é do contraditório (visto em seu primeiro momento, da informação, que se materializa na citação do réu) que brota o exercício da defesa; mas é esta o correlato ao de acção – que garante o contraditório. "A defesa, assim, garante o contraditório, mas também por este se manifesta e é garantida. Eis a íntima relação e interacção da defesa e do contraditório"[460] .

"O contraditório", escreve Silva, "impõe a conduta dialéctica do processo. Isso significa dizer que em todos os actos processuais às partes deve ser assegurado o direito de participar,

[455] RIBEIRO, Maria da Conceição Fernandes. ***ob. cit***. p.47.
[456] Cfr., art. 40 da CRM.
[457] Cfr., art. 59 da CRM; art. 3 do CPP.
[458] Cfr., os arts 62 e 65 da CRM.
[459] CAGLIARI, José Franciscol, ***ob. cit.***
[460] ibidem.

em igualdade de condições, oferecendo alegações e provas, de sorte que se chegue à verdade processual com equilíbrio, evitando-se uma verdade produzida unilateralmente"[461]. E, por ampla defesa, deve se entender, prossegue o ilustre Professor, como "o asseguramento que é feito ao réu de condições que lhe possibilitem trazer para o processo todos os elementos tendentes a esclarecer a verdade. Com efeito, é por isso que ela assume múltiplas direcções: ora traduzir-se-á na inquirição de testemunhas, ora na designação de defensor dativo, não importando, assim, as diversas modalidades, em primeiro momento. É por isso que a defesa ganha um carácter necessariamente contraditório. É pela afirmação e negação sucessivas que a verdade irá se insurgindo nos autos. Nada poderá ter valor inquestionável ou irrebatável. A tudo terá de ser assegurado o direito de contra agir processualmente, contraditar, contradizer e contraproduzir"[462].

Disso, presume-se que a defesa, vista como exteriorização do contraditório, mas também por ele garantida, não deve ser concebida apenas no sentido negativo de oposição ou resistência à pretensão do autor (*in casu do Estado, titular do jus puniendi)*, senão também, e principalmente, deve ela ser entendida em sua dimensão positiva, como o direito de participar, influenciar, incidir activamente sobre o desenvolvimento do processo, objectivando o seu resultado. Nessa ordem de ideias, insere-se, entre os recursos e meios inerentes à ampla defesa, o direito à prova, e que também é assegurado ao Estado, enquanto litigante, a quem se também confere o direito ao contraditório. Por isso, salientam Grinover, Scarance e Gomes Filho "o direito à prova como aspecto de particular importância no quadro do contraditório, uma vez que a actividade probatória representa o momento central do processo: estritamente ligada à alegação e à indicação dos factos visa ela a possibilitar a demonstração da verdade, revestindo-se de particular relevância para o conteúdo do provimento jurisdicional. O concreto exercício da acção e da defesa fica essencialmente subordinado à efectiva possibilidade de se representar ao juiz a realidade do facto posto como fundamento das pretensões das partes, ou seja, de estas poderem servir-se das provas"[463].

Assim, do parafraseado, entendemos que o direito à prova é decorrente do contraditório, um dos meios por que este se manifesta. Contudo, se o direito à prova é decorrente do contraditório, não se deve descurar que o contraditório exerce, por outro lado, limitações à formação e produção das provas, que são resumidas por Grinover et al:

> "a) proibição de utilização de fatos que não tenham sido previamente introduzidos pelo juiz no processo e submetidos a debate pelas partes; b) proibição de utilização de

[461]CAGLIARI, José Franciscol, ***ob. cit***.
[462] Ibidem.
[463] ibidem.

> provas formadas fora do processo, ou de qualquer modo colhidas na ausência das partes; c) obrigação do juiz, quando determine a realização de provas ex officio, de submetê-las ao contraditório das partes, que devem ainda participar de sua produção e ter oportunidade de oferecer contraprova. Em suma, como sintetizam os autores, "tanto será viciada a prova que for colhida sem a presença do juiz, como o será a prova colhida pelo juiz, sem a presença das partes" (...) "A concomitante presença de ambos – juiz e partes – na produção das provas é essencial à sua validade"[464].

3.3.5.5. Princípio da Publicidade

O Princípio da Publicidade, previsto no 2 do art. 60º da Constituição da República de Moçambique, observa que "As audiências de julgamento em processo criminal são públicas, salvo quando a salvaguarda da intimidade pessoal, familiar, social ou da moral, ou ponderosas razões de segurança da audiência ou de ordem pública aconselharem a exclusão ou restrição de publicidade". O Direito Processual Penal acomoda este princípio no art. 365 do CPP, ao preceituar que "A audiência do julgamento é pública, sob pena de nulidade insanável, salvo nos casos em que o juiz da causa decidi a exclusão ou a restrição da publicidade" (nº 1). Ademais, "a decisão de exclusão ou de restrição da publicidade é, sempre que possível, precedida de audição contraditória dos sujeitos processuais interessados". (nº 3).

O alcance do princípio constitucional da publicidade assenta na predisposição de que os actos processuais devem ser realizados de forma pública, ou seja, sem sigilo ou segredo, como forma de permitir o controlo social dos actos e das decisões do Poder Judiciário.

Desse modo, a publicidade fica restrita apenas em situações excepcionais, como o interesse social e a preservação da intimidade. Diante desses casos, o juiz pode limitar o acesso aos autos e a prática de actos processuais, desde que a sua decisão seja fundamentada.

Na alvorada doutrinal, há um entendimento segundo o qual a publicidade "pode ser dividida em geral e específica. A publicidade geral é o acesso aos actos e autos do processo a qualquer pessoa. A publicidade específica diz respeito ao acesso restrito aos actos e autos processuais às partes envolvidas (representante do MP, advogado de acusação e o defensor) "[465]. Portanto, o que se pode restringir é apenas a publicidade geral

3.3.5.6. Princípio da Não Auto-incriminação

O Princípio da Não Auto-incriminação, ou *nemo tenetur se detegere*, significa que ninguém é obrigado a produzir provas contra si mesmo. Este princípio consiste, de forma geral,

---

[464] CAGLIARI, José Franciscol, ***ob. cit***.

[465] BARBOSA, Caroline Ap. Sales, ***Teoria Geral da Prova no Direito Processual penal Brasileiro***. Disponível no https://www.jusbrasil.com.br/artigos/teoria-geral-da-prova-no-direito-processual-penal-brasileiro/337514638, acessado no dia 30 de Dezembro de 2023.

na proibição de uso de qualquer medida de coerção ou intimidação ao acusado, para obtenção de uma confissão ou para que colabore com actos que possam ocasionar sua incriminação. É o que observa a norma constitucional prevista no nº 3 do art. 65, quando observa que "São nulas todas as provas obtidas mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão na sua vida privada e familiar, no domicílio, na correspondência ou nas telecomunicações". Também podemos observar a manifestação do "Principio da Não Auto-incriminação" no art. 156 do CPP. " São nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coacção ou, em geral, ofensa da integridade física ou moral das pessoas" (nº 2); "São ofensivas da integridade física ou moral das pessoas as provas obtidas, mesmo com consentimento delas, mediante: perturbação da liberdade de vontade ou de decisão através de maus-tratos, ofensas corporais, administração de meios de qualquer natureza, hipnose ou utilização de meios cruéis ou enganosos (al. a) do nº 3); Perturbação, por qualquer meio, da capacidade de memória ou de avaliação ((al. b) do nº 3); Utilização da força, fora dos casos e limites permitidos por lei (al. c) do nº 3); A ameaça com medida legalmente inadmissível e, bem assim, com denegação ou condicionamento da obtenção de benefício legalmente previsto ((al. d) do nº 3); Promessa de vantagem legalmente inadmissível (al. e) do nº 3); são igualmente nulas as provas obtidas mediante intromissão na vida privada no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respectivo titular (nº 4); se o uso dos métodos de obtenção de provas previstos neste artigo constituir crime, podem aquelas ser utilizadas com o fim exclusivo de proceder contra os agentes do mesmo (nº 5).

Este princípio é de extrema importância, já que está previsto no Pacto Internacional dos Direitos Civis e Políticos[466] bem como na Convenção Americana sobre Direitos humanos[467].

3.3.6. Meios de Obtenção de Prova nos Crimes Cibernéticos

Os crimes cibernéticos são voláteis e a sua massificação ocorre com a globalização, onde os agentes deste tipo de criminalidade conseguem adaptar-se e cometer os ilícitos mais facilmente, tornando-se difícil para os sistemas formais de controlo, acompanharem o ritmo dessa criminalidade, uma vez que a investigação encontra limitações de natureza processual, na salvaguarda de direitos fundamentais.

[466] cfr., al. g) do art. 14.3, do Pacto Internacional dos Direitos Civis e Políticos (PIDCP).
[467] Cfr., § 2º, "g", art. 8 da Convenção Americana sobre Direitos Humanos (CADH).

Devido à ausência de uma legislação no nosso ordenamento jurídico, não existe uma definição legalmente formalizada sobre provas digitais. O mesmo cenário ocorre a nível da doutrina em que não existem ainda muitas definições de prova digital. Porém, trazemos algumas s definições distintas: Por exemplo, Rodrigues define prova electrónico-digital "como qualquer tipo de informação, com valor probatório, armazenada [em repositório electrónico-digitais de armazenamento] ou transmitida [em sistemas de redes informáticas ou rede de comunicações electrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital"[468]. Na mesma senda, Ramos define esta prova "como sendo toda a informação passível de ser obtida ou extraída de um dispositivo electrónico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta"[469]. No nosso entendimento esta definição de Ramos é mais clara que a de Rodirgues, tendo em atenção que estamos perante um delito virtual.

Ainda na senda conceptual sobre provas e os meios de sua obtenção, Albuquerque[470] distingue-os do seguinte modo: "Os meios de obtenção de prova visam a detecção de indícios da prática do crime, constituindo um meio de aquisição para o processo de uma prova pré-existente" e, em regra, contemporânea ou preparatória do crime. Os meios de prova formam-se no momento da sua própria produção no processo, visando a "reprodução" ("avaliação") do facto e, nessa medida, constituindo um meio de aquisição para o processo de uma prova "posterior" à prática do crime".

Para Miranda, meios de prova são "as fontes probantes, os meios pelos quais o juiz recebe os elementos ou motivos de prova: os documentos, as testemunhas, os depoimentos das partes. Elementos ou motivos de prova são, por um lado, os informes sobre factos ou julgamentos sobre eles, que derivam do emprego daqueles meios."[471]. Por outro lado, Grinove et al, distinguindo entre fontes e meios de prova, ensinando que fontes de prova são "os factos percebidos pelo juiz" e meios de prova "são os instrumentos pelos quais os mesmos se fixam em juízo"[472]. Já os elementos de prova, conforme o magistério de Manzini, são "todos os factos ou circunstâncias em que repousa a convicção do juiz"[473]."Meios de prova", Greco Filho

[468] RIBEIRO, Maria da Conceição Fernandes***, ob. cit***. p.48.
[469] Ibidem, p.48.
[470] Ibidem, p.41.
[471] CAGLIARI, José Franciscol, ***ob. cit.***
[472]ibidem.
[473] ibidem**.**

conceptual como sendo "os instrumentos pessoais ou materiais aptos a trazer ao processo a convicção da existência ou inexistência de um facto"[474].

O Código de Processo Penal Brasileiro (CPPB) especifica vários meios de prova (arts. 158 a 250), que constituem os chamados meios legais de prova. A enumeração, entretanto, não é taxativa. Outros meios de prova admitem-se, desde que compatíveis com os princípios de respeito ao direito de defesa e à dignidade da pessoa humana – são as provas inominadas, na expressão de Carnelutti[475].

Em conformidade com Rosa Neves, a prova nem sempre foi obtida e valorada pelos tribunais como é hoje. Começou com o sistema inquisitório, passando para o modelo processual penal de estrutura acusatória integrado pelo princípio da investigação. "O sistema inquisitório tinha como objectivo satisfazer os interesses do Estado na tarefa de punir, reunindo numa só pessoa, o Juiz, as funções de investigar, acusar e de julgar. Tinha natureza secreta para que não ocorresse o desaparecimento das provas e eram admitidos todos os meios probatórios, incluindo a tortura[476].

Por seu turno, no sistema acusatório, diz a autora que "o indivíduo é parte no processo, sendo-lhe reconhecidos direitos, é um verdadeiro processo de partes, sendo estas que acarretam os elementos probatórios ao processo, onde ao Juiz incumbe dirigir o processo e decidir"[477]. O modelo acusatório consiste essencialmente na separação entre a entidade que acusa e a entidade que julga[478].

A autora aborda-nos o sistema misto ou ecléctico, segundo o qual procurou concretizar vantagens dos dois sistemas, sendo o processo dividido em duas partes:

> "a fase de instrução, destinada a investigar o crime e os seus agentes, era dirigida por um magistrado especializado; a iniciativa e a titularidade da acção penal encontrava-se nas mãos de um oficial do poder executivo junto do poder judicial. A instrução era escrita, secreta e não contraditória. A fase de julgamento destinada a apreciação e valoração da prova estava organizada segundo o modelo acusatório, prevalecia a oralidade, e a publicidade da audiência de julgamento[479].

Como aponta, Rosa Neves[480], "o sistema ecléctico funda-se na relação dialéctica decorrente da necessidade sentida pela comunidade de perseguir os culpados pelos crimes cometidos - incumbindo ao Estado a tarefa pública de exercer o seu ius puniendi - mas, em cada caso concreto, assegura-se ao arguido a possibilidade de exercer os seus direitos de defesa,

---

[474] CAGLIARI, José Francisco, ***ob. cit.***.
[475] Ibidem.
[476] RIBEIRO, Maria da Conceição Fernandes, ***ob. cit***. p.39.
[477] Ibidem, p. 39.
[478] Ibidem, p.39.
[479] Ibidem, p.39.
[480] Ibidem, p.40.

evitando-se os perigos decorrentes de uma real aniquilação da condição humana (do arguido) em prol da busca, levada ao extremo no sistema inquisitório, da descoberta da verdade material".

Fazendo um recuo para a história processual, frisamos que o Código de Processo Penal de 1929, a instrução era da competência de um juiz, cabendo ao Ministério Público (doravante designado por MP) apenas promover as diligências concretas de instrução (artigo 35.º). Com o Decreto-Lei n.º 35.007, introduziram-se profundas alterações na instrução, havia uma fase de instrução preparatória da competência do MP, que visava a descoberta dos indícios da existência do crime e do seu agente. Havia ainda depois desta fase, uma de instrução contraditória da competência do Juiz, obrigatória nos processos de querela. Neste caso, devia o MP requerer a instrução contraditória no mesmo acto em que deduzia acusação. "Este Decreto-Lei, preparado por Cavaleiro Ferreira mediante atribuição da instrução preparatória ao MP, que se adoptou o princípio do acusatório[481].

O modelo processual é de estrutura acusatória[482] integrada por um princípio da investigação[483], pois a entidade que acusa e define o objecto do julgamento é diferente da que julga, havendo também contribuição por parte da acusação e da defesa. O tribunal pode ordenar oficiosamente todos os meios de prova cujo conhecimento lhe afigure necessário à descoberta da verdade e à boa decisão da causa" (não há um verdadeiro ónus da prova)[484], faculdade esta que permite que a todo tempo se faça junção de documentos requerida pelas partes, sem que haja necessidade de alegar e provar a impossibilidade de os juntar no decurso do inquérito ou da instrução[485] na procura da verdade material, acentuando que "não valem em julgamento, nomeadamente para o efeito de formação da convicção do tribunal, quaisquer provas que não tiverem sido produzidas ou examinadas em audiência"[486].

A produção de provas constitui uma fase crucial para a descoberta da verdade material e a boa decisão da causa, daí a necessidade de uso de métodos e técnicas previstas na legislação do ordenamento jurídico moçambicano, para a sua validação no acto do julgamento. E é por

---

481 RIBEIRO, Maria da Conceição Fernandes, ***ob. cit.*** p.41.

482 Relativamente aos modelos: ***"Enquanto o inquisitório exprime uma confiança na bondade do poder e na sua capacidade de alcançar a verdade, o acusatória deriva de uma desconfiança no poder enquanto fonte autónoma da verdade".*** RIBEIRO,…..ibidem. p.41.

483 O Processo Penal subordina-se ao Princípio do Contraditório (Cfr., o art. 5 do CPP)

484 Nas palavras de Fernando Gonçalves e Manuel João alves, "Num puro sistema acusatório conjugado com o princípio da inocência, a acusação tem o ónus de provar os factos que imputa ao arguido. Se o não conseguir, nem por isso a defesa tem qualquer ónus de provar a inocência para que a absolvição surja." in A prova do crime, meios legais para a sua obtenção, p. 146). Apud RIBEIRO, Maria da Conceição Fernandes. ibidem, p.41.

485 ibidem p.41.

486 Cfr., art. 357 do CPP.

meio de provas que o Ministério público procura convencer ao juiz sobre o cometimento de crime por parte do arguido. E, por sua vez, usando das provas a sua disposição o arguido ou o seu representante legal demonstra que não cometeu crime algum, solicitando ao juiz a sua absolvição.

A produção de provas envolve os factos documentados por meio de um processo complexo de busca da verdade baseado na investigação criminal, assim como das declarações do arguido desde o primeiro interrogatório até em sede do julgamento. Em todo caso, António Coelho[487] aconselha sempre que possível, aquelas declarações tenham, à sua volta, já outros elementos probatórios em relação aos quais, sempre que tal não prejudique a investigação em curso, possa ser chamada a atenção do arguido ou com que este possa ser confrontado (por ex., documentos e objectos encontrados e/ou apreendidos que se considere terem ligação com os factos, depoimentos de outras pessoas já ouvidas nos autos, relatórios de pura observação policial, relatórios de perícia, etc…).

Deste modo, ter-se-á mais "substância" para o interrogatório e poder-se-á alcançar uma melhor conformação entre as primeiras declarações aí prestadas e os factos sobre que versam, podendo com mais êxito elucidar-se do papel do arguido ou arguidos nos factos, o que poderá relevar decisivamente em audiência de julgamento nos termos sobreditos.

Os meios de obtenção de prova são todos os instrumentos de que se servem as autoridades judiciárias para investigarem e recolherem os meios de prova. Na perspectiva técnico-operativa, Germano Silva[488] afirma que os meios de obtenção de prova caracterizam-se pelo modo e também pelo momento da sua aquisição no processo, em regra nas fases preliminares.

Importa referir que os praticantes dos crimes cibernéticos são indivíduos que tempo após tempo sofisticam as suas formas de actuação, procurando assim dificultar o seu alcance por parte das pessoas lesadas assim como das autoridades judiciais. Este facto coloca os órgãos da Administração da Justiça num desafio permanente, o que se deve traduzir na melhoria qualitativa dos meios técnicos e materiais para que estejam a altura das sofisticações dos criminosos de modo a conseguir esclarecer os delitos digitais.

O nosso ordenamento jurídico já predispõe dos meios de obtenção da prova como instrumentos usados pelas autoridades judiciárias com a finalidade de investigar e recolher os

[487]COELHO, António Manuel Mendes, ***Meios de prova e meios de obtenção de prova***, Fórum de Investigação Criminal, organizado pelo Comando de Polícia de Aveiro da PSP a 26 de Outubro de 2006, no Centro Multimeios de Espinho. In Revista Verbo Jurídico, disponível em .www.verbojuridico.pt/.eu/.net/.org/.com. Acesso a 14 de Dezembro de 2023.

[488]SILVA, Germano M***, Curso de Processo Penal***, 5ª edição revista e actualizada, Editorial, Lisboa, Vol. II, 2011.

meios de prova. O objectivo desses meios, circunscrevem – se na obtenção da prova em si. Aferir que esses meios de obtenção da prova não são aplicados para convencer o juiz, mas apenas, um caminho para se chegar a prova. Nesse corolário, temos os seguintes meios de obtenção da prova, em conforme configura o CPP:

1. Os exames, "realizados em pessoas, lugares das coisas, inspecção dos vestígios que possa ter deixado o crime e todos os indícios relativos ao modo como e lugar onde foi praticado, as pessoas que o cometeram ou sobre as quais foi cometido" (art. 206.º e ss.);

2. Revistas e buscas, nos casos em que haja indícios de que alguém oculta na sua pessoa quaisquer objectos relacionados com um crime ou que possa servir de prova (art. 209.º e ss.);

3. As apreensões dos objectos que tiverem servido ou estivessem destinados a servir a prática de um crime (art. 213.º e ss.)

4. A escuta, considerado meio especial de obtenção da prova, "consiste na intercepção e a gravação de conversas ou comunicações telefónicas, acto coordenado ou autorizado por despacho do juiz competente…" (art. 222 e ss). Nisso, aquele que interceder as comunicações sem que para tal seja autorizado (…), comete a infracção de intercepção ilegal das comunicações (…)", punível nos termos do art. 64.º da Lei n.º 8/2004, de 21 de Julho (Lei das Telecomunicações).

Neste contexto, Coelho[489] refere que, sendo a escuta telefónica um meio de obtenção de prova, o elemento probatório obtido é, pois, o conteúdo, o teor, da conversa escutada naquilo que tal conteúdo tenha de indiciação sobre a prática do crime, sendo sempre desejável que este se articule com outros meios de prova. Nessa perspectiva, a produção de provas, a semelhança de qualquer legislação, exige para a sua validação legal, o respeito de um longo processo, procedimentos complexos envolvendo pessoas e meios, devidamente credenciados, visto tratar – se de um crime com uma natureza muita complexa. Nisso, vale ressaltar que para a produção de provas nos crimes cibernéticos exige toda uma acção coordenada e conjunta para todos os intervenientes no processo investigativo. Nesse corolário, Inês Pillar[490] acentua que "a investigação criminal não actua isoladamente, consiste numa gestão em que o agente ou órgão de polícia criminal e a acção, por um lado, são intencionados, ou seja, por um lado, "o agente não está limitado a uma determinada categoria funcional", por outro lado, consideramos um conjunto de "pessoas em situação de trabalho com outras pessoas, independentemente da

[489]COELHO, António Manuel Mendes, *ob. cit.*

[490] ARRONE, Ilídio Samuel, ***a investigação criminal em Moçambique: gestão e cadeia de custódia da prova***, Lisboa, 2018.

hierarquia ou atribuições, sem deixar de reconhecer as particularidades de cada situação funcional, articuladas à cada singularidade de cada agente.

Assim sendo, é necessário o cultivo duma cultura organizacional de registo histórico, sequencial e permanente de todas as actividades realizadas com a matéria probatória, registo de todos os intervenientes que dela hajam tido contacto e a catalogação de todo o processo espácio-temporal que essa evidência venha a ser sujeita, desde o local onde foi identificada e recolhida, até o seu destino final.

3.3.6.1. Acções Encobertas, Previstas no art. 226 do CPP

As acções encobertas "são aquelas que são desenvolvidas por funcionários de investigação criminal ou por terceiro actuando sob o controlo do Serviço Nacional de Investigação Criminal para a prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade". Este meio de obtenção de provas está previsto no art. 226º do CPP. Olhando pelos pressupostos definidos pela própria lei (art. 228 do CPP), "As acções descobertas devem ser adequadas aos fins de prevenção e repressão criminais identificados em concreto, nomeadamente a descoberta de material probatório… do crime em investigação" (nº 1), ilidimos que o agente encoberto terá, com toda a certeza, um importante papel no contributo da investigação criminal. Porém, na intervenção encoberta em sistemas informáticos, o legislador não criou uma norma processual específica para esta nova forma de investigação, nem procedeu à sua regulamentação sobre os meios técnicos a utilizar.

Em matéria de regime de prova, (1) princípio da legalidade; (2) princípio da livre apreciação da prova; (3) princípio da verdade material, com suas subdivisões (princípio da presunção de inocência ou do *in dúbio pro* réu; e o princípio de imediação; (4) o princípio do contraditório; (5) princípio da publicidade e (6) princípio da não auto-incriminação, posteriormente serão matéria de análise nesta abordagem, para a sua preservação, exigem, da investigação criminal, no campo cibernético, o recurso à ciência e ao método científico. Para dar azo a esse argumento, ressalta-nos recorrer a normal prevista no art. 185 do nosso CPP que preceitua que "a prova pericial tem lugar quando a percepção ou apreciação dos factos exigirem especiais conhecimentos técnicos, científicos ou artísticos". Está patente no dispositivo em referência, uma nota importante que a prova pericial é dos meios probatórios mais utilizados na recolha de prova dos crimes informáticos, tendo em atenção a especificidade dos contornos do próprio crime. Por isso, ocupar-nos-emos em seguinte dos contornos funcionais da perícia, nos crimes cibernéticos.

3.3.6.2. Perícia de Informática nos Crimes Cibernéticos

Nos processos criminais de natureza cibernética, é de suma importância a realização de exames periciais nos vestígios deixados por infracções, consequentemente, a elaboração dos laudos assinados por peritos oficiais. O nosso CPP não define taxativamente quem são os peritos. Porém, fazendo um respaldo pelo capítulo VI (da prova pericial) prevista nos termos do art. 185 a 198), somos de entendimento que os peritos são todos os que tem conhecimentos técnicos, científicos ou artísticos nas áreas que exige a percepção ou apreciação dos factos, para o apuramento da verdade material. Nisso, são peritos, consultores técnicos (art. 189 do CPP), médico-legista e psiquiatra (art. 193 do CPP), criminologista, psicólogo, sociólogo e psiquiatra (nº 2 do art. 195 do CPP). Nesse âmbito, compete aos Serviços de Investigação Criminal (SERNIC) coadjuvar as autoridades judiciárias na realização das finalidades do processo, auxiliando os serviços dos peritos (art. 61 do CPP).

A perícia de informática é importante para praticamente todo tipo de investigação, haja vista a ubiquidade dos computadores. Entretanto, "para aqueles crimes cujos vestígios principais não são digitais, normalmente os vestígios deixados em computadores e mídias de armazenamento não se tornam evidência do crime, mas sim indícios que auxiliam na investigação"[491]. Por exemplo, "em crimes financeiros ou de tráfico de entorpecentes, mensagens de correio electrónico, documentos digitais, entre outros elementos, são analisados pelos policiais dedicados ao caso para trazer informações e factos circunstanciais que orientem o curso da investigação, bem como a obtenção de outros vestígios e, possivelmente, provas"[492]. Ainda na referência do autor, para esses crimes, a perícia de informática realiza uma extracção dos dados dos computadores aplicando filtros objectivos para o contexto desejado.

Como lecciona Carneiro, "pela limitação de efectivo e pelo desconhecimento do perito sobre o assunto, cabe aos policiais da investigação, bem como às partes durante o processo criminal, analisar efectivamente o conteúdo do material questionado"[493].

Em conformidade com Carneiro[494], as investigações de crimes cibernéticos demandam a perícia de informática com vestígios efectivamente deixados pela acção criminosa, onde os computadores contêm arquivos, registos de sistema, entre outras informações, que são

[491] CARNEIRO, Márcio Rodrigo de Freitas, ***Perícia de Informática nos Crimes Cibernéticos,*** pp. 36-37 (33-53). In EMAG- Escola de Magistrados da Justiça Federal da 3ª Região. Caderno de estudos (1- 354) Investigação e prova nos crimes cibernéticos. TRF3, São Paulo 2017.
[492] ibidem.
[493] Ibidem.
[494] Ibidem.

evidências do crime e podem servir de prova material. Nisso, o exame pericial e o laudo produzido servirão de esclarecimento e convencimento para o juízo sobre o conteúdo ilícito, tal como sobre o meio e método utilizados para se cometer o crime denunciado"[495]. O nosso CPC dispõe que "a prova pericial pode consistir em exame, vistoria ou avaliação" (nº 1 do art. 568). E no seu nº 2 diz que "Os exames e vistoria têm por fim a averiguação, feita por peritos, de factos que tenham deixado vestígios ou sejam susceptíveis de inspecção ou exame ocular: se a averiguação recai sobre coisas móveis ou pessoas, diz-se exame; se recai sobre imóveis, tem o nome de vistoria".

Partindo do pressuposto das leis plasmados na norma do art. 568 do CPC, podemos aludir que trata-se de um tipo ou meio de prova material que exige muito da ética de investigação criminal, particularmente por ser bastante sensível e pela necessidade de garantir a integridade da prova.

Ressalta-nos aludir que no contexto dos crimes cibernéticos, as evidências digitais que são essenciais para a comprovação da materialidade do crime, assim como, se possível, sua autoria, podem ser encontrados nos Computadores, onde são arquivados vestígios digitais e outros tipos de dados que podem sustentar ou refutar um determinado crime, ou ainda apenas fornecer suporte para uma investigação.

No percurso de uma investigação de crime cibernético, após a identificação do endereço do imóvel do qual partiram os acessos à Internet identificados como acção criminosa, ou mesmo após a identificação de localidades por outras maneiras, diz o Carneiro[496] que "cumprem-se os mandados de busca e apreensão emitidos pelos juízos competentes. O objectivo principal das buscas e apreensões, nesse contexto, é a recolha de vestígios digitais, além de quaisquer outros vestígios que possam esclarecer os factos".

Há um aspecto importante a reter nesse processo: apesar de o cumprimento de mandato de buscas e apreensões será necessário requerer a presença de perito, mesmo que não seja criminal para examinar os vestígios do material apreendido, para a averiguar a verdade material.

Como afirma Carneiro,[497] "em outros tipos de investigações, nas quais os computadores normalmente não contêm evidências digitais de materialidade e/ou autoria, mas sim indícios ou dados correlatos aos factos investigados, a extracção ampla dos dados para posterior análise é a principal demanda à perícia de informática". Já nos crimes cibernéticos, o contrário disso é regra, e espera-se que a perícia traga luz às evidências digitais e a prova material para o processo

[495] CARNEIRO, Márcio Rodrigo de Freitas, ***ob. cit.***.
[496] Ibidem.
[497] Ibidem.

criminal. Nisso, cada tipo de crime cibernético pode trazer desafios específicos ao perito, como mostram os exemplos a seguir:

1. "Clonagem de cartões - Nos computadores e mídias apreendidos no combate à clonagem de cartões, principalmente nos computadores de investigados mais actuantes na obtenção de dados e na utilização dos números clonados, é praxe a pesquisa por expressões que remetam a arquivos contendo dados em formatos típicos, lidos da tarja magnética do cartão. Dependendo do grupo investigado, pode-se pesquisar por programas indevidamente instalados em terminais de transacção electrónica de lojas, ou programas conhecidos como malwares, enviados por e-mail ou outros métodos de mala directa, na tentativa de "infectar" computadores alheios para obtenção de dados bancários. Há, ainda, aplicativos utilizados para gravação e impressão de cartões de tarja magnética. Finalmente, também se podem obter outros indícios importantes para a investigação e o processo criminal, tais como mensagens de correio electrónico, mensagens de comunicação instantânea, histórico do navegador e outros tipos de documentos.
2. Pornografia envolvendo crianças ou adolescentes Nos exames periciais de informática em mídias de armazenamento e computadores apreendidos em locais de busca relacionados a investigações de pornografia infantil, cabe ao perito extrair arquivos que possam conter cenas de nudez ou sexo envolvendo crianças ou adolescentes, além de verificar o compartilhamento dos arquivos e a utilização de aplicativos que permitam transmitir dados pela Internet. O primeiro objectivo do perito é encontrar as imagens e vídeos cujo conteúdo seja claramente ilegal.
3. Aparelhos celulares, smartphones e tablets – esses equipamentos portáteis, utilizados em massa, são na prática computadores compactados na palma da mão, o que mostra que cada vez mais pessoas carregam um aparelho portátil consigo e, portanto, cada vez mais são apreendidas em investigações e procedimentos criminais. Apesar de se tratar de computadores, algumas particularidades nesses itens trazem dificuldades à perícia: a) Comummente, utilizam-se senhas de bloqueio ao aparelho, que por padrão bloqueiam automaticamente em pouco tempo de inactividade do equipamento, impossibilitam o acesso aos dados e não há métodos de quebra conhecidos. Por isso, é importante que a equipe, durante o mandado de busca ou na prisão em flagrante, consiga obter a senha directamente com o proprietário do dispositivo. b) O acesso à mídia de armazenamento interno não é simples e directo como nos computadores e notebooks. As memórias flash internas aos celulares são soldadas ao circuito impresso do aparelho, e todo acesso é limitado à porta USB de comunicação. Utilizando-se de equipamentos dedicados, como o Cellebrite UFED, pode-se realizar a extracção de dados do sistema instalado (a grande maioria, hoje, utiliza sistema Android ou iOS); ou ainda, em alguns casos, realizar o que é chamado de extracção física, que se assemelha ao espelhamento de uma mídia de armazenamento. Posteriormente, esse arquivo extraído poderá ser analisado com o próprio software da Cellebrite ou ainda com o IPED. c) Alguns aplicativos criptografam os dados com chaves armazenadas em áreas especiais do sistema operacional, que só podem ser acessadas alterando o dispositivo, de um modo impossível ao usuário normal, com credenciais de administrador do sistema (vulgo "root", de onde vem a expressão "rootar o aparelho"). Essas condições trazem nova luz aos procedimentos periciais, que anteriormente evitavam a qualquer custo alterações aos vestígios digitais. Dada a quantidade de marcas e modelos disponíveis no mercado, bem como a variedade de configurações tanto dos sistemas instalados como das maneiras de acesso aos dados internos, os equipamentos portáteis constituem enorme desafio aos fabricantes de extractores de dados, bem como à perícia, que, em determinados casos, pode ver esgotadas as alternativas de acesso aos dados, quando certa versão de sistema ou de software não é suportada pelos equipamentos e técnicas forenses disponíveis" [498].

[498] CARNEIRO, Márcio Rodrigo de Freitas, ***ob. ct***.

Ressalta-nos, a partir dos exemplos apresentados na óptica do autor ora citado, dizer que a perícia de informática enfrenta constantemente o problema da demanda excessiva, frente a um diminuto quadro de peritos formados na área. Como prova disso, os procedimentos envolvidos nos exames de informática são extensos e, adicionalmente, mais complexos e demorados quando a análise minuciosa das mídias é imprescindível, como nos casos em que os vestígios digitais são essenciais à comprovação do crime. Outrossim, como se pode ter presente o caso das investigações de crimes cibernéticos, como aqueles envolvendo pornografia infantil, a perícia tem um papel crucial mais ao fim da investigação, com o exame minucioso dos vestígios electrónicos, que trarão as evidências digitais e serão formalizados como prova material, se possível de autoria do delito. São os exames pontuais.

Podemos inferir ainda, que os desafios de novas tecnologias, como os equipamentos portáteis (celulares, smartphones e tablets), em conformidade com o terceiro exemplo apresentado pelo autor podem causar, em certo momento, um estrangulamento na capacidade de atendimento da perícia, caso o poder executivo não proporcione condições materiais e humanas para responder satisfatoriamente à demanda.

A prova pericial representa, em processo penal, um desvio ao princípio da livre apreciação da apreciação da prova, previsto no art. 198 do CPP. Nessa senda, tratando-se de exame de perícia o resultado obtido no mesmo apenas pode ser colocado em crise por outro meio de prova idêntico e nunca pela análise das testemunhas, ou pelas declarações dos arguidos.

3.3.7. A Comprovação da Materialidade do Crime Cibernético

O número de usuários activos em redes sociais "atingiu 4,88 biliões, o que representa 60,6% da população mundial, de acordo com um relatório trimestral sobre a internet. Essa estimativa marca um aumento de 3,7% em relação ao segundo trimestre de 2022"[499]. Isto demonstra que a população mundial está conectada à rede mundial de computadores. Diante desse contingente expressivo de internautas, surgem ao menos duas constatações:

> "A primeira é positiva, pois o número demonstra que a maioria da população possui condições materiais para ingressar na rede e está disposta a enfrentar os desafios do mundo tecnológico para obter informações e facilidades, ou apenas para fins recreativos. A segunda é sombria: na medida em que cresce o número de internautas operando na rede, também cresce a quantidade de infractores que, aproveitando-se das facilidades de um suposto anonimato e fazendo uso de aparatos tecnológicos, buscam obter alguma vantagem ilícita e/ou imoral, de ordem material, psicológica ou emocional, causando prejuízos patrimoniais e morais a outros usuários individuais e

[499] Cfr., no https://gaucha2h.clicrbs.com.br, acessado no dia 3 de Janeiro de 2024.

> a instituições públicas e privadas. Notoriamente, os órgãos estatais incumbidos da repressão à prática de ilícitos penais têm investido recursos humanos e materiais para a adequada apuração deste tipo de delito, criando delegacias especializadas em crimes de informática e grupos especiais de perícia criminal digital, além de firmar convénios com entidades nacionais e internacionais voltadas ao aperfeiçoamento técnico das equipes. Todavia, como é previsível, dada a expansão da tecnologia nos meios sociais, dificilmente se logrará uma resposta estatal rápida e efectiva ao problema da criminalidade digital. Haverá de se incrementarem os mecanismos automáticos de localização e inibição imediata das práticas virtuais ilícitas, de forma a tornar certa a identificação do criminoso e sua persecução penal[500].

Como afirma Roncada, "a par das questões criminológicas, uma vez ocorrida a infracção penal com uso da informática, surge o problema jurídico da sua adequada demonstração, de modo a fornecer aos agentes do Estado a prova dos elementos técnicos vinculados directamente à infracção, de todo indispensável ao início da actividade persecutória"[501]. O autor ora citado, apregoa ainda que "o problema em destaque é designado no foro processual como prova da materialidade delitiva, pressuposto lógico-jurídico indispensável para a afirmação da culpa do acusado, sem o qual não se prossegue no exame prático da subsunção dos factos à norma penal"[502].

Nessa senda, computadores e outros dispositivos digitais armazenam dados que podem sustentar ou refutar um determinado crime, ou ainda apenas fornecer suporte para uma investigação. De facto, uma vez constatada a ocorrência de infracção penal com uso de informática, diante das características da espécie, envolvendo sensíveis aspectos técnicos e quase sempre "uma identidade camuflada, desde já nasce a problemática da comprovação, pelos meios admitidos em Direito, da sua existência e de quem foi o seu autor"[503]. No contexto dos crimes cibernéticos, esses vestígios digitais tornar-se-ão "evidências digitais que são essenciais para a comprovação da materialidade do crime, assim como, se possível, sua autoria."[504]

A comprovação da materialidade do delito é de todo importante para a prossecução criminal. Isto porque, se inexistente ela, estará ausente na espécie um requisito mínimo para a deflagração da acção penal, qual seja justa causa[505]. Nisso, e consoante a lição de Nestor Távora[506], "o exercício da acção penal não pode ser uma aventura irresponsável, só assistindo

---

[500] RONCADA, Rodiner, A ***prova da materialidade delitiva nos crimes cibernéticos*** p.p. 175 (1-354) in EMAG-Escola de Magistrados da Justiça Federal da 3ª Região. Caderno de estudos: Investigação e prova nos crimes cibernéticos. TRF3, São Paulo 2017.
[501] Ibidem.
[502] Ibidem.
[503] Uma vez constatada a ocorrência de infracção penal com uso de informática, diante das características da espécie, envolvendo sensíveis aspectos técnicos e quase sempre uma identidade camuflada, desde já nasce a problemática da comprovação, pelos meios admitidos em Direito, da sua existência e de quem foi o seu autor.
[504]EMAG- Escola de Magistrados da Justiça Federal da 3ª Região. Caderno de estudos: Investigação e prova nos crimes cibernéticos. TRF3, São Paulo 2017. p.37.
[505] Cfr., art. 13 do CP
[506] SALES, Marcos Levy Gondim. ob. cit., p.51.

razão ao início do processo se existirem elementos mínimos que façam concluir pela ocorrência da infracção e dos seus autores" tendo em atenção ao parafraseado do autor citado, nos leva ao entendimento de que, a investigação dos crimes cibernéticos tem de demonstrar a contento, ao final da instrução processual, a ocorrência da(s) conduta(s) descrita(s) no tipo penal no caso concreto, bem como, eventualmente, a presença de substrato probatório suficiente que indique a presença dos elementos subjectivos[507] contidos no tipo, de modo a possibilitar a valoração das provas.

De facto, tal como se procede em quaisquer tipo de crime, nos crimes cibernéticos, a prova da materialidade pode ser obtida por diversas modalidades usuais de produção de prova, tais como: documental (art. 199 do CPP), Pericial (art. 185 CPP), prova por acareação (art. 180 CPP), por reconhecimento (art, 181 do CPP), (testemunhal (art. 159 do CPP), declarativas (art. 174 do CPP). Quanto aos meios de obtenção da prova, o CPP apresenta os seguintes: os exames (art. 206), revistas e buscas (art. 209), apreensões (213). Temos ainda como meios especiais de prova: escutas telefónicas (art. 222 do CPP) as acções encobertas (art. 226 do CPP). Os mecanismos para produção de provas e os respectivos meios a adoptar, depende do valor e da espécie do crime, o conteúdo arquivado no dispositivo da vítima e no dispositivo utilizado pelo ofensor.

No caso dos crimes relacionados à pornografia de menores, que classificamos como crimes virtuais impróprios, figuradas na Secção II, previstos nos arts. 221 a 213 do CP, por exemplo, a busca e apreensão dos materiais (computador, celular, laptop, tablet, dentre outros) que contenham registos pornográficos envolvendo menores, se mostram, a contento, suficientes para a condenação do acusado, logicamente quando também demonstrada a sua autoria. Isso porque a mera conduta de adquirir, possuir ou armazenar, por qualquer meio (fotografia, vídeo etc.) cenas de sexo explícito ou pornográficas envolvendo menores é crime, ao qual é cominado a pena de 1 a 8 anos de prisão (art. 212 do CP). Portanto, pouco importa se tais arquivos são impressos ou se estão contidos em um dispositivo electrónico: a existência deles em posse de alguém comprova a materialidade do delito, por si.

A questão da comprovação da materialidade dos delitos cibernéticos é extremamente complexa. Partindo de um dos métodos usados pelos infractores - *phishing*, em que o criminoso usa exclusivamente por meio da engenharia social, induzindo a vítima a fornecer voluntariamente dados pessoais e outras informações para locupletar-se em detrimento daquela,

[507] Os **elementos subjectivos** são compostos pelo dolo e pela culpa e dolo. Isto é, o elemento subjectivo se refere à culpa do agente na prática do acto. Ao passo que o elemento objectivo, que não é o caso, se refere à descrição abstracta e genérica da conduta proibida pela lei.

entendemos ser tarefa tão complexa para a constatação da materialidade do delito previsto no art. 289 do CP, em virtude da ausência de um dos elementos desse, qual seja a violação de mecanismo de segurança de um dispositivo.

Nessas condições, pode confundir-nos que não existe a ocorrência de uma figura delitiva própria do direito penal no âmbito dos crimes cibernéticos, mas se afere, a consumação do crime de burla, previsto no art. 288 do CPP, em razão de a vítima, induzida ao erro, voluntariamente fornecer meios para que o criminoso obtenha vantagens em detrimento daquela. Importante é que a máquina invadida por outrem ou que, de outro modo, tornou-se efectivamente "um corpo de delito" seja mantida intacta até que seja ela submetida ao manuseio dos peritos para comprovar a essência do acto na esfera cibernética.

Assim sendo, da invasão ao dispositivo em que o hacker mal-intencionado em obter conteúdo de comunicações electrónicas privadas, conteúdo pessoal, informações sigilosas etc., alguns vestígios restam na máquina que só serão apagados mediante a utilização diária daquela formatação da unidade de armazenamento, intencionalmente pelo hacker etc. Dentre eles, sobressaem os chamados "«*logs* de eventos[508]» do sistema operacional, cuja informação neles contida pode devidamente ser "traduzida" para uma linguagem acessível aos operadores de Direito e, assim, ser utilizada em juízo para a constatação da ocorrência de infracção na espécie"[509].

De tudo isso, cumpre-nos dizer que é fundamental não se descurar pela sensibilidade de desaparecimento e volatilidade nas evidências dos crimes cibernéticos. De um lado, é o seu carácter de depreciação; de outro podem ser apagadas em segundos ou perdidas facilmente. Além disso, "possuem formato complexo e costumam estar misturadas a uma grande quantidade de dados legítimos, demandando uma análise apurada pelos técnicos e peritos que participam da persecução penal"[510]. Um aspecto que merece destacar para a comprovação da materialização do delito no cibercrime é a necessidade de interceptar o fluxo de comunicações

[508] "Os «***logs de eventos***» são arquivos especiais que registram eventos importantes no computador (por exemplo, quando um usuário faz logon ou quando um programa encontra um erro). Sempre que esses tipos de eventos ocorrem, o Windows registra o evento em um log de eventos que pode ser lido com o recurso Visualizar Eventos. Os detalhes nos logs de eventos podem ser úteis para usuários avançados que precisem solucionar problemas com o Windows e outros programa" MICROSOFT. "Que informações aparecem nos logs de eventos? (visualizar eventos)". Apud SALES, Marcos Levy Gondim. ob. cit., p.54).

[509] Existem, também, os logs de evento no âmbito da utilização da internet, consoante será visto somente no próximo tópico em virtude de esses cumprirem melhor papel no rastreamento do autor da infracção cibernética (SALES, Marcos Levy Gondim. ob. cit., p.54).

[510] NETO, João Araújo Monteiro, ***Aspectos Constitucionais e Legais do Crime Electrónico***. Dissertação de Mestrado em Direito Constitucional. Fundação Edon Queiroz, Universidade de Fortaleza – Unifor. Centro de Ciências Jurídicas. Programa de Pós Graduação em Direito Constitucional. Fortaleza – Ceará, 2008. Disponível em https://egov.ufsc.br/portal/sites/default/files/cp055676.pdf, acessado em 28 de Dezembro de 2023.

realizadas pelo infractor através de um computador que é o meio próprio e adequado para a efectivação do acto delituosos. Porém, nos termos processuais, tais interceptações, somente podem ser feitas mediante autorização judicial[511].

Para a sua perfeita prova, a maioria dos crimes cibernéticos exige perícia. Uma vez identificado o endereço real do criminoso, e determinada a busca e a preensão de seu computador e quaisquer Mídias que possam conter indícios da materialização será procedido o exame de corpo de delito, que é "o conjunto de diligências destinadas à instrução do processo, com a excepção da instrução contraditória" [512].

Conforme Costa, "as evidências dos crimes cibernéticos, em um computador, podem ser classificadas como evidências do usuário e evidências do sistema"[513]. O autor explica que as evidências do usuário são aquelas produzidas pelo próprio sujeito activo, em arquivos de texto, imagem ou qualquer outro tipo. Já as evidências do sistema são as produzidas pelo sistema operacional, em função da acção do sujeito activo[514]. De igual modo, se não restar comprovado durante a instrução processual a materialidade dos factos típicos imputados na inicial acusatória, ao juízo condutor do feito não restará alternativa senão a absolver o réu em razão de estarem ausentes provas da existência do facto criminoso.

Contudo, podemos aferir que a prática de crimes cibernéticos não é sinónimo de impunidade, uma vez que os dois elementos que compõem o crime, a autoria e a materialização, são passíveis de comprovação por meio de investigação criminal. A questão central será de olhar pela capacidade que a esfera penal moçambicana, com os impactos dos avanços tecnológicos, pode fazer face a esses crimes, isto é, a capacidade de investigar esses crimes que se mostram cada vez mais frequentes, para assim reduzi-los.

Aludimos que a prova da materialidade delitiva exige especial atenção dos órgãos persecutórios, já que os meios utilizados na, ou para, a infracção penal não são comuns, de conhecimento geral, mas técnicos, a impor uma demonstração científica da forma de execução do delito. O meio de prova mais adequado para a demonstração da prática criminosa "é o exame de corpo de delito, materializado em um laudo pericial emitido por técnico habilitado na área de conhecimento científico, de acordo com o previsto nos arts. 158 a 184 do Código de Processo

---

[512] Cfr., o art. 170º do Código do Processo Civil ".

[513] COSTA, Marcelo António Sampaio Lemos, ***Computação Forense***. p. 26, Disponível no www.estantevirtual.com.br/b/marcelo-sampaio-lemos-costa/computação-forense/593469987, acessado no dia 20 de Julho de 2017.

[514] Ibidem.

Penal brasileiro (CPPB)"[515]. Define-se como corpo de delito "o conjunto dos vestígios deixados pela infracção penal; já o exame de corpo de delito é a análise e o registo feito por peritos acerca desses vestígios, com as conclusões técnicas derivadas do material observado"[516]. Em conformidade com Roncada, o exame do corpo de delito, pode ser directo ou indirecto, a depender se recai sobre o próprio corpo de delito (objectos vinculados directamente à infracção penal) ou sobre elementos obtidos por outras fontes (dados ou informes que não compõem o corpo de delito, mas podem elucidar o ocorrido)[517].

Partindo da visão Roncada, "várias questões podem surgir a partir da assertiva de que a prova da materialidade do crime de informática depende do exame de corpo de delito: o laudo pericial é mesmo imprescindível para a prova da materialidade em infracções penais de informática? Pode ele ser substituído validamente por outros meios legítimos de prova? Se o corpo de delito desapareceu, por destruição ou ocultação, o laudo pericial fica prejudicado? Qual é o momento mais oportuno para a realização do exame?"[518]

Para encontrar algumas respostas a volta das questões problemáticas assentes nesta asserção, recorremos ao entendimento de Roncada, que nos fala do assunto nos seguintes termos:

> "Nas infracções penais de informática, o exame de corpo de delito é inevitável: não há como confirmar de modo seguro a sua existência e a sua extensão sem constatar o caminho lógico percorrido pelo agente criminoso dentro do ambiente virtual, até mesmo determinando a origem dos actos executórios, fundamental para circunscrever a autoria do crime. Isso só pode ser feito por exame técnico, em que os vestígios são analisados e classificados por profissional habilitado em informática, que vai elaborar uma opinião crítica e abalizada sobre os fatos científicos observados. Somente sob circunstâncias muito especiais dispensa-se o exame de corpo de delito, aplicável, como regra, a qualquer infracção penal, inclusive a cibernética"[519].

Ainda na senda das questões levantadas nos parágrafos anteriores, Roncada alude a duas situações como resposta das questões ora colocadas:

> "Em primeiro lugar, por mais evidente, dispensa-se o exame pericial em caso de desaparecimento dos vestígios, por destruição ou ocultação total dos objectos que compõem o cenário do crime. Sem objecto a examinar, impossível qualquer verificação técnica, ficando autorizada a substituição da prova pericial pela prova testemunhal (art. 167 do CPPB). Ressalva-se que, nas infracções cibernéticas, vários vestígios são virtuais (incorpóreos), cujos dados não raras vezes independem da máquina desaparecida e que podem ser úteis na elucidação da materialidade e da

[515] RONCADA, Rodiner. A prova da materialidade delitiva nos crimes cibernéticos pp. 189 (1-354) in EMAG-Escola de Magistrados da Justiça Federal da 3ª Região. Caderno de estudos: Investigação e prova nos crimes cibernéticos. TRF3, São Paulo 2017.
[516] Ibidem, p. 179 (1-354) .
[517] Ibidem, ***p.*** 189 (1-354)
[518] Ibidem, p. 189 (1- 354).
[519] RONCADA, Rodiner. ***Ob. cit***. p. 189 (1- 354).

> autoria (a exemplo de dados gravados em servidor de rede), impondo-se então a realização do exame pericial indirecto. Segundo, os fatos evidentes, decorrentes de um silogismo simples, e os fatos notórios, de conhecimento geral do povo, não precisam ser provados, prescindindo do exame pericial. Por exemplo, num crime de posse de material pornográfico infantil envolvendo criança de tenra idade, não é necessária prova técnica para confirmar a qualidade de "criança", evidenciada pelas imagens apreendidas. Aqui é preciso bastante cuidado para não confundir fato notório ou evidente, que pressupõe a certeza do conhecimento, com presunção comum, retirada do raciocínio dedutivo mais complexo, insuficiente para comprovar a materialidade delitiva. Por exemplo, um determinado site é conhecido pela venda de softwares piratas; alguém adquiriu, para revender, programas de informática naquele site; há grande oportunidade de esses programas serem piratas, violadores de direitos autorais, mas há-de ser comprovada tal circunstância"[520].

Do entendimento dos pressupostos constituintes das questões relativas à problemática do corpo de delito, podemos aferir que pelo facto de estarmos presentes a uma infracção penal que assenta na ciência da informática, a prova da materialidade delitiva deve ser feita por exame de corpo de delito, aquilatando-se o caminho técnico percorrido pelo agente para a prática da infracção digital. Somente o exame de corpo de delito, "formalizado em laudo pericial, trará a necessária segurança jurídica para a afirmação da existência ou não da infracção penal cibernética, de modo a atender adequadamente aos postulados constitucionais do estado de inocência e do sistema penal acusatório"[521].

[520] Ibidem.
[521] Ibidem.

CAPÍTULO IV: A TUTELA JURÍDICA DOS CRIMES CIBERNÉTICOS NO DIREITO COMPARADO.

Entende-se por tutela jurídica a protecção dos direitos enunciados pelo legislador, podendo ser de cunho material ou processual. A tutela atinge seu objectivo final quando o direito é efectivamente protegido ou é devidamente realizado[522].

Neste capítulo propusemo-nos fazer um estudo comparado, a fim de verificar quais directrizes são assumidos nos demais ordenamentos jurídicos na temática relativa a políticas implementadas no combate e prevenção dos crimes cibernéticos, de forma a perceber em que passos se encontra o ordenamento jurídico moçambicano face aos demais.

4.1. Convenção sobre Cibercrime (do Conselho da Europa).

A Convenção sobre o Cibercrime, também conhecida como Convenção de Budapeste sobre o Cibercrime ou simplesmente Convenção de Budapeste, é um tratado internacional sobre direito penal e direito processual penal, firmado no âmbito do Conselho da Europa a fim de promover a cooperação entre os países no combate aos crimes praticados por meio da Internet e com o uso de computadores[523].

A referida Convenção e sua Minuta do Relatório Explicativo foram adoptados pelo Comité de Ministros do Conselho da Europa em 2001. A Convenção prevê a criminalização de condutas, normas para investigação e produção de provas electrónicas, e meios de cooperação internacional. Quanto ao direito penal material, ela disciplina violações de direito autoral, fraudes relacionadas a computador, material de abuso sexual infantil, crimes de ódio e violações de segurança de redes. No aspecto processual, prevê uma série de poderes e procedimentos, como a pesquisa de redes de computadores e interceptação legal. E na parte de internacional, trata de extradição, assistência jurídica mútua[524].

A Convenção de Budapeste sobre o cibercrime tem 48 artigos e a seguinte sistematização:

Preâmbulo

[522] MARINONI, 2003, *apud* COLLI, Jonathan Delli, & BEZERRO, Eduardo Buzetti Eustachio. A tutela jurídico-penal dos crimes digiatais. Colloquium Socialis, Presidente Prudente, v. 01, n. Especial 2, Jul/Dez, 2017, p.142.
[523] Cfr. Convenção sobre cibercrime, disponível em: https://rm.coe.int/16802fa428 - acesso- 01-10-2024
[524] Cfr. Convenção sobre cibercrime, disponível em: https://rm.coe.int/16802fa428 - acesso- 01-10-2024

Capítulo I- Terminologia: (artigo 1 definições)

Capítulo II- Medidas a tomar a nível nacional;

Secção I – Direito penal Material

Título 1 - infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos: (artigo 2 – acesso ilegítimo); (artigo 3- interceptação ilegítima); (artigo 4- interferência em dados); (artigo 5- interferência em sistemas); (artigo 6- uso abusivo de dispositivos);

Título 2 - infracções relacionadas com computadores: (artigo 7- falsidade informática); (artigo 8 – Burla informática);

Título 3 - infracções relacionadas com o conteúdo: (artigo 9- infracções relacionadas com a pornografia infantil);

Título 4 - infracções relacionadas com a violação de direito de autor e conexos: (artigo 10 – infracções relacionadas com o direito do autor e conexos);

Título 5 - outras formas de responsabilidade e sanções: (artigo 11- tentativa e cumplicidade); (artigo 12- responsabilidade de pessoas colectivas); (artigo 13 – sanções e medidas;

Secção 2- Direito Processual

Título 1- disposições comuns: (artigo 14- âmbito das disposições processuais); (artigo 15- condições e salvaguardas);

Título 2 - conservação expedita de dados informáticos armazenados: (artigo 16- conservação expedita de dados informáticos armazenados); (conservação expedita e divulgação parcial de dados de tráfego);

Título 3 - injunção: (artigo 18- injunção);

Título 4 - Busca e apreensão de dados informáticos armazenados: (artigo 19- Busca e apreensão de dados informáticos armazenados);

Título 5 - recolha em tempo real de dados informáticos: (artigo 20 – recolha em tempo real de dados relativos ao tráfego); (artigo 21- interceptação de dados relativos ao conteúdo);

Secção 3 - Competência: (artigo 22 – Competência);

Capítulo III- Cooperação internacional

Secção I – Princípios gerais;

Título 1- Princípios gerais relativos à cooperação internacional: (artigo 23- Princípios gerais relativos à cooperação internacional);

Título 2 – Princípios relativos à extradição: (artigo 24 – extradição);

Título 3- Princípios gerais relativos ao auxílio mútuo: (artigo 25- Princípios gerais relativos ao auxílio mútuo); (artigo 26 – informação espontânea);

Título 4- Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis: (artigo 27 - Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis); (artigo 28 – confidencialidade e restrição de utilização);

Secção 2- Disposições específicas

Título 1- Auxílio mútuo em matéria de medidas provisórias: (artigo 29 – conservação expedita de dados informáticos armazenados); (artigo 30 – divulgação expedita dos dados de tráfego conservados);

Título 2- Auxílio mútuo relativamente aos poderes de investigação: (artigo 31 – auxílio mútuo relativamente ao poder de acesso a dados informáticos armazenados); (artigo 32 – acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público); (artigo 33- auxílio mútuo relativamente à recolha de dados de tráfego em tempo real); (artigo 34 – auxílio mútuo em matéria de interceptação de dados de conteúdo);

Título 3- rede 24/7: (artigo 35 – rede 24/7);

Capítulo V- Disposições finais: (artigo 36 – assinatura e entrada em vigor); (artigo 37 – adesão à convenção); (artigo 38 – aplicação territorial); (artigo 39 – efeitos da convenção); (artigo 40 – declarações); (artigo 41 – cláusula federal); (artigo 42 – reservas); (artigo 43 – estatuto e levantamento das reservas); (artigo 44 – aditamentos); (artigo 45 – resolução de litígios); (artigo 46 – consulta entre as partes); (artigo 47 – denúncia); (artigo 48- notificação).

Moçambique ainda não aderiu a Convenção de Budapeste sobre o cibercrime, mas é um dos países a ser oficialmente convidado a aderir à Convenção Europeia sobre Crimes

Cibernéticos também conhecida como Convenção de Budapest, como aprovado e divulgado no site do Conselho da Europa no dia 7 de Fevereiro de 2024([525]) ([526]).

4.2. Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais

"Em 2014, os membros da União Africana (UA) aprovaram a Convenção da União Africana sobre Cibersegurança e Protecção dos Dados Pessoais ("a Convenção"). Os Ministros da UA responsáveis pela Comunicação e Informação e Tecnologia da Comunicação (CICT) e serviços Postais confirmaram o seu empenho na Convenção no Comité Técnico Especializado da União Africana sobre Comunicação e na Declaração Ministerial de TIC (AU/CCICT - 2) "[527].

Segundo a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais, os "Estados-membros devem adoptar nos correlatos ordenamentos jurídicos internos, através da aprovação de diplomas legais que as concretizem, o capítulo relativo à "*Promoção da Cibersegurança e a Luta contra o Cibercrime"*[528].

A Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais foi **"introduzida em Moçambique após a sua ratificação em 2019, através da Resolução n.º 5/2019 de 20 de Junho,** mas existe alguma legislação que foi adoptada antes da sua ratificação (em 2019), "como se sucede com a Legislação de Combate ao Cibercrime (introdução dos "crimes informáticos" no Código Penal de 2014), Autoridades Reguladoras Nacionais (Lei n.º 2/2017 – Cria o Serviço Nacional de Investigação Criminal "SERNIC"); Protecção de Infra-estruturas Críticas (Aviso do Banco de Moçambique que estabelece as Directrizes de Gestão de Risco, abreviadamente designadas por *DGR* – Aviso n.º 4/GBM/2013) "[529].

---

[525] Instituto Nacional de Tecnologias de informação (de Moçambique).https://intic.gov.mz/mocambique-e-convidado-a-aderir-a-convencao-europeia-sobre-crimes-ciberneticos-convencao-de-budapest/

[526] Cfr. o Convite de Moçambique em: https://www.coe.int/fr/web/cybercrime/-/grenada-and-mozambique-have-been-invited-to-accede-to-the-convention-on-cybercrime),

[527] Cfr. https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_201809June_Final_Portuguese.pdf

[528] NOA, Francisco. *Direito Digital na ordem jurídica moçambicana (VII) – Cibersegurança – Medidas legais ao combate do cibercrime*. In Jornal o País, de 19.03.2020, disponível em: https://opais.co.mz/direito-digital-na-ordem-juridica-mocambicana-vii-ciberseguranca-medidas-legais-ao-combate-do-cibercrime/ - acesso: 01.10.2024

[529] NOA, Francisco. *Direito Digital na ordem jurídica moçambicana (VII) – Cibersegurança – Medidas legais ao combate do cibercrime*. In Jornal o País, de 19.03.2020, disponível em: https://opais.co.mz/direito-digital-na-ordem-juridica-mocambicana-vii-ciberseguranca-medidas-legais-ao-combate-do-cibercrime/ - acesso: 01.10.2024

O artigo 25 n°1 da Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais, *''cada Estado-parte 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 infra-estruturas de redes subjacentes, assim como as medidas consideradas eficazes para a busca e julgamento de criminosos''*.

4.3. Tutela Jurídica dos Crimes Cibernéticos em Portugal

Em conformidade com Marques, o Código Penal português, não tendo nenhuma lei específica sobre cibercrime, tem algumas regras que são aplicáveis aos crimes informáticos ou praticados via internet. O artigo 180.º é um dos exemplos, ao incidir sobre a difamação, e é aplicável às afirmações que sejam feitas via internet. As regras dos artigos 153.º, 154.º e 155.º sobre ameaça e coacção também são aplicáveis a actos cometidos através da Web[530].

No entanto, a partir de 1991, como apregoa Vidigal[531], foram criadas regras especificas relativas ao cibercrime, tendo sido produzida a Lei da Criminalidade Informática, Lei 109/91, de 17 de Agosto. Posteriormente foi criada a Lei do Cibercrime, Lei 109/2009, de 15 de Setembro. Esta nova lei " (…) estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa"[532]

Na Lei 109/2009, de 15 de Setembro, são definidos "sistema informático", "dados informáticos", "dados de tráfego", "fornecedor de serviço", "intercepção", "topografia" e "produto semicondutor". O artigo 3.º, relativo à falsidade informática, estabelece o seguinte:

> 1) Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com

[530] Marques A, Anjos M, Vaz S (2002) 101 Perguntas e respostas do direito da internet e da informática, Centro Atlântico.PT, pp. 49/50, 341/342, apud VIDIGAL, Inês Maria Andrade, ***As Políticas de Combate a Cibercrime na Europa***, Dissertação de Mestrado em Políticas Europeias, Instituto de Geografia e Ordenamento Territorial, Universidade de Lisboa, 2012, p.92.

[531] VIDIGAL, Inês Maria Andrade, ibidem, p. 92.

[532] BDJUR (2011) ***Código do direito de autores e dos direitos conexos,*** Almedina, pp. 151- 166. Apud VDIGAL, Inês Maria Andrade, ***ob., cit.,*** p. 92.

a intenção de que estes sejam considerados ou 93 utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.

2) Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.

3) Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente.

4) Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos.

5) Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.

O artigo 4.º, relativo ao dano relativo a programas ou outros dados informáticos, estabelece:

1) Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.

2) A tentativa é punível.

3) Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número.

4) Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias.

5) Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.
6) Nos casos previstos nos n.ºs 1, 2 e 4 o procedimento penal depende de queixa.

Relativamente à sabotagem informática, o artigo 5.º, estabelece:
1) Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.
2) Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.
3) Nos casos previstos no número anterior, a tentativa não é punível.
4) A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado.
5) A pena é de prisão de 1 a 10 anos se:

a. O dano emergente da perturbação for de valor consideravelmente elevado;

b. A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

Quanto ao acesso ilegítimo, o 6.º artigo, estabelece que:
1) Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2) Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.
3) A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.
4) A pena é de prisão de 1 a 5 anos quando: a. Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou b. O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.
5) A tentativa é punível, salvo nos casos previstos no n.º 2. 6) Nos casos previstos nos n.ºs 1, 3 e 5 o procedimento penal depende de queixa.

No que concerne à intercepção ilegítima, o artigo 7.º, estabelece:
1) Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa.
2) A tentativa é punível.
3) Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número.

O artigo 8.º, relativo à reprodução ilegítima de programa protegido, estabelece:

1) Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa.

2) Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.

3) A tentativa é punível. A lei estabelece ainda as disposições processuais relativas à "Preservação expedita de dados" (artigo 12.º), "Revelação expedita de dados" (artigo 13.º), "Injunção para apresentação ou concessão do acesso de dados" (artigo 14.º), "Pesquisa de dados informáticos" (artigo 15.º), "Apreensão de dados informáticos" (artigo 16.º), "Apreensão de correio electrónico e registos de comunicações de natureza semelhante" (artigo 17.º), "Intercepção de comunicações" (artigo 18.º) e "Acções encobertas" (artigo 19.º)[533].

Como afirma Vidigal, "Profissionais desta área salientam ainda a necessidade de criar um órgão coordenador de todos os serviços necessários para combater o cibercrime, a colaboração entre entidades e um reforço dos meios repressivos"[534]. Segundo o Público, Perante os ataques a portais do governo, ocorridos em 2012, foi aprovada a criação de um Centro Nacional de Cibersegurança mas que ainda não tem data de entrada em funcionamento[535].

- Principais ilações das políticas implementadas no âmbito do combate e prevenção nos quatro países estudados:

Tendo em revista a análise comparativa no âmbito das políticas implementadas para o combate e prevenção dos crimes cibernéticos nos quatro países, ora estudados, somos do entendimento que o cibercrime desafia os valores fundamentais que o mundo defende: direitos humanos, democracia e o estado de Direito. Contudo, o aumento da importância e da utilização das tecnologias de informação e comunicação em todos os domínios do comércio global e da sociedade revela-se o grande motivo para o combate ao cibercrime, exigindo uma regulação multidisciplinar.

Observamos que há um elemento comum em todos os países estudados, que tem a ver com discrepância entre os cibercrimes e os sistemas de direito penal, uma vez que os traços fundamentais, funcionalidades e práticas do cibercrime escapam ao enquadramento da lei tradicional e do seu sistema:

---

533 . Diário da República (2009, 179 Série I) ***"Lei do Cibercrime***", Lei 109/2009, de 15 de Setembro in Diário da República - http://www.cnpd.pt/bin/legis/nacional/LEI109-2009- %20CIBERCRIME.pdf [acedido em 6 de Dezembro de 2012], apud VIDIGAL, Inês Maria Andrade, ***ob., cit***., p.96

534 VIDIGAL, Inês Maria Andrade, ***ob., cit***., p.96

535 Público, 17-02-2012, apud VIDIGAL. Inês Maria Andrade, ibidem, p. 96.

a. Enquanto o direito penal tradicional lida sobretudo com a protecção de bens claramente definidos contra ataques humanos, o cibercrime viola frequentemente valores intangíveis que dependem do difícil equilíbrio de interesses, complicados de definir pelos meios tradicionais.

b. O sistema judicial tradicional tem por base a ideia de soberania, cujo raio de acção é limitado ao seu território. No entanto, a internet e o cibercrime são globais;

c. O sistema judicial tradicional é lento: as decisões tomadas pela polícia têm que ser assinadas por um juiz, o acusado tem direito a ser ouvido em tribunal (entre outras precauções), o que torna o processo muito lento e muito burocrático. Pelo contrário, a internet é extremamente rápida – tal também o são os cibercrimes. A velocidade de transferência de processos e a interacção multinacional representam um desafio para qualquer sistema legal e para qualquer instituição nacional;

d. Num processo penal, o acusado tem que ser claramente identificado e têm de ser apresentadas provas sólidas do crime por ele cometido. Porém, estas exigências colocam dificuldades acrescidas à acusação de alguém que tenha cometido um cibercrime. Por um lado, quem tiver um conhecimento alargado sobre a utilização do sistema informático sabe esconder o seu rasto, e a internet garante um anonimato difícil de transpor. Outro problema frequente coloca-se na recolha das provas necessárias para a acusação de um infractor, o que exige a disponibilização de informação por parte de diversos países – e em vários países a Constituição proíbe-o; e ainda no campo do Direito, é necessário não só ir incluindo as novas formas de ataques cibernéticos no sistema penal, mas também adicionar e relacionar o cibercrime à legislação já existente nas áreas de violação dos direitos de autor, da protecção de dados e da protecção de menores;

f. A questão do anonimato e da falta de provas é outro campo a necessitar de reformulação, mas em que as intervenções são difíceis.

4.4. Tutela Jurídica dos Crimes Cibernéticos no Brasil

Em conformidade com Letícia dos Santos, existem hoje algumas políticas públicas implementadas em atenção aos Cibercrimes, como por exemplo “a Estratégia Nacional de Segurança Cibernética – E-Ciber – aprovada somente em fevereiro de 2020, porém eleita pelo Gabinete de Segurança Institucional da Presidência da República, em janeiro de 2019, como o primeiro módulo da ENSI (Estratégia Nacional de Segurança da Informação), esta elaborada a partir do Decreto nº 9637, de 26 de dezembro de 2018, para implementação da Política Nacional

de Segurança da Informação"[536]. Nesse corolário, foram estabelecidos como objectivos e acções estratégicas: "tornar o ambiente virtual do Brasil mais confiável, ampliar a resistência à ameaças cibernéticas e fortalecer a actuação do País em segurança cibernética internacional"[537]

Segundo a Letícia Santos, a E-Ciber propõe ainda, que "é fundamental que se invista em uma cultura de segurança cibernética através da educação dos usuários, promovendo ac utilização responsável dos meios digitais, por meio da elaboração de cursos superiores em segurança cibernética, acções de consciencialização da sociedade sobre o tem, além da inclusão na educação básica escolar sobre o uso ético da tecnologia"[538] .

Outro exemplo de política social implantada no campo brasileiro, "é o projecto 'Ministério Público pela Educação Digital nas Escolas', que através da actuação do Ministério Público Federal, tem como público-alvo educadores de escolas da rede pública e privada, oferecendo incentivo para a realização de actividades que ensinem crianças e adolescentes sobre o uso seguro e responsável da Internet, evitando assim que sejam vítimas ou pratiquem crimes virtuais"[539].

O referido projecto foi "Instituído em 2015 por meio da Portaria PGR/MPF nº 753, o mesmo segue as Directrizes do Marco Civil da Internet (Lei 12965/14), que evidencia o dever do Estado em promover a utilização da internet de forma segura, responsável e consciente. Sob a coordenação da Procuradoria Federal dos Direitos dos Cidadãos, o MPF realiza, em parceria com a ONG SaferNet, a oficina "Segurança, ética e cidadania na Internet: educando para boas escolhas on-line, que é promovida em vários estados pelo país"[540].

No Estado da Bahia, ainda no Brasil, "o Ministério Público criou um núcleo de investigação especializado, voltado para os delitos virtuais, o NUCCIBER[541] – Núcleo de Combate aos Crimes Cibernéticos -, que tem por objectivo acções de incentivo e cooperação às

---

[536] SANTOS, Letícia Dutra de Oliveira, Políticas Públicas de Educação Digital: Prevrnção e Combate aos Crimes Cibernéticos, Monografia apresentada na UniEvangélica, para obtenção de grau de Bacharel em Direito, Anápolis, 2020, p. 27.

[537] BRASIL. Lei 13853, de 8 de julho de 2019. Altera a Lei de Proteção de Dados; e dá outras providências. Presidência da República. Secretaria Geral. Subchefia para Assuntos Jurídicos, apud Santos, Leticia, ob., cit. p

[538] Ibidem, pp. 26-27.

[539] BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. ***Crimes Cibernéticos***/ 2ª Câmara de Coordenação e Revisão Criminal. Brasília: MPF, 2018. p.275. (Coletânea de artigos; v. 3). Apud, SANTOs, Letcia, ***ob., cit,.*** p. 27.

[540] SANTOS, Letícia, ***ob., cit,.*** p. 27

[541] "O NUCCIBER utiliza ainda a própria internet, para, através das redes sociais, divulgar dicas e maneiras de prevenção contra os ataques cibernéticos. São 28 publicados cartazes, banners, cartilhas e vídeos acerca do tema nos meios de comunicação digitais e também na televisão e rádio. Após a análise de algumas dessas políticas públicas adotadas no Brasil, é possível perceber que a Educação Digital é um importante vetor de colaboração na luta contra as infrações virtuais, já que dessa forma os usuários além de conhecer quais são esses delitos, ainda aprendem maneiras de se proteger e quais são as sanções contra quem os comete". SANTOS, Letícia, ob. cit., p. 27.

actividades que visam combater tais crimes"[542] . Na locução da autora, o Núcleo actua proporcionando "capacitação à Promotores de Justiça e outros agentes actuantes na persecução penal, através de treinamentos, seminários e oficinas"[543]. São desenvolvidas ainda, em conformidade com Letícia Santos[544] "actividades repressivas e preventivas, tais como o auxílio nas investigações criminais, inclusão digital dos cidadãos através de palestras em instituições de ensino, oficinas voltadas para profissionais do Direito e instruções para profissionais que trabalham usando plataformas digitais".

4.4.1. Educação Digital

Como apregoa Letícia Santos[545], "A Era Digital vivenciada nos dias actuais, traz como uma de suas várias consequências, a facilidade de interacção entre diversas pessoas, ideias e opiniões acerca de diferentes temas. No ambiente virtual a vida dos usuários pode ser exposta e se tornar alvo fácil de ataques on-line, sejam eles na esfera patrimonial ou moral, e para evitar esses episódios a educação digital dos utilizadores é fundamental".

A escola exerce importante papel na formação da consciência ética e moral dos alunos, devendo se adequar à nova realidade na qual o acesso aos meios digitais está cada vez mais difundido entre crianças e adolescentes, ensinando sobre temas como responsabilidade digital, prevenção contra roubo de dados, assédio virtual, e também sobre as consequências jurídicas do uso inadequado da internet, criando usuários mais éticos no ciberespaço.

Ficou estabelecido na "Lei 12965/2014, Marco Civil da Internet, em seu artigo 26, que é dever constitucional do Estado a prestação de educação para uso responsável da internet, e para isso, fica também sob sua responsabilidade proporcionar ferramentas de capacitação para atingir tal objectivo, tornando a tecnologia aliada ao desenvolvimento da cultura e exercício da cidadania"[546]. Decorrente da mesma Lei, o art. 27 determina os objectivos que devem ser buscados pelas acções do Estado de incentivo à cultura digital, tais como a inclusão digital e a redução de desigualdades no tocante ao acesso às tecnologias, além de ainda procurar impulsionar a produção e circulação de conteúdo digital nacional[547].

---

[542] Ibidem, p. 27.
[543] Ibidem, p. 27.
[544] Ibidem., p.27.
[545] Santos, Letícia, ***ob., cit.,*** p. 27.
[546] BRASIL. Lei 12965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Apud SANTOS, Letícia, ob., cit., p. 28.
[547] Ibidem, p.29.

O Ministério Público do estado da Bahia, em seu artigo acerca da política criminal adoptada no combate aos crimes cibernéticos, confirma que "a protecção aos bens jurídicos advindos do ambiente virtual será melhor alcançada quando a educação e inclusão digital forem adoptadas como principais ferramentas de combate, e que a consciencialização da necessidade da ética nas condutas no campo digital trará redução dos crimes informáticos"[548] É nítida a percepção de que a educação digital é um indispensável vector de colaboração na luta contra os cibercrimes, e o Ministério Público, juntamente com actuação do Governo e de ONG's, é o actor principal nessa tarefa, buscando, além da repressão, a prevenção por meio da consciencialização da população.

4.4.2. O Papel do Ministério Público

O Ministério Público, na qualidade de órgão de defesa dos interesses sociais, é efectivamente, actuante nos projectos definidos pelas políticas públicas, sendo, dessa forma, importante o estudo de seu papel de maneira mais detalhada. Trazido pela Carta Magna de 1988, em seu artigo 127, como sendo instituição permanente, responsável pela defesa da ordem jurídica, dos interesses sociais e individuais indisponíveis, dentre outros, é um Órgão que actua como colaborador das actividades estatais[549].

O Promotor de Justiça do Ministério Público do Estado de São Paulo, Luiz Sales do Nascimento, em seu artigo 'Ministério Público: aspectos gerais' (2017), aponta que "tal órgão, devido à sua autonomia perante os três poderes, executivo, legislativo e judiciário, possui a incumbência de ser fiscalizador destes, além de possuir também a função de acusador, já que a função de julgador é privativa do Estado"[550].

Quanto às áreas de actuação da instituição, especificamente relativas à cidadania, educação e segurança, que são os temas tratados na abordagem de Letícia Santos, "a CONAMP, Associação Nacional dos Membros do Ministério Público, esclarece que é dever institucional do Órgão, actuar em actividades de interesse social, defesa e garantia dos direitos dos cidadãos, e relativas à educação, fiscalizando a qualidade dos serviços escolares e ainda promovendo iniciativas de colaboração com os mesmos"[551]. Dessa forma, as políticas públicas sendo ferramentas utilizadas pelo Estado para garantir a efectividade dos direitos sociais dos indivíduos, e os crimes cibernéticos actos infraccionais que lesam direitos de usuários da

[548] SANTOS, Letícia, ***ob., cit.,*** p. 29.
[549] Ibidem, p. 30.
[550] Ibidem, p.30.
[551] Ibidem, p.30.

internet, cabe ao Ministério Público, tanto Federal quanto estadual, estar à frente das actividades de prevenção e combate, cumprindo seu dever de tutela dos interesses da população.

O Ministério Público, exercendo seu papel de controlo da Administração Pública, tem a obrigação, como ensina a Procuradora da República, Mona Lisa Duarte (2014)[552] de fiscalizar a implementação de políticas públicas, além de actuar também na realização de actividades pertinentes ao programa, e na adequação dele para melhor alcançar os fins traçados como objectivos. Ainda nas palavras da Procuradora, "a Instituição dispõe de papel essencial no monitoramento das políticas sociais, indo além da fiscalização, actuando também na concretização destas na sociedade, por meio da realização de projectos e actividades, além ainda do dever de, ante à inércia do Estado frente à alguma política, cobrar tal actuação por vias judiciais ou extrajudiciais"[553].

No nosso entendimento, além do Ministério Público, existem outros actores de participação fundamental no processo das políticas sociais implementadas em atenção aos crimes virtuais, tais como OGN's, empresas privadas e delegacias especializadas, dotadas de maior capacidade técnica para investigação dos actos delituosos.

4.4.3. Delegacias Especializadas

A adequada investigação dos crimes cibernéticos é a parte importante no processo de repressão dessas condutas, e para que isso seja possível, é imprescindível que existam órgãos que disponham de recursos e profissionais capacitados para uma averiguação eficiente dos actos ilícitos à eles reportados. Nesta perspectiva, a Constituição Brasileira de 1988 trouxe, em seu Título V, Capítulo III, a Defesa do Estado e das Instituições Democráticas e a Segurança Pública, às delimitando, no artigo 144, como dever do Estado, direito e responsabilidade de todos, e sendo concretizadas através dos órgãos de Polícia[554]. Nisso, as delegacias são as bases policiais, que prestam atendimento à população, e nas quais actuam os membros da força policial, seja ela federal, civil ou municipal, exercendo as funções delimitadas pelo Estado.

Ainda citando o disposto na Constituição Federal de 1988, "ficou ao cargo da Polícia Civil a função de polícia judiciária e a investigação de ilícitos penais", como define o art. 144 em seu parágrafo 4º. Cabendo então, a ela apurar os crimes cibernéticos, na busca pela sanção dos infractores. Porém, a investigação de crimes ocorridos no ambiente digital, ou através dele,

[552] SANTOS, Letícia , ***ob., cit.,*** p. 30.
[553] Ibidem, p.31.
[554] A Constituicção da República Federativa da do Brasil de 1988, foi aprovada pela Assembleia Nacional Constituinte em 22 de Setembro de 1988 e promulgada em 5 e Outubro de 1988.

exige profissionais com conhecimento mais especializado e técnico na área, além de exigir também ferramentas mais específicas para possibilitar a apuração dos fatos, e as delegacias comuns não vinham atendendo de maneira eficaz esses requisitos, fazendo com que surgisse assim, a necessidade de delegacias especializadas.

Foi com a promulgação da Lei 12735/12, que ficou estabelecida a criação nos órgãos da polícia judiciária, de departamentos e grupos especializados na actuação contra cibercrimes, como dispõe seu artigo 4º[555]. A Secretaria Nacional de Segurança Pública, no artigo "Modernização da Polícia Civil Brasileira" conceptua Delegacias Especializadas "como unidades operacionais com actividades especializadas em determinados ilícitos penais, actuando como apoio às delegacias comuns, fornecendo informações específicas, apoio técnico e auxiliando nas investigações, mas que também podem dispor de autonomia investigativa em situações especiais"[556].

Em conformidade com Letícia Santos[557], no Brasil, os primeiros Estados a possuir delegacias especializadas na actuação contra os crimes cibernéticos, foram São Paulo e Espírito Santo, e actualmente elas já estão presentes em 15 Estados e no Distrito Federal. A ONG Safernet, que também apoia projectos desenvolvidos pelo Ministério Público, disponibiliza, na sua página na internet, a relação das delegacias presentes nos Estados. Entre elas, estão a DRCI, Delegacia de Repressão aos Crimes Informáticos, no Rio de Janeiro; o Grupo Especializado de Repressão aos Crimes por Meios Electrónicos, na Bahia; a DEICC, Delegacia Especializada de Investigação de Crimes Cibernéticos.

Dessa forma, o trabalho executado por esses órgãos especializados é mais um factor de colaboração na luta contra a ocorrência dos Ilícitos Informáticos, apesar de o mecanismo mais adequado ainda ser a prevenção por meio da educação e consciencialização digital.

4.4.4. Prevenção, Combate e Efectividade das Políticas

No tangente a perspectiva de Prevenção, Combate e Efectividade das Políticas de combate a criminalidade cibernética, é possível quando são elaboradas em tendo em conta a educação, buscando incentivar a prevenção para que haja menor ocorrência dos ilícitos. É facto que a repressão aos crimes cibernéticos, aplicada através de sanções previstas na lei, apesar de esta estar constantemente se aperfeiçoando, não consegue extinguir as condutas delituosas, em parte devido a falhas existentes na legislação, deixando lacunas obscuras, parte pela rápida

[555] SANTOS, Letícia, ***ob., cit.,*** p.32.
[556] Ibidem, p. 32.
[557] Ibidem, p.32.

evolução da tecnologia e formas de praticar condutas criminosas, as quais a lei não consegue acompanhar de maneira eficiente.

Letícia Santos[558] apregoa que a prevenção almejada através da consciencialização da população e da educação digital de crianças, adolescentes e usuários da internet de modo geral, tem-se mostrado cada vez mais essencial, pois apesar de os planos implementados não serem perfeitos, se mostram eficazes na construção de uma sociedade cada vez mais responsável quanto ao uso das ferramentas digitais, tanto para não serem vítimas, quanto para não se tornarem futuros agressores, acarretando, assim, na diminuição da criminalidade no meio digital.

É do nosso entendimento que o avanço da tecnologia tende a ser cada vez maior, fazendo com que ela esteja presente na realização de diversas actividades da sociedade, trazendo vários desafios, entre eles, o aumento da criminalidade no ambiente virtual e através dele. Sendo, dessa forma, de extrema importância que sejam desenvolvidas políticas públicas de atenção à essas situações vividas pela sociedade, contribuindo para o desenvolvimento de internautas responsáveis e um ambiente virtual seguro, e sem dúvida, a educação é a maneira mais adequada de alcançar esse objectivo, e aliados como o Ministério Público são essenciais para que esses programas atinjam a população como um todo.

4.5. Tutela Jurídica dos Crimes Cibernéticos na Espanha

No caso Espanhol "não existe uma definição nacional de cibercrime. A legislação nacional refere-se aos tratados europeus e convenções assinados nesta matéria da seguinte forma: "Conclusões do Conselho de 26 de Abril de 2010 sobre Plano de Acção Contra o Cibercrime" e "Conclusões da Presidência sobre a Conferência de Cibercrime que teve lugar a 12-13 de Abril 2011 em Budapeste"[559]

Relativamente à legislação nacional espanhola, diz Vidigal[560] que, depois da última reforma, o Código Penal diz especificamente no preâmbulo: «Crimes informáticos – para além das mudanças no que concerne ao respeito da protecção penal da propriedade intelectual, outro

[558] SANTOS, Letícia, ***ob., cit***., p.32.
[559] VIDIGAL, Inês Maria Andrade, apud VIDIGAL, Inês Maria Andrade, As Políticas de Combate a Cibercrime na Europa, Dissertação de Mestrado em Políticas Europeias, Instituto de Geografia e Ordenamento Territorial, Universidade de Lisboa, 2012, p.67.

[560] VIDIGAL, Inês Maria Andrade, ob., cit., p. 67.

aspecto importante presente na reforma têm a ver com o que a própria reforma denomina como "crimes informáticos"[561].

No âmbito da chamada criminalidade informática, para completar a decisão 2005/222/JHA, de 24 de Fevereiro de 2005, sobre ataques contra sistemas de informação, foi decidido separar as condutas puníveis em duas secções diferentes, por se tratar de bens jurídicos diferentes[562].

Na primeira secção estão inclusas as condutas que envolvem danos, deterioração, alteração, supressão ou formas de tornar inacessíveis os dados informáticos ou programas de terceiros, assim como condutas que dificultem ou interrompam o funcionamento de um sistema informático alheio.

A segunda refere-se à descoberta e revelação de segredos, onde está compreendido o acesso não autorizado, incluindo a violação de medidas de segurança, de dados ou de *software* contidos num sistema ou em parte dele.

Ainda no que se refere a "crimes informáticos", mas tendo por objecto o "acesso a sistemas", foi introduzido um novo artigo, o 197.º-3, onde se estabelece que "quem, por qualquer meio ou processo, e vulnerabilizando as medidas de segurança existentes para prevenir acesso não autorizado, aceda sem autorização a dados ou programas informáticos dentro dum sistema informático ou de uma parte do sistema ou permaneça dentro do mesmo contra a vontade daqueles que têm o legítimo direito de excluí-lo, será punido com pena de prisão de seis meses a dois anos. Quando, em conformidade com o disposto no artigo 31.º-bis, uma pessoa jurídica seja responsável pelas infracções previstas neste artigo, deve ser obrigada a pagar uma multa de seis meses a dois anos. E atendendo às regras estabelecidas no artigo 66.º-bis, juízes e tribunais poderão também impor as sanções previstas nas alíneas b) à g) do n.º 7 do artigo 33.º".

Tipifica-se a intromissão em sistemas externos de uma forma clara e expressa, complementando o que já estava estabelecido no documento 197.º-2. No entanto, pune-se apenas a entrada no sistema, quer se produzam ou não danos ou prejuízos aos direitos do proprietário do sistema atacado. Segundo especialistas, o problema é o que se entende por aceder a dados ou programas informáticos contidos num sistema. Entroncam também nesta questão os procedimentos que modificam páginas *Web*, aproveitando-se as vulnerabilidades das

[561] VIDIGAL, Inês Maria Andrade, ibidem, p. 67.

[562] European Council (2005) ***"Council Framework Decision on attacks against information systems***" (2005/222/JHA) - http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF. apud VIDIGAL, Inês Maria Andrade, ob., cit., p. 67.

mesmas. Esclarecem os especialistas que "só decorrido um certo período será possível verificar se esta medida contribui ou não para melhorar a segurança informática, visto que, de uma maneira geral, a forma de comprovar vulnerabilidades é submetendo os sistemas a determinadas provas".

No que se refere às fraudes, também foi adicionada uma secção ao artigo 284.º-2 do Código Penal:

> 1. Cometem fraude, aqueles que, com objectivo de lucrar, distorçam a verdade o suficiente para induzir em erro outra pessoa, levando-a a realizar um acto que a prejudique a si ou a outros.
> 2. Também são culpados de fraude:
>
> a) Aqueles que, com objectivo do lucrar e servindo-se de alguma manipulação informática ou artifício semelhante, consigam uma transferência, não consentida, de qualquer activo financeiro em detrimento de outro.
>
> b) Aqueles que fabricarem, introduzirem, possuírem ou facilitarem programas informáticos específicos para cometer as fraudes previstas neste artigo".

Como se pode depreender, o artigo 284.º-2 do Código Penal Espanhol, "penaliza a programação de aplicações que permitam a prática de fraudes, assim como a sua disseminação e até a sua posse, mesmo que esta não tenha sido utilizada. Contudo, os programas devem estar especificamente desenhados para cometer este tipo de crimes, porque se tiverem outros usos ou fins a conduta não será punível (destaca-se o caso dos chips das consolas) "[563].

No que concerne a danos, foi alterado o artigo 264.º, de forma a albergar os danos causados a sistemas informáticos:

> 1. Aquele que por qualquer meio, sem autorização e de uma forma grave apague, danifique, deteriore, altere, suprima ou faça com que fiquem inacessíveis dados, programas ou documentos electrónicos de outros, quando o resultado for grave, será punido com uma pena de prisão de seis meses a dois anos.
>
> 2. Quem por qualquer meio, sem estar autorizado e de forma grave obstruir ou interromper o funcionamento de um sistema informático externo, introduzindo, transmitindo, danificando, apagando, deteriorando, alterando, suprimindo ou

[563] VIDIGAL, Inês Maria Andrade, ***ob., cit.***, p. 68.

tornando inacessíveis os dados informáticos, quando o resultado produzido for grave, será punido com uma pena de prisão de seis meses a três anos"[564].

O artigo 264 do Código Penal Espanhol, como cita Vidigal, "pune tanto a destruição de informação como os ataques que impedem um sistema de funcionar correctamente. Têm sido levantadas algumas dúvidas quanto ao significado jurídico de "o resultado produzido for grave", porque caberá unicamente ao juiz decidir o que é ou não grave e, dado que as provas deste tipo de crimes são difíceis de compilar, os resultados dos julgamentos destes crimes podem não ser sempre os mais adequados"[565].

[564] Código Penal Español, 2011, htpp://pt.scribd.com/doc/48885589/nuevo – ***CODIGO -PENAL-ESPANOL***-2011 – pdf, Apud VIDIGAL, Inês Maria Andrade, p69.
565 VIDIGAL, Inês Maria Andrade, ibidem, p. 69.

CAPÍTULO V: A TUTELA JURÍDICA DOS CRIMES CIBERNÉTICOS NO DIREITO MOÇAMBICANO.

5.1. Quadro Jurídico dos Crimes Cibernéticos em Moçambique

Moçambique é um Estado de Direito Democrático, baseado no respeito e garantia dos direitos e liberdades fundamentais do Homem (art. 3 da CRM). Nesse corolário, o Direito é um instrumento regulador e organizador da sociedade. Para tal, cabe acompanhar todas as mudanças decorrentes da evolução tecnológica pela qual passa a sociedade, buscando se adaptar das transformações, a fim de promover novas soluções para as novas peculiaridades trazidas com a prática dos crimes virtuais.

Os Crimes cibernéticos estão cada vez mais frequentes, sofisticados e mais difíceis de combater, por se tratar de uma espécie de crime originária da evolução tecnológica pela qual a sociedade contemporânea passa. Os avanços tecnológicos e as novas descobertas científicas trouxeram uma nova realidade para o ser humano, onde o espaço e a presença física não são fundamentais para a realização de condutas ilícitas. Nesse quadrante, procuramos trazer um entendimento em relação a posição do legislador moçambicano no âmbito da legislação quadro, bem como as regulamentações que podem ser aplicadas nos crimes cibernéticos. Ressalta-nos admitir que se não haver tipificação penal sobre crimes cibernéticos, não será cominado como crime, em respeito pelo princípio constitucional[566] e cuja materialização assenta na Lei Penal (Princípio da Legalidade do Direito Penal[567]. Nesse corolário, temos a legislação seguinte no ciberespaço moçambicano:

1. Constituição da República de Moçambique (CRM, 2004) – *lex fundamantallis,* revista pontualmente pela Lei nº 1/2018 de 12 de Junho, que proíbe o acesso a arquivos, ficheiros e registos informáticos ou de banco de dados para conhecimento de dados pessoais relativos a terceiros nem a transferência de dados pessoais, salvo nos casos estabelecidos pela lei ou por decisão judicial (nº 3 do art. 71 da CRM).

2. Resolução n°5/2019 de 20 de Junho, que ratifica a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais.

[566] Cfr., art. 60 da CRM (Aplicação da lei penal): "Ninguém pode ser condenado por acto no qualificado como crime no momento da sua prática (nº 1)"

[567] Cfr., art. 1 do CP "Num facto consista em acção ou omissão, pode julgar-se crime sem que uma lei, no momento da sua prática, o qualifique como tal (nº1); Não podem ser aplicadas medidas ou penas criminais que não estejam previstas na lei (nº 2).

3. Lei das Telecomunicações – Lei nº4/2016, 3 de Junho. Esta lei escabece disposições que pune (no artigo 57, aquele que interceptar as comunicações sem que para tal esteja autorizado por um Juiz de Instrução Criminal, com pena de prisão maior de dois a oito anos**.**

4. Lei das Transacções Electrónicas - Lei n.º 3/2017 de 9 de Janeiro; que trata de todo tipo de crime transaccional electrónico, sejam transacções bancárias, comerciais, ou outras onde se utiliza o meio electrónico. Esta Lei estabelece os princípios, as normas gerais e o regime jurídico das transacções electrónicas em geral, do comércio electrónico e do governo electrónico em particular, visando garantir a protecção e a utilização das TIC`s.

A Lei de Transacções Electrónicas (LTE), além de regular, disciplinar e proteger o ambiente cibernético, cria um regime sancionatório aos praticantes de crimes cibernéticos como rege o artigo 68 sobre as infracções cometidas no espaço digital. Também persistem desafios de certificação e assinaturas digitais, desafios em criptografia e forense, desafio na regulamentação do uso da Internet e desafios da harmonização da legislação internacional para crimes cibernéticos com instrumentos legais nacionais. A LTE tem impacto nas redes sociais, tem influência na redução de abuso excessivo de ataques em mensagens de ofensas a figuras públicas, intromissão na privacidade das pessoas e reduziu drasticamente as violações de segredo do Estado.

As operadoras das telecomunicações e os provedores da internet passaram a ser mais responsáveis e mais atentos sobre os utilizadores dos seus serviços. A "lei coloca Moçambique em conformidade com os protocolos internacionais, como a Convenção de Budapeste sobre Crimes Cibernéticos, adoptada em 2001. Alinha também com a Lei-modelo da SADC sobre Crimes de Informática e Cibernéticos de 2013, que estabelece um quadro de cooperação internacional no combate aos complexos crimes cometidos virtualmente no espaço cibernético".

A Lei das Transacções Electrónicas reconhece o domínio «.mz» como espaço de Internet tutelado por Moçambique; não só, como também regula e disciplina as actividades no âmbito das transacções electrónicas. Outrossim, a mesma lei em alusão, estabelece um ordenamento jurídico em que o comércio electrónico, as mensagens de dados, comunicações electrónicas e serviços do governo electrónico se processem com celeridade e segurança jurídica. A lei apresenta um glossário que inclui, para além de outras, as definições de Provedor primário de serviços e provedor intermediário.

5. O Regulamento de Registo de Cartões SIM - Decreto n.º 18/2015 de 9 de Julho, estabelece o regime jurídico aplicável ao processo de registo e activação dos Módulos de Identificação do Subscritor.

6. Código Penal – Lei n.º 24/2019, de 24 de Dezembro; o Código Penal, configura no âmbito das suas normas as Disposições Gerais, que nelas contemplam os Princípios da Territorialidade (artigo 4º) e factos praticados fora do território nacional (artigo 5º), consentâneos com artigo 22, da Convenção de Budapeste. Ainda, o Código Penal vigente prevê Infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos: Acesso ilegítimo (art. 256º); Intercepção ilegítima (art. 256, nº 2); Violação de correspondência ou de comunicações (art. 253º); Interferência em dados (art. 337º); Interferência em sistemas (artigo 338º) e Uso abusivo de dispositivos (art. 339º).

Dentro da estrutura das suas normas, o CP, contempla Infracções relacionadas com computadores: Falsidade informática (art. 336º) e Burla informática e nas comunicações (art. 289º). Inclui, igualmente, Infracções relacionadas com o conteúdo: Pornografia de menores (art. 211º); Utilização de menores em pornografia (art. 212º); Distribuição ou posse de pornografia de menores (artigo 213º). Ainda dentro do Código Penal, são estabelecidas as Formas de Responsabilidade e Sanções e Responsabilidade das pessoas colectivas em conformidade com os artigos 11 e 12, da Convenção de Budapeste.

7. Código de Processo Penal – Lei n. º25/2019, de 26 de Dezembro - Prevê Princípios Fundamentais e garantias do Processo Penal designadamente: Direito fundamental à presunção de inocência (art. 3); Proibição de provas obtidas por meios ilícitos (art. 4); Princípio do contraditório (art. 5); Direitos das pessoas detida (artigo 6); Direito `a defensor (art. 7) e Dever de fundamentação (art. 8), em conformidade com o art. 15, da Convenção de Budapeste. Permite o recurso a escutas telefónicas (arts 222 e 225) como meios de obtenção de prova, na criminalidade informática, em conformidade com o art. 21, da Convenção de Budapeste.

8. Lei n.º 2/2017 – Cria o Serviço Nacional de Investigação Criminal ("SERNIC"), que constitui um serviço policial de investigação criminal a quem compete coadjuvar as autoridades judiciárias na realização das finalidades do processo.

9. A Resolução n.º 5/2019, de 20 de Junho, que ratifica a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais ("CUACPDP"),

disciplina, no seu capítulo III, a matéria relativa a "*Promoção da Cibersegurança e a Luta contra o Cibercrime*".

10. Lei n.º21/2019, de 11 de Novembro – que Aprova os Princípios e Procedimentos de Cooperação Jurídica e Judiciaria Internacional em matéria Penal. A Lei de Cooperação Internacional de Moçambique tem disposições relativas a pedidos de extradição de Moçambique para outros Estados (arts 32 – 68); outrossim, a Lei contém uma norma (art. 157) que possibilita o Auxílio mútuo em matéria de intercepção de dados de conteúdo, conforme o disposto no art. 34 da Convenção de Budapeste.

Ao abrigo desta cooperação judiciária, ressaltamos destacar o estatuído no art. 23 da Lei em referência, nos termos do qual, os Estados podem «*utilizar na transmissão dos pedidos [de informação] os meios telemáticos adequados, desde que estejam garantidas a autenticidade e a confidencialidade do pedido e a fiabilidade dos dados transmitidos*», no âmbito da troca de informação sobre detidos/suspeitos/arguidos relativamente aos quais se impõe a respectiva extradição, de Moçambique para outros Estados e vice-versa.

Apesar da existência de instrumentos legais, anteriormente referidos, ressalta-nos afirmar que ainda há fragilidade no Ordenamento Jurídico moçambicano. Nessa alusão, o País ainda não está preparado para assegurar a segurança jurídica necessária para a sociedade mediante os ataques dos criminosos no âmbito virtual. Assim, há uma insuficiência ou ausência de norma penal tipificando, de forma precisa, os crimes digitais, o que limita a função punitiva estatal, uma vez que influencia na sensação de insegurança e impunidade, com repercussão negativa para a sociedade e, em especial, para a comunidade internacional, que há mais de uma década vem chamando a atenção para a necessidade e urgência de controlo e prevenção de condutas delituosas no ciberespaço:

1. A legislação moçambicana ainda não contempla Disposições Específicas da prova digital no âmbito dos meios de obtenção de prova como sejam a conservação expedita de dados informáticos; Pesquisa de dados informáticos, Apreensão de dados informáticos e Injunção para apresentação ou concessão do acesso a dados, o que dificulta as investigações;
2. Moçambique ainda não ratificou ainda a Convenção de Budapeste, que facilitaria a cooperação internacional e a recolha de obtenção de prova digital;
3. Falta de equipamento tecnológico adequado para os profissionais de justiça criminal bem como a falta de pessoal qualificado em matéria de criminalidade informática.

Desse modo, a legislação moçambicana tem dificuldade em acompanhar a evolução tecnológica, pois a cada dia surge um novo delito nesse ambiente, do qual o legislador não é capaz de caminhar em paralelo com essas evoluções, e consequentemente os crimes virtuais não recebem as devidas punições, deixando a sensação de impunidade.

Nesta perspectiva, aferimos que o crime digital não tem ganho a devida atenção, sendo tipificado por apenas algumas leis, sendo que, outras não são específicas para o devido tema. Por essa razão, é necessário chamar a atenção para este ambiente, expondo uma série de meios que permitam enxergar novas percepções sobre este problema que vem, a internet, embora tenha trazido benefícios, trouxe sérios prejuízos como a criminalidade virtual. Desta feita, a legislação deve acompanhar essa evolução tecnológica com novos estudos, buscando solução para esses conflitos virtuais.

Ficou demonstrado que fazer face a este fenómeno não é fácil e apenas consegue-se com uma cooperação internacional das entidades que investigam estes crimes, permitidas pelas legislações nacionais, já harmonizadas e em consonância. Entretanto, o ser humano está, a cada dia que passa, mais dependente da tecnologia, a legislação deve atender as necessidades dos usuários através de leis regulamentadoras do espaço virtual e tornar competentes os profissionais que estão trabalhando com o combate desses crimes, criando mecanismos para a segurança dos usuários, entre outros. Portanto, a legislação deve cursar o caminho junto com a evolução virtual, o Cibercrime nunca irá desaparecer, mas pode ser prevenido e combatido se a sociedade for instruída neste sentido.

5.2. Políticas Implementadas no âmbito do Combate e Prevenção dos Crimes Cibernéticos em Moçambique

5.2.1. No Âmbito da Política de Segurança Cibernética em Moçambique

A Política Nacional de Segurança Cibernética e sua Estratégia de Implementação foi aprovada pelo Conselho de Ministros a 30 de Agosto de 2021, um dos assuntos abordados no Fórum de Governação da Internet em Moçambique - 2022, pelo seu impacto na busca de soluções para a protecção do cidadão, dos activos de informação e das infra-estruturas críticas no espaço cibernético[568].

[568] CARLOS, Soares, ***Uma visão panorâmica sobre o sistema cibernético e suas políticas***, Vol. III, Atlas Editora, Brasil, 2011.p. 234.

A política de segurança cibernética tornou-se uma necessidade básica para o desenvolvimento sustentável da economia, bem como para a melhoria da qualidade de vida dos moçambicanos. O Governo de Moçambique tem a questão da segurança cibernética como uma das suas prioridades. Nisso, pela Resolução n.º 69/2021 de 31 de Dezembro, o Governo Moçambicano aprovou a Política de Segurança Cibernética e Estratégia da sua Implementação, com vista a adequá-la aos instrumentos orientadores e aos desafios impostos pelo crescente progresso das Tecnologias de Informação e Comunicação (TIC's).

Com a Política pretende-se demonstrar o compromisso crescente do Estado Moçambicano e do seu Governo com a segurança cibernética a nível nacional, regional e continental e global, e em particular com o aumento da consciência da sociedade sobre a importância das diferentes dimensões de segurança cibernética e o nível de envolvimento do País no desenvolvimento e na segurança do espaço cibernético.

De acordo com a Política, a questão de segurança cibernética está enquadrada na defesa e Segurança Nacional através do Conselho Nacional de Segurança Cibernética, estabelecendo uma ponte entre a segurança nacional e a governação cibernética.[569]

A Política é um instrumento, parte da materialização da Política para a Sociedade de Informação, aprovada por Resolução n.º 17/2018, de 21 de Junho, que visa orientar os esforços de Moçambique na resolução dos novos problemas trazidos pela revolução tecnológica, que passa por acções que garantam:

- A regulamentação de funcionamento do espaço cibernético;
- O desenvolvimento de capacidade institucional e operacional em matéria de segurança cibernética;
- A protecção de infra-estruturas críticas e activos de informação;
- O ordenamento da coordenação e colaboração institucional em matéria de segurança cibernética;
- A promoção de boas práticas no uso das TIC's.

A estratégia de implementação da Política, baseia-se na adaptação da legislação, que deve acompanhar o aprimoramento das capacidades da justiça criminal, desde o estabelecimento de unidades especializadas em investigação de crimes cibernéticos e computação forense, até ao fortalecimento da aplicação da lei e formação judicial, cooperação

[569] MUCHANG, José, ***Internet em Moçambique,*** Centro de Informática Universidade Eduardo Mondlane (CIUEM) – Maputo, Moçambique, 2006.p. 67.

entre interagências, investigações financeiras, protecção à criança e cooperação público-privada e internacional[570].

A Política prevê um total de 25 iniciativas através das quais serão implementadas várias acções que concorrem para a materialização em alinhamento com os seguintes pilares:[571]

- Liderança e Coordenação;
- Protecção de Infra-estruturas Críticas de Informação;
- Quadro Legal e Regulatório;
- Protecção de activos de informação;
- Desenvolvimento de Capacidade, Pesquisa e Inovação;
- Cultura de Segurança Cibernética e de Consciencialização.

Todas as iniciativas previstas concorrem para a melhoria da avaliação do País de acordo com os indicadores internacionais de segurança cibernética, bem como para a promoção de uma imagem de um país seguro e atractivo ao investimento.[572]

A aprovação da Política de Segurança Cibernética, tem em vista a dar resposta aos problemas sentidas na presente era digital coloca países de todo o mundo perante um novo conceito de segurança, o de segurança cibernética, que deve ser encarado com responsabilidade e envolvimento de todas as forças vivas da sociedade, para que Moçambique possa tirar o melhor proveito do espaço cibernético.

Para efeitos do presente documento entende-se por espaço cibernético ao ambiente complexo, de valores e interesses, materializado numa área de responsabilidade colectiva, que resulta da interacção entre pessoas, redes e sistemas de informação, e por segurança cibernética ao conjunto de medidas e acções de prevenção, monitorização, detecção, reacção, análise e correcção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no espaço cibernético, e das pessoas que nele interagem[573].

A segurança cibernética inclui todas as medidas legais, tecnológicas e processos que visam proteger pessoas, colectivas e singulares, e bens, com destaque para as infra-estruturas críticas de informação, no espaço cibernético. A PENSC vai ao encontro dos anseios dos

---

[570] MARCELINO, H, ***Dimensão de Defesa e Segurança Cibernética, Caso de Moçambique". (Dissertação de mestrado)***, Instituto Superior de Estudos de Defesa "Armando Emílio Guebuza" – Maputo, Moçambique. 2014.p. 215.

[571] MANDARINO, Rafael, ***Segurança e defesa do espaço cibernético brasileiro***, Recife: CUBZAC, 2010.p. 166.

[572] KISSINGER, Henry. ***Ordem mundial***. Tradução Cláudio Figueiredo. 1. ed. Rio de Janeiro: Objectiva, 2015.p. 189.

[573] Cfr. ***Resolução nº 69/2021 de 31 de Dezembro***.

moçambicanos no sentido de criarem uma visão nacional que lhes permita desenvolverem uma plataforma comum de resiliência a ataques cibernéticos ou a quaisquer outras formas de perturbação da ordem pública, com recurso às Tecnologias de Informação e Comunicação (TIC) [574].

As preocupações com a segurança cibernética vêm se avolumando desde que o país decidiu enveredar pela massificação do uso das TIC`s, quando o Governo aprovou a primeira Política de Informática, através da Resolução número 28/2000, de 12 de Dezembro, que 18 anos depois foi revista e aprovada sob a nova perspectiva de Política para a Sociedade da Informação, através da Resolução nº 17/2018, de 21 de Junho[575].

A Política e Estratégia Nacional de Segurança Cibernética (PENSC) é um instrumento parte da materialização da Política para a Sociedade de Informação que vai orientar os esforços de Moçambique na resolução dos novos problemas trazidos pela revolução tecnológica, que passa por acções que garantam como a regulamentação de funcionamento do espaço cibernético, o desenvolvimento de capacidade institucional e operacional em matéria de segurança cibernética. A protecção de infra-estruturas críticas e activos de informação, o ordenamento da coordenação e colaboração institucional em matéria de segurança cibernética.

A PENSC complementa uma série de outros instrumentos orientadores e regulatórios do sector das TIC`s que foram sendo aprovados e implementados pelo Governo ao longo dos últimos anos, dos quais se destacam: a Política para a Sociedade da Informação; a Lei de Transacções Electrónicas, Lei n.º 3/2017, de 9 de Janeiro; a Lei de Telecomunicações;[576] Lei n.º 4/2016, de 3 de Junho; o Regulamento do Quadro de Interoperabilidade de Governo Electrónico, o Decreto nº 67/2017, de 1 de Dezembro[577]; o Regulamento de Segurança de Redes de Telecomunicações, Decreto n.º 62/2019, de 1 de Agosto[578]; o Regulamento do Sistema de Certificação Digital de Moçambique, Decreto n 59/2019, de 1 de Dezembro; o Regulamento do Domínio[579] "mz", Decreto n.º 82/2020, de 10 de Setembro; a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais, Resolução n.º 5/2019, de 20 de Junho e

[574] Cfr-***Resolução nº 69/2021 de 31 de Dezembro***.
[575] Cfr., ***Resolução 69/2021 de 31 de Dezembro***.
[576] Cfr., Lei n.º 3/2017, de 9 de Janeiro***, aprova a Lei de Transacções Electrónicas***,
[577] Cfr., O Regulamento do Quadro de Interoperabilidade de Governo Electrónico (Decreto n 67/2017, de 1 de Dezembro).
[578] Cfr., Decreto n.º 62/2019 de 1 de Agosto***, aprova o Regulamento de Segurança de Redes de Telecomunicações***
[579] Cfr., Resolução n.º 5/2019 de 20 de Junho, ***rectifica a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais*** *in* Boletim da República.

as recentes[580] iniciativas legislativas no que se refere ao Código Penal, que, de um modo geral, permitiram dar cobertura universal aos crimes de natureza informática no país[581].

A 14ª Sessão Ordinária da Cimeira dos Chefes de Estado e de Governo da União Africana, sobre as TIC`s em África realizada sob o lema Desafios e Perspectivas para o Desenvolvimento, orientou cada Estado membro a elaborar uma Política Nacional de Segurança Cibernética que reconheça a importância da Infra-estrutura da Informação Crítica (IIC), identificar os riscos que enfrenta e definir a forma de alcançar os objectivos dessa política.

O trabalho de preparação da presente Política e Estratégia Nacional de Segurança Cibernética (PENSC) enquadra-se não só nas orientações emanadas na 14.ª Sessão Ordinária da Cimeira dos Chefes de Estado e de Governo da União Africana, sobre as TIC, mas também no cumprimento do artigo 24 da Resolução n° 5/2019, de 20 de Junho, Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais, que recomenda os Estados membro a estabelecerem um quadro regulamentar composto pela política e estratégia nacional de segurança cibernética que visam definir, coordenar e implementar iniciativas e prioridades relativas a protecção das instituições, pessoas e bens contra incidentes decorrentes do uso das TIC no espaço cibernético[582].

Todas as iniciativas que constam da PENSC concorrem para a melhoria da avaliação do país nos indicadores internacionais de segurança cibernética, bem como para a promoção de uma imagem de um país seguro e atractivo ao investimento.

A PENSC é um instrumento chave que o país precisa para melhor definir e coordenar as iniciativas e prioridades no âmbito da utilização segura das TIC`s, a fim de proteger instituições públicas e privadas, pessoas e bens contra-ataques cibernéticos, em alinhamento com as convenções regionais e internacionais.

Há exemplos de muitos países, que têm vindo a adoptar leis, políticas e estratégias que promovem o uso e o desenvolvimento de Tecnologias de Informação e Comunicação (TIC) por reconhecer que estas, têm um papel importante como catalisadoras dos processos de modernização e transformação digital, pois servem de plataformas de suporte em várias áreas de desenvolvimento económico e social como a agricultura, educação, saúde, energia, turismo, exploração de recursos naturais, economia e finanças, de entre outras[583].

---

[580] Cfr., Resolução n.º 5/2019 de 20 de Junho, ***rectifica a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais***.
[581] Cfr., Resolução 69/2021 de 31 de Dezembro.
[582] Cfr., Resolução 69/2021 de 31 de Dezembro.
[583] NETO, Filomeno, ***ob., cit.,*** p. 236.

O espaço cibernético promove mercados abertos e sociedades abertas catapultando o desenvolvimento das nações. Porém, essa mesma abertura também pode tornar os internautas mais vulneráveis a criminosos, serviços de contra-inteligência de entidades estrangeiras e outros tipos de ataques cibernéticos com vista a prejudicar, comprometer ou danificar as infra-estruturas críticas e activos de informação no geral e a integridade do cidadão e do Estado em particular[584].

A Política Nacional de Segurança Cibernética e a sua Estratégia de Implementação (PENSC) visam mitigar os efeitos dos ataques e incidentes cibernéticos no nosso país. Dados de base multiplicam-se no país nos últimos anos o assédio e abuso no espaço cibernético, a propagação de informação falsa, as burlas, o roubo de identidade, crimes financeiros, o ciberterrorismo e outros crimes informáticos[585].

Estes actos afectam a vida económica e social, para preocupação das autoridades que têm que lidar com matérias de garantia da segurança e da soberania nacional e que devem tralhar no sentido de garantir um espaço digital credível para a protecção das infra-estruturas críticas de informação, da privacidade e das liberdades do cidadão e para o combate ao crime cibernético[586].

A situação do País, no contexto da segurança cibernética, o referencial geográfico do espaço cibernético compreende uma área de 801.537 quilómetros quadrados do território nacional e os seus 2.770 quilómetros da costa marítima, onde vivem actualmente cerca de 30 milhões de habitantes, segundo as projecções do último censo populacional, realizado em 2017[587].

Cerca de 66% desta população está concentrada nas zonas rurais, dominadas por solos aráveis, bacias hidrográficas, recursos minerais e energéticos, em quantidades consideráveis. Moçambique, país detentor de enormes reservas de gás natural na sua plataforma marítima continental, pode vir a tornar-se, a médio prazo, um dos maiores exportadores de hidrocarbonetos, capitalizando os ganhos na recuperação e desenvolvimento socioeconómico, em benefício das suas populações[588].

---

[584] Cfr., Resolução 69/2021 de 31 de Dezembro.
[585] MUCHANG, José, ***ob., cit.,*** p. 234.
[586] MATUSSE, R.,. ***História da Informática em Moçambique***, Mozambique Acácia Advisory Committee Secretariat. Universidade Eduardo Mondlane, Maputo, 2003.p. 118.
[587] Cfr., Resolução 69/2021 de 31 de Dezembro.
[588] Cfr., Resolução 69/2021 de 31 de Dezembro.

Os esforços de recuperação e desenvolvimento nacional têm sido contrariados, porém, pelos efeitos negativos das mudanças climáticas, que, ciclicamente, vem afectando de forma negativa o crescimento do Produto Interno Bruto (PIB) do país.[589].

O Relatório da União Internacional de Telecomunicações (UIT) sobre o Índice Global de Segurança Cibernética (GCI) de 2018 colocou Moçambique entre os países com o pior nível de Segurança Cibernética, com base na análise das seguintes categorias:

- Medidas legais;
- Medidas técnicas;
- Medidas organizacionais
- Desenvolvimento de capacidades;
- Cooperação internacional.

É por esta razão que, num ranking de 194 países, Moçambique ocupou as posições 26 e 132, no índice continental e global respectivamente. No Relatório do Índice Global de Segurança Cibernética de 2020, divulgado pela União Internacional de Telecomunicações (UIT), agência do sector de tecnologias da ONU, Moçambique subiu 9 posições, tendo passado da posição 132 em 2018 para a posição 123, numa lista com 193 países avaliados[590].

O Índice Global de Segurança Cibernética da UIT avalia as acções que os países empreendem com o objectivo de fomentar a consciencialização sobre os compromissos das nações em relação a segurança cibernética e identificar os pontos fortes e as áreas onde são necessárias melhorias, além de partilhar as boas práticas de segurança cibernética[591].

A posição conquistada pelo nosso país nos dois últimos relatórios da UIT do Índice Global de Segurança Cibernética demostra o compromisso crescente de Moçambique e do Governo com a segurança cibernética a nível nacional, regional, continental e global, em particular com o aumento da consciência da sociedade sobre a importância das diferentes dimensões de segurança cibernética e o nível de envolvimento do país no desenvolvimento e na segurança do espaço cibernético. Um importante indicador socioeconómico normalmente usado para avaliar os países é o Índice do Desenvolvimento Humano (IDH).

---

[589] MUCHANG, José, ***Internet em Moçambique,*** Centro de Informática Universidade Eduardo Mondlane (CIUEM) – Maputo, Moçambique, 2006.p. 265.
[590] Cfr., Resolução 69/2021 de 31 de Dezembro, ***aprova a política de segurança cibernética e a estratégia de sua implementação,*** *in* Boletim da República, I série, número 253 de 31 de Dezembro.
[591] ibidem.

Em 2020 Moçambique reduziu uma posição, tendo passado da posição 180º para 181º numa lista com 189 Estados membros das Nações Unidas avaliados, do total dos 193 Membros das Nações Unidas[592].

O outro instrumento importante é o indicador de negócios, o *Doing Business*. Moçambique continua com índices de desempenho baixos no *Doing Business*, pois no ranking global de 2020, que avaliou 189 países, o país reduziu três posições, tendo passado da posição 135º em 2019 para a posição 138º em 2020. O Relatório do *Doing Business* de 2000, uma das principais publicações do Banco Mundial, é a 17ª edição de um estudo anual que avalia como as leis e instrumentos legais promovem ou restringem as actividades empresariais[593].

A Decisão do Conselho Executivo da União Africana que aprovou a Estratégia de Transformação Digital para África solicitou à Comissão da União Africana para desenvolver a sua matriz de implementação que preconize o desenvolvimento de uma sociedade digital e económica inclusiva em África.

A Estratégia está alinhada com as cinco áreas transversais da Estratégia de Transformação digital para África (2020-2030), concretamente no que concerne ao tema de segurança cibernética e protecção de dados pessoais[594].

A PENSC é um importante instrumento orientador da governação, não só porque foi preparada para atender aos anseios dos moçambicanos no domínio de segurança cibernética, mas porque concorre para que o país se conforme com uma das grandes preocupações de actualidade em todo o mundo no âmbito do desenvolvimento da Sociedade Global da Informação[595].

O uso das TIC`s e a crescente digitalização de serviços no nosso país tem resultado em profundas transformações económicas, sociais e culturais, bem como em substanciais melhorias de governação e da vida das populações.

Para avaliar o nível de desenvolvimento e utilização das TIC`s entre países é usado o estudo comparativo designado Índice de Desenvolvimento das TIC`s (IDI - ICT *Development Index*), que mostra a situação de cada país nos diferentes aspectos de uso das TIC`s nas áreas prioritárias de desenvolvimento social e económico como a educação, a saúde, a agricultura, energia, turismo, dentre outras[596].

---

[592] ibidem.
[593] Ibidem.
[594] Cfr., Resolução 69/2021 de 31 de Dezembro.
[595] Cfr., Resolução 69/2021 de 31 de Dezembro.
[596] Ibidem.

No último Relatório do Índice de Desenvolvimento das TIC`s (IDI - ICT *Development Index*) publicado em 2017 Moçambique ficou na posição 150, tendo reduzido três posições relativamente a 2016, num ranking de 176 países, apesar dos esforços que o Governo tem feito para investir em infra-estruturas, promoção do acesso e disseminação do uso de TIC[597].

A face mais visível do impacto da digitalização da economia nacional, para a maioria da população, sobretudo nas zonas rurais e outras classes menos favorecidas, é a dos serviços de dinheiro móvel, nomeadamente as plataformas *Mkesh*, Mpesa e e-Mola, entre outras formas de transacção electrónica a nível dos produtos e serviços financeiros básicos como o pagamento de água e de electricidade. O Governo de Moçambique, consciente desta situação, desenvolveu a Estratégia Nacional de Inclusão Financeira (2016- 2022), que se enquadra na Estratégia do Desenvolvimento do Sector Financeiro[598].

Um dos enfoques chave desta estratégia está no aumento da acessibilidade a serviços financeiros pela população, especialmente nas áreas rurais. O serviço de dinheiro móvel é um dos canais que está a ser mais usado para se acelerar a inclusão financeira oferecendo uma alternativa aos serviços financeiros formais. Com os serviços de dinheiro móvel, mais moçambicanos anteriormente excluídos do ponto de vista financeiro obtiveram acesso a serviços através de plataformas digitais de serviços de dinheiro móvel.[599]

No que tange a inclusão digital, importa realçar a expansão das praças digitais, que permitem o acesso grátis à Internet. Como resultado, até meados de 2020, tinham sido instaladas ao todo 69 praças digitais em diferentes regiões do país. O serviço de telefonia móvel atingiu em 2019 14,908,191 assinantes, uma cobertura que aproxima o país das tendências regionais e mundiais, em termos de acesso à telefonia. [600]

O indicador inclui o número de assinantes pós-pagos e o número de assinantes pré-pagos activos e aplica-se a todos os assinantes de telefonia móvel que oferecem comunicações de voz. Exclui assinantes via cartões de dados ou modens USB e assinantes de serviços públicos de dados móveis.[601]

A nível da educação, no ensino superior e no ensino técnico em particular, há a registar o estabelecimento da Rede de Instituições de Ensino Superior e de Investigação de

---

[597] KISSINGER, Henry. ***Ordem mundial***. Tradução Cláudio Figueiredo. 1. ed. Rio de Janeiro: Objectiva, 2015.p. 256.
[598] Cfr., Resolução 69/2021 de 31 de Dezembro.
[599] Cfr., Resolução 69/2021 de 31 de Dezembro.
[600] DIAS, Donaldo de Souza; SILVA, Mónica Ferreira da, ***Como escrever uma monografia: manual de elaboração com exemplares e exercícios***, 1. ed. São Paulo: Atlas, 2010.p.146.
[601] Cfr., Resolução 69/2021 de 31 de Dezembro.

Moçambique, a MoRENet (Mozambique *Research and Education Network*), que em finais de 2020 interligava 180 instituições de ensino superior, de ensino técnico profissional e de investigação distribuídas por todas as províncias do país, disponibilizando os serviços digitais aos membros das comunidades académica científica assentes nas diversas aplicações de plataformas digitais de apoio aos processos de ensino e aprendizagem e de gestão académica e pedagógica. Houve progressos também no processo de migração digital, que permitiu a televisão passar a transmitir de forma digital ou satélite.

5.2.1.1. Pilares da Política

Os pilares que sustentam a PENSC são cinco, a saber:

a) Liderança e Coordenação: estabelecer um Mecanismo Nacional de Promoção, Partilha, Cooperação e Coordenação em Matérias de Segurança Cibernética.

b) Protecção de Infra-estruturas Críticas de Informação (ICI): o objectivo deste pilar é a identificação e protecção das ICI e toda sua envolvente cobrindo sistemas, dispositivos, processos e pessoas, para garantir que não sejam afectadas, e, consequentemente, também a segurança territorial, a estabilidade política, económica e social do país, assim como a reputação das instituições e dos cidadãos. A responsabilidade de protecção destas infra-estruturas recai a todos os actores da PENSC, através de aplicação de medidas de detecção, prevenção e observância da legislação aplicável.

O objectivo deste pilar é a protecção de informação e aplicações, através de estabelecimento de programas de certificação de qualidade e segurança das aplicações e infra-estruturas, mecanismos de controlo de acessos, estratégias de protecção da confidencialidade, integridade e disponibilidade da informação, regulamentos de protecção de informação, adopção de soluções tecnológicas de protecção e de resiliência de sistemas e Activos de Informação, assim como de realização de auditorias e avaliação dos níveis de maturidade no âmbito de segurança cibernética.

A informação constitui um importante recurso para o desenvolvimento, segurança e defesa das nações, e qualquer impedimento ao acesso ou destruição podem pôr em causa a confiança de cidadãos ou interesses particulares, inclusive a soberania de um país. Por isso, devem ser implementadas medidas contra situações de ameaças às liberdades individuais, aos dados pessoais e, em suma, à privacidade, confidencialidade e integridade de dados.[602]

[602] Cfr., ***Resolução 69/2021 de 31 de Dezembro***.

c) Quadro Legal e Regulatório: o objectivo deste pilar é desenvolver um quadro legal e regulatório capaz de harmonizar as práticas a nível nacional, regional e internacional, simplificar e efectivar o combate a crimes cibernéticos, proporcionando segurança jurídica no ciberespaço. Nesta perspectiva, o quadro jurídico-administrativo deve ser melhorado para facilitar a actuação das autoridades, identificação, investigação, esclarecimento e aplicação de medidas em casos de contravenção.

d) Desenvolvimento de Capacidade, Pesquisa e Inovação: o objectivo deste pilar está focado em acções voltadas para a criação e fortalecimento das capacidades organizacionais, dos recursos humanos e tecnológicos, consciencialização, promoção da pesquisa e inovação. Para o alcance deste objectivo, devem ser desenvolvidos programas de formação técnica, capacitação, certificação, consciencialização, promoção de pesquisa e inovação, de modo que a sociedade, a academia, os sectores público e privado disponham **dos recursos necessários para actuarem no ciberespaço.**[603]

e) Cultura de Segurança Cibernética e Consciencialização: o objectivo é tornar o cidadão cada vez mais consciente de ameaças e riscos cibernéticos. Por isso, devem ser desenvolvidos programas de consciencialização para transmitir as boas práticas de uso das TIC`s, que possam contribuir para a redução de exposição a riscos de incidentes cibernéticos[604].

5.2.1.2. Factores Críticos de Sucesso na Implementação da PENSEC

A implementação bem-sucedida da PENSEC dependerá amplamente ou será influenciada pelos seguintes factores: a liderança a alto nível é fundamental uma liderança política ao mais alto nível, comprometida com a segurança cibernética nacional. Ela é assegurada pelo mecanismo de orientação política coordenado pelo Conselho Nacional de Segurança Cibernética. Portanto, a liderança política constitui o factor crítico principal para o sucesso da PENSC, porque cabe a ela garantir a sua coordenação, articulação, motivação e integração de esforços para a estratégia de implementação.[605]

O Capital humano a implementação eficiente da segurança cibernética requer recursos humanos altamente qualificados em todos os sectores da sociedade. A capacidade das instituições do sector público e privado de obter e reter recursos humanos qualificados é,

---

[603] Cfr., ***Resolução 69/2021 de 31 de Dezembro***.
[604] Cfr., Resolução 69/2021 de 31 de Dezembro.
[605] MARCELINO, H, ***Dimensão de Defesa e Segurança Cibernética, Caso de Moçambique". (Dissertação de mestrado)***, Instituto Superior de Estudos de Defesa "Armando Emílio Guebuza" – Maputo, Moçambique. 2014.p.156.

portanto, importante para manter e garantir uma forte abordagem de protecção contra ameaças cibernéticas, especialmente com operadores de Infra-estrutura crítica, assim sendo é extremamente importante que o Governo invista na formação do capital humano.[606]

A Coordenação e colaboração o Sincronismo das acções entre os diversos sectores deve ser assegurado, para que no final o conjunto de todas acções garantam a implementação efectiva.

No nosso entendimento esse sincronismo é vital, na medida em que a garantia da segurança cibernética ser somente possível se houver acções transversais em todos os sectores. A natureza do espaço cibernético é sem fronteiras e complexa; isso implica que a gestão de riscos seja uma responsabilidade partilhada[607].

Vários actores importantes além do governo de Moçambique, incluindo operadores de infra-estruturas críticas, sector público, sector privado, academia, sociedade civil e cidadãos, devem partilhar essa responsabilidade com base em colaboração harmoniosa. A colaboração internacional é essencial para garantir a presença de capacidade e mecanismos para lidar com ameaças cibernética sem fronteiras, além de fornecer assistência a aliados internacionais quando necessário.

A capacidade de criar confiança e relacionamentos com os principais interessados (indústria, organizações internacionais de segurança cibernética e Estados soberanos) é importante devido ao facto de que as ameaças cibernéticas abrangerem várias jurisdições a monitoria: de forma a regular a implementação da PENSC é necessária uma monitorização constante das acções realizadas por todas partes envolvidas. A supervisão da conformidade de todas as principais partes interessadas e actores do sector público e privado fornece garantia para melhorar a maturidade de segurança cibernética do país. Isso requer esforço e iniciativa deliberada de cada parte interessada para cumprir com as suas obrigações[608].

É necessária uma coordenação adequada dos esforços com o objectivo de realizar as actividades relacionadas com segurança cibernética entre os sectores e garantir que soluções a nível nacional e sectorial sejam coordenadas. Para o sucesso da implementação da presente estratégia, tornasse crucial a adopção de directrizes emanadas por órgãos nacionais, regionais e internacionais[609].

---

606 KISSINGER, Henry, ***Ordem mundial***. Tradução Cláudio Figueiredo. 1. ed. Rio de Janeiro: Objectiva, 2015.p.445.
607 MANDARINO, Rafael, ***Segurança e defesa do espaço cibernético brasileiro***, Recife: CUBZAC, 2010.p. 156.
608 Cfr., Resolução 69/2021 de 31 de Dezembro.
609 CARLOS, Soares, ***Uma visão panorâmica sobre o sistema cibernético e suas políticas***, Vol. III, Atlas Editora, Brasil, 2011

Os recursos financeiros são uma importante componente da PENSC, sem a qual não será possível alcançar os objectivos pretendidos na sua plenitude. Trata-se de um factor crítico-chave que merecerá uma maior atenção na implementação da política, para que uma grave lacuna financeira não ponha em causa a soberania cibernética do país. 3. Estratégia de implementação. A presente estratégia tem um horizonte de 5 anos, e está alinhada com as cinco áreas transversais da Estratégia de Transformação Digital de África (2020-2030), concretamente no que concerne ao tema de segurança cibernética e protecção de dados pessoais.[610]

Neste contexto, a PENSC é um importante instrumento orientador da governação, não só porque satisfaz os anseios dos moçambicanos no domínio cibernético, mas também porque conforma o país com uma das grandes preocupações de actualidade em todo o mundo, no âmbito da Sociedade Global da Informação.[611]

Os projectos e iniciativas da estratégia de implementação da política de segurança cibernética foram definidos em alinhamento com os pilares da PENSC, associando a cada um deles parte das vinte e cinco (25) iniciativas através das quais serão implementadas várias acções que concorrem para a materialização dos seus objectivos específicos.

5.2.1.3. Os Desafios na Implementação da Política de Segurança Cibernética em Moçambique

Infra-estrutura Tecnológica Limitada - a falta de infra-estrutura tecnológica avançada em algumas regiões dificulta a implementação eficaz de medidas de segurança cibernética.[612]

Conscientização e Educação - níveis variados de conscientização sobre segurança cibernética entre os usuários, destacando a necessidade de programas educacionais abrangentes.

Escassez de Profissionais Qualificados - carência de especialistas em segurança cibernética em Moçambique é um desafio significativo para o desenvolvimento e execução de estratégias eficazes.

Ameaças Cibernéticas Emergentes - a rápida evolução das ameaças cibernéticas, como ataques de *ransomware* e *phishing*, representa um desafio constante para a actualização das defesas.[613]

[610] Cfr., Resolução 69/2021 de 31 de Dezembro.
[611] MANDARINO, Rafael, ***Segurança e defesa do espaço cibernético brasileiro***, Recife: CUBZAC, 2010.p. 537.
[612] MARCELINO, H, ob., cit. p. 178.
[613] MARCELINO, H, ob., cit. p. 178.

Cooperação Internacional Limitada - a falta de colaboração eficaz com organizações internacionais e outros países pode limitar a capacidade de combater ameaças cibernéticas transfronteiriças.[614]

Regulamentação e Legislação Deficiente - a ausência de leis e regulamentos específicos em segurança cibernética pode dificultar a aplicação de medidas de conformidade e responsabilização[615].

Orçamento Restrito - recursos financeiros limitados para investir em tecnologias de segurança e programas de treinamento podem comprometer a eficácia das políticas de segurança cibernética[616].

Protecção de Dados Pessoais - a necessidade de desenvolver e aplicar medidas robustas para proteger dados pessoais em conformidade com padrões internacionais[617].

Ambiente Empresarial em Crescimento - o rápido crescimento do sector empresarial em Moçambique pode criar desafios adicionais na implementação de políticas de segurança cibernética em todas as empresas

Falta de Estratégias de Resposta a Incidentes - ausência de planos de resposta a incidentes coordenados pode resultar em tempos de recuperação mais longa após ataques cibernéticos.

Inclusão Digital Desigual - disparidades na inclusão digital entre áreas urbanas e rurais podem criar lacunas significativas na aplicação de políticas de segurança cibernética em todo o país.

Monitoramento e Fiscalização insuficientes - a falta de mecanismos eficazes de monitoramento e fiscalização podem permitir a proliferação de actividades cibernéticas maliciosas.

A superação desses desafios requer um compromisso contínuo do governo, sector privado e sociedade civil em Moçambique. A colaboração, investimento em educação e treinamento, bem como a modernização da legislação são elementos cruciais para fortalecer a postura de segurança cibernética do País.

5.3. Categorias de Crimes Informáticos/Cibernético no Direito Penal Moçambicano

[614] Idem. p. 176,
[615] Idem, p. 178.
[616] Idem. p. 179.

Em conformidade com Rossini, o conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele e que ofenda, directa ou indirectamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade"[618].

A doutrina aponta a existência de diversos tipos de ataques perpetrados por criminosos no universo virtual, configurando alguns dessas figuras tipicamente previstas na lei. Porém, a doutrina é unânime em apontar os seguintes crimes:

> "No Brasil, o crime mais comummente cometido pela internet trata-se do roubo de identidade. De igual modo, afere-se a usual ocorrência de furtos de dados (arquivos) pessoais, crimes relacionados à pedofilia e materiais pornográficos contendo crianças e adolescentes, actos ofensivos à honra de outrem (calúnia, injúria, difamação), ameaças, crimes de discriminação e, ainda, a ocorrência de espionagem industrial. De fato, no roubo de identidade e no furto de dados"[619].

Ainda quanto a matéria em discussão, é fundamental trazer um entendimento quanto à tipologia dos crimes cibernéticos. Nessa senda, tem sido avançada a seguinte tipologia, que é unânime na doutrina: os crimes informáticos, no entender de Pacheco[620], dividem-se em puros, mistos e comuns. Porém, Atheniense[621] trata os cibercrimes como crimes virtuais, estabelecendo uma diferenciação entre os delitos informáticos, apenas como puros e impuros:

> Entende-se por crimes virtuais qualquer acção em que o computador seja o instrumento ou o objecto do delito, ou então, qualquer delito ligado ao tratamento automático de dados. Distinguem-se os crimes virtuais entre delitos informáticos impuros, aqueles que podem ser cometidos também fora do universo do computador, encontrando já definição no sistema punitivo actual, e os delitos informáticos puros, ou seja, aqueles que só podem ser concebidos em face de um sistema informático, ainda não tipificados.

Por sua vez, Fiorillo[622] aprofunda mais essa divisão: "Evidencia-se que o crime digital impuro ou impróprio é a utilização do ambiente virtual como um meio para executar o delito, ou seja, o alvo não é o meio virtual ou electrónico em si, mas uma pessoa, retirar dinheiro de uma conta bancária, fraudar dados, entre outros". O que não acontece no crime digital puro ou próprio. Neste tipo de crime, "o criminoso tem o escopo de causar dano à máquina, ambiente virtual ou até mesmo invadir o sistema de uma determinada pessoa, seja ela física ou jurídica, sem autorização deste e não levando nenhum tipo de informação dali".

---

618 ROSSINI, Augusto Eduardo de Souza, ***Informática, telemática e direito penal*.** 1. Ed. São Paulo: Memória Jurídica, 2004. p. 67.
619 SALES, Marco. Ob., cit., p. 42.
620 PACHECO, Gisele Freitas, ***Crimes virtuais e a legislação penal brasileira*.** p. 7.
621 ATHENIENSE, Alexandre, ***Crimes virtuais: soluções vigentes e projetos de lei***. 2000.
622 FIORILLO, Celso Antônio Pacheco, ***Crimes no meio ambiente digital***. 1 Ed. São Paulo: Saraiva, 2013. p. 167.

Fazendo um respaldo na nossa esfera jurídico-penal (Código Penal, aprovado pela Lei n.º 24/2019, de 24 de Dezembro), estão configurados como os crimes de "devassa da vida privada" (art. 252), "base de dados automatizada" (art. 254), "acesso Ilegítimo" (art. 256), "gravações ilícitas" (art. 257), "burla informática e nas comunicações" (art. 289), "fraudes relativas aos instrumentos e canais de pagamento electrónico" (art. 294); chama-se também à colação de determinadas formas de cometimento dos crimes de "difamação" (art. 233) e "injúria" (art. 234), na parte em que a Lei se refere à «qualquer outro meio de publicação»; a secção do CP respeitante à "falsidade informática e crimes conexos", nos quais se incluem os crimes de "falsidade informática" (art. 336), "interferência em dados" (art. 337), "interferência em sistemas" (art. 338), "uso abusivo de dispositivos" (art. 339).

1. Devassa da vida privada (art. 252 do CP)

Tendo por objecto de protecção o bem jurídico a "reserva da intimidade da vida privada", nos termos do art. 41 da CRM[623], encontra-se previsto no art. 252 do CP. O tipo criminal em questão envolve a conduta de, sem consentimento e com intenção de devassar a vida das pessoas, designadamente a intimidade da vida familiar ou sexual, por exemplo, captar, fotografar, filmar, registar ou divulgar imagens das pessoas ou de objectos ou espaços íntimos, trata-se de um crime semipúblico, ou seja, o respectivo procedimento criminal depende da apresentação da queixa.

2. Base de dados automatizada (art. 254 do CP),

Para o cometimento do crime de base de dados automatizada, previsto no art. 254 do CP, o infractor, sem consentimento, cria, mantém ou utiliza ficheiro automatizado de dados individualmente identificáveis e relativos às convicções políticas, filosóficas ou ideológicas, à fé religiosa, à filiação partidária ou sindical e à vida privada. É um crime cujo objecto visa proteger a reserva da intimidade da vida privada. Decorrente, disso é um crime semipúblico.

3. Acesso ilegítimo (acesso sem autorização – artigo 256 do CP)

O desejo de ganhar o acesso sem autorização a sistemas de computador pode ser iniciado por vários motivos. Tal como refere Silva[624], da simples curiosidade em quebrar os códigos de acesso aos sistemas de segurança, até o acesso intencional para causar danos ou cometer outros ilícitos.

[623] "Todo o cidadão tem direito à honra, ao bom nome, à reputação, à defesa da sua imagem pública e à reserva da sua vida privada"
[624] SILVA, R. G, ***Crimes da Informática***, Editora: CopyMarket.com, 2000.

A protecção de contra senha é frequentemente utilizada como um dispositivo protector contra acesso sem autorização, porém, os *hacker´s* modernos podem evitar esta protecção, descobrindo a contra senha que lhe permite o acesso, introduzindo programas específicos para este fim, isto é, quando alguém queira capturar outras senhas de usuários legítimos.[625]

Com o computador é possível produzir muitas realidades, e cada um produz a sua. Pinheiro[626] diz que, no computador, cada um pode assumir muitas faces, pode mascarar-se, desempenhar vários papéis, mudar de raça, sexo, idade, voz, humor e atitudes, assumir muitas identidades, identidades novas, falsas, mutantes. O computador e os jogos computadorizados tornam-se, em parte, substitutos dos parceiros reais.

Esta categoria de delito equipara-se ao delito denominado *Acesso ilegítimo*, que legislação penal Moçambicana, no seu respectivo n.° 1 do art. 256. °, é caracterizado pelo mero acesso ao dispositivo informático alheio com a finalidade de tomar conhecimento de certa informação ou objecto de natureza privada, ou seja, que não sejam públicos.

O infractor nos crimes informáticos, objectivamente previsto no nº 1, do art. 256 do CP (acesso ilegítimo), comete por motivos estritamente pessoais, acedendo ao sistema informático, consultando declarações de ligadas a sua área de trabalho. O tipo subjectivo daquele ilícito penal não exige qualquer intenção específica (como seja o prejuízo ou a obtenção de benefício ilegítimo), ficando preenchido com o dolo genérico de intenção de aceder o sistema. O bem jurídico protegido é a segurança dos sistemas informáticos.

4. Gravações ilícitas (artigo 257 do CP)

Tendo por objecto de protecção, os bens jurídicos «reserva da intimidade da vida privada» e «imagem», protegidos nos termos do art. 41 da CRM[627], o crime de gravações e fotografias ilícitas encontra-se previsto no art. 257 CP. Esta norma tipifica o acto de fotografar, filmar ou captar a voz de pessoa, sem autorização ou sem fins lícitos, prevendo qualificadoras para as diversas formas de sua divulgação. O procedimento criminal depende da queixa do ofendido – pela sua natureza é um crime semipúblico.

5. Burla informática e nas comunicações (artigo 289 do CP)

A Burla informática nas comunicações, previsto no art. 289.° do CP, faz parte da categoria dos crimes informáticos, a acção do infractor manifesta-se quando, "usando de

[625] Ibidem.
[626] PINHEIRO, E. P, ***Crimes virtuais: uma análise da criminalidade informática e da resposta estatal***.
[627] O art. 41 da CM, preceitua que: "Todo o cidadão tem direito à honra, ao bom nome, à reputação, à defesa da sua imagem pública e à reserva da sua vida privada"

programas, dispositivos electrónicos ou outros meios informáticos que separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações, com intenção de obter para si ou para terceiro um benefício ilegítimo, causando a outrem prejuízo patrimonial. Ou ainda, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causando a outra pessoa prejuízo patrimonial"[628].

A burla informática consiste sempre num comportamento que constitui um artifício, engano ou erro consciente, não por modo de afectação directa em relação a uma pessoa (como na burla prevista no art.º 287.º do CP), mas por intermediação da manipulação de um sistema de dados ou de tratamento informático, ou de equivalente utilização abusiva de dados. Mas, prescindindo do erro ou engano em relação a uma pessoa, prevê, no entanto, actos com conteúdo material e final idêntico: manipulação dos sistemas informáticos, ou utilização sem autorização ou abusiva determinando a produção dolosa de prejuízo patrimonial. Por exemplo, nos casos em que um sujeito utiliza indevidamente as máquinas automáticas de pagamento (ATM), incluindo os casos de manipulação ou utilização indevida no sentido de utilização sem a vontade do titular.

A manipulação de dados de uma máquina ATM com o propósito de que a mesma, sem motivo legítimo, ejecte uma grande quantidade de notas, preenche o tipo de crime de burla informática. Na burla informática, a lesão do património produz-se através da intromissão nos sistemas e da utilização em certos termos de meios informáticos - é um crime de resultado, exigindo-se que seja produzido o prejuízo patrimonial de alguém.

6. Fraudes relativas aos instrumentos e canais de pagamento electrónico" (Fraude Informática – artigo 294 do CP)

Esta fraude é utilizada em muitos casos de crimes económicos, como manipulação de saldos de contas, balancetes em bancos, etc., alterando, omitindo ou incluindo dados, com o intuito de obter vantagem económica. A fraude informática é "o crime de computador mais comum, mais fácil de ser executado, porém, um dos mais difíceis de ser esclarecido. Não requer

[628] Cfr., nº 1, do art. 289 do CP.

conhecimento avançado em computação e pode ser cometido por qualquer pessoa que obtenha acesso a um computador"[629].

Podem ocorrer fraudes financeiras através de acesso remoto a contas bancárias. Os ataques fraudulentos às contas são normalmente realizados através de *e-mails* falsos ou do *download* de ficheiros maliciosos, sem que o utilizador do computador se aperceba do que está a acontecer. Para enganar o utilizador, estes ataques usam logótipos ou páginas de internet com aspecto semelhante ao das páginas das instituições de crédito.

A solicitação de informação sigilosa, como dados pessoais ou códigos de acesso *online* é também vulgar. Deve ter-se em atenção que as instituições de crédito nunca solicitam dados pessoais e códigos de acesso completos através de páginas de internet, mensagens de correio electrónico ou telemóvel.

Para este contexto, podemos dar o exemplo de casos de pessoas que têm dívidas em bancos que ao ter acesso ao computador podem apagar suas dívidas ou aumentar seus saldos. Conforme podemos constatar nas alíneas a), b), c) e f) do n.° 1 e os n.°s 2 e 3 do art. 294.° do CP, nos quais se pode verificar, com recurso a um ou mais dispositivos informáticos, a falsificação de um instrumento ou canal de pagamento electrónico (o dispositivo ou registo electrónico que permite ao utilizador transferir fundos ou pagar a um beneficiário), o acesso ilegítimo a um sistema de pagamento electrónico, mediante a violação indevida dos mecanismos de segurança, a instalação de objectos que afectem o funcionamento do canal ou sistema de pagamento electrónico, visando obter, adulterar ou destruir dados ou informações, e a criação de programas informáticos, instrumentos, objectos e outros meios preparados deliberadamente para a prática de infracções relacionadas com instrumentos de pagamento electrónicos (ainda subsistindo o recurso dos dispositivos informáticos à perpetração de tais delitos.

Decorrente da norma prevista no art. 294 CP, o legislador prevê uma pena de 5 anos e multa correspondente, nos casos em que "as acções descritas nos números anteriores incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado"[630].

O crime de Fraudes relativas aos instrumentos e canais de pagamento electrónico que também pode designar Fraude Informática, é equiparada ao crime de sabotagem informática,

[629] SILVA, R. G, ***Crimes da Informática***, Editora: CopyMarket.com, 2000.
[630] Cfr., o nº 3 do art. 294 do CP.

que é um dos mais danosos delitos praticados por meio de um sistema informático e tem como objecto o próprio sistema. Pode ser efectuado pela destruição do programa ou dos dados por meio de elementos criados pelos sabotadores como vírus ou miniprogramas que quando activados inutilizam os programas principais destruindo-os ou distorcendo o seu funcionamento, tornando o sistema inapto a processar. Pode ocorrer ainda quando estes mecanismos desfiguram os dados já armazenados, o que acarreta inúmeros prejuízos aos programas principais.

A sabotagem informática, em conformidade com uma IBCCRIM[631], é uma modalidade da mais recente forma de manifestação delituosa, que é a chamada criminalidade informática, que compreende todas as lesões relacionadas com dados processados de maneira automática, sejam aquelas praticadas por meio do sistema informático ou da Internet, sejam aquelas praticadas contra os elementos lógicos do sistema, que são os dados e os programas dos computadores.

No entendimento do IBCCRIM, sabotagem informática consiste na introdução dos chamados vírus num sistema ou rede de computadores. É também conhecida como terrorismo ou vandalismo informático, sendo normalmente praticada pelos conhecidos delinquentes virtuais: os *hackers*[632]. Além disso, é "capaz de produzir enormes prejuízos através de uma única acção isolada, seja devido ao alto desenvolvimento alcançado pelos sistemas de comunicação que compartilham os actuais computadores, seja devido à possibilidade de concentração de um grande número de informações num pequeno espaço"[633].

Equivalendo com o crime de fraude relativa aos instrumentos e canais de pagamento electrónico (al. b) e c) do n.° 1 e o n.º 2 do art. 294 do CP), pode verificar-se a instalação de objectos que afectem o funcionamento do canal ou sistema de pagamento electrónico, visando obter, adulterar ou destruir dados ou informações, aceder ilegalmente a um sistema de pagamento electrónico, mediante a violação indevida dos mecanismos de segurança.

Quanto à sua natureza, há uma corrente que defende ser um crime contra património. Outra, tendo em vista o dano, considera ser um crime contra a propriedade, que fica configurado quando uma acção reduz o poder de disposição sobre certo bem de terceiro, ainda que não

---

631 Instituto Brasileiro de Ciências Criminais (IBCCRIM), ob. cit.

632 Conforme ensina José Antonio Choclan Montalvo, ***"La teoría en el ámbito de la informática há acuñado el término Hacking o terrorismo lógico para referirse a los supuestos de vandalismo, terrorismo, destruicción de los elementos lógicos del sistema, que provocan perjuicios y están motivados por venganzas, chantajes, sabotaje o incluso por una muy sui géneris curiosidad intelectual que caracterizaba como se dijo a los primeros hackers o manipuladores no autorizados de sistemas informáticos" ("Estafa por Computacion y Criminalidad Economica Vinculada a la Informática***", in "Revista de Ac IBCCRIM, ibidem,

633 Ibidem..

possua valor económico. E, por isso, "estariam no âmbito de sua punição as acções de inutilização ou destruição de dados ou programas de computador, ainda que sem acarretar qualquer diminuição patrimonial, haja vista que estariam reduzindo o poder de disposição sobre referido bem[634].

Concordando com a visão do autor, não pode ser considerado como crime de dano, pelo facto de que o crime de dano exige a destruição de coisa alheia, que é um dos elementos objectivos indispensáveis para o aperfeiçoamento desse específico tipo penal, e os dados de computador decididamente não possuem o *status* de coisa. Os dados de computador são bens incorpóreos, e como ensina Nelson Hungria: "o objecto do crime de dano é a coisa móvel ou imóvel, devendo tratar-se obviamente de coisa corpórea no sentido realístico, pois somente essa pode ser danificada por acção física"[635].

Somos de entendimento de que para que a sabotagem informática seja considerada crime de dano, é fundamental preencher elementos imprescindíveis para o preenchimento do tipo penal do dano, que é a destruição de coisa alheia, uma vez que os dados de um computador não podem ser considerados como coisas passíveis de serem objecto do referido crime. Sendo assim, não há dúvida de que estamos diante de uma conduta praticada contra o sistema de informática (a sabotagem informática).

7. Falsidade informática (artigo 336 do CP)

A falsidade informática faz parte das categorias dos crimes informáticos. O tipo objectivo do crime de falsidade informática previsto no n.º 1 do art. 336 do CP, é integrado, no plano objectivo, pela introdução, modificação, apagamento ou supressão de dados informáticos ou por qualquer outra forma de interferência num tratamento informático de dados, de que resulte a produção de dados ou documentos não genuínos, consumando-se o crime com a produção deste resultado

Do entendimento do artigo 336 do CP, comete o crime de falsidade informática aquele que cria informaticamente contas, nas quais produz dados de perfil não genuínos de outra pessoa, através da utilização dos seus dados pessoais que, simulando ser a própria, introduz no sistema informático, para criar, via internet, um sítio próprio da plataforma da rede social *facebook*, imagem psicológica, carácter, personalidade e identidade daquela pessoa, que não correspondem à realidade, com intenção de serem considerados genuínos; e, através daquelas

[634] Ibidem..
[635] Instituto Brasileiro de Ciências Criminais (IBCCRIM), ob. cit.

contas, fingindo ser tal pessoa, divulgar conteúdos íntimos da sua vida pessoal, provocando dessa forma engano, com intenção de que fossem tomadas por verdadeiras e reais, aquelas contas, causando dessa forma prejuízo à honra e imagem de tal pessoa, como era seu desiderato.

Neste crime, o prejuízo não tem de ser patrimonial, pois o bem jurídico que nele se protege não é o património, mas a confidencialidade, integridade e disponibilidade de sistemas informáticos, das redes e dados informáticos.

Do ponto de vista subjectivo, o tipo legal supõe o dolo, sob qualquer das formas previstas no artigo 14 do CP, exigindo, enquanto elemento subjectivo especial do tipo, a intenção de provocar engano nas relações jurídicas, bem como, relativamente á produção de dados ou documentos não genuínos, a particular intenção do agente de que tais dados ou documentos sejam considerados ou utilizados para finalidades juridicamente relevantes como se fossem genuínos.

O crime de falsidade informática previsto no artigo 336º do CP visa proteger a segurança das relações jurídicas enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar e não a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos.

A utilização do nome ou de parte do nome de outrem no nome de utilizador e/ou endereço electrónico, por parte de quem criou conta de correio electrónico, traduz, no plano objectivo, a produção de dados ou documentos não genuínos, mediante a introdução de dados informáticos, e é idóneo a fazer crer que foi a pessoa a quem respeita o nome ou parte de nome quem efectivamente criou e utilizou a conta de correio electrónico em causa.

Resumindo, as falsificações informáticas têm como objecto, quando se alteram, dados de documentos armazenados em formato computadorizado; como instrumento, quando o computador é utilizado para efectuar falsificações de documentos de uso comercial, criando ou modificando-os, com o auxílio de impressoras coloridas a base de raio laser, cuja reprodução de alta qualidade, em regra, somente pode ser diferenciada da autêntica por perito.

O instituto da falsidade informática" cuja previsão legal enquadra-se no art. 336 CP, compõe de crimes conexos, como sejam, os crimes de "interferência em dados" (art. 337), "interferência em sistemas" (art. 338), "uso abusivo de dispositivos" (art. 339).

7.1. Interferência em dados (art. 337 do CP)

O crime de interferência em dados, previsto no art. 337 do CP, Essa norma tipifica o acto de alteração, deterioração, inutilização, apagamento, supressão, destruição, ou de qualquer forma, alteração de dados informáticos. Outrossim, qualifica como crime, a instalação de

vulnerabilidades, interferência no funcionamento de sistema informático causando intencionalmente danos a alguém.

7.2. “Interferência em sistemas (art. 338 CP)

O crime de interferência em sistemas, previsto no art. 338 do CP, refere-se à introdução de sinais ou elementos indesejados num sistema, com o objectivo de perturbar seu funcionamento normal. Essas interferências podem ocorrer em redes de comunicação, sistemas electrónicos, dispositivos de segurança, entre outros. Os métodos utilizados para comprometer uma rede podem variar desde o entravamento, impedimento, interrupção ou perturbação grave de funcionamento de um sistema informático, introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento de acesso ou supressão dos programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático

As implicações de uma interferência bem-sucedida em sistemas podem ser graves. Uma rede comprometida pode levar à interrupção dos serviços, vazamento de informações sensíveis, violação da privacidade dos usuários e danos financeiros consideráveis. Além disso, em sectores como o bancário e de saúde e de outros sectores chaves, as interferências podem representar um risco à segurança pública.

7.3. Uso abusivo de dispositivos” (art. 339 do CP).

O uso abusivo de dispositivos, como crime informático, previsto no art. 339 do CP, refere-se à produção, venda, distribuição, importação, disseminação ou introdução num dos sistemas informáticos, dispositivos, programas ou outros dados informáticos ilegitimamente, destinados a produzir as acções que interferem no sistema informático.

8. Difamação” (art. 233 do CP)

A difamação constitui um dos crimes contra honra, com a sua previsão no art. 233 do CP, consistindo em imputação de factos ofensivos à vítima, desse modo, o bem jurídico protegido é a honra objectiva, em outras palavras, o foro externo do indivíduo e sua imagem para com a sociedade, por consequência, a veracidade do facto é pormenorizado, assim, o que, de facto, importa para o delito da difamação é a imputação do ocorrido à pessoa.

O bem jurídico tutelado através dessa tipificação é a honra objectiva, a imagem da vítima no meio social. Nesse viés, a previsão legal visa coibir actos, sejam verbais/escritos, sejam verídicos ou não, por consequência, actos que manchem a honra da vítima, impedindo qualquer forma de desprezo ou depreciação face terceiros, mantendo incólume o respeito. Desse

modo, o objecto material é a própria vítima, ou a pessoa que sofre a imputação desses factos, cabe ressaltar que os mesmos devem se sustentar pelo princípio da razoabilidade.

9. "Injúria" (art. 234 do CP),

A injúria é a conduta típica que consiste no acto de ofender a dignidade e o decoro de alguém. Ao contrário da difamação, a tipificação do crime de injúria (art. 234 do CP), visa proteger a honra subjectiva do indivíduo, a visão, em sentido amplo, que o sujeito tem de si mesmo. Por conta dessa protecção da honra subjectiva, a injúria pode ser considerada, no âmbito dos crimes contra a honra, tanto como sendo a infracção penal menos grave, na sua modalidade simples, como sendo a mais grave, na sua modalidade preconceituosa. O bem juridicamente protegido no art. 234 do CP é a honra subjectiva do indivíduo.

A honra subjectiva pode ser caracterizada como as qualidades, sentimentos e conceitos que o indivíduo tem de si mesmo, que englobam valores morais e sociais da pessoa. Já o objecto material do delito de injúria é a pessoa contra a qual é dirigida a conduta ofensiva praticada pelo agente.

O legislador, ao formular na sua tipicidade criminal, a difamação e a injúria tem em vista proteger o direito à honra das pessoas, assegurando que a violação do direito em alusão seja sujeito a sanções criminais. Nessa perspectiva, a concretização dos dois institutos, como crimes informáticos, depende do meio em que o infractor usa para difamar ou injuriar a vítima. São as situações em que alguém com recurso a sua conta nas redes sociais, partilhe com os seus seguidores qualquer informação escrita que visa imputar um facto ofensivo a honra e imagem de uma pessoa.

10. Pornografia de menores (art. 211 do CP)

Tendo por objecto de protecção do bem jurídico «Liberdade sexual», o crime de pornografia de menores encontra-se previsto no artigo 211.º do CP. O tipo criminal em questão envolve as condutas a utilizar menores em comportamentos sexuais, utilizando qualquer material.

Trata-se de um crime público, ou seja, o respectivo procedimento criminal não depende nem da apresentação de queixa nem da dedução de acusação particular. O crime de pornografia de menores, encontra-se inserido na secção do CP relativo aos crimes contra a liberdade sexual e, pelo facto de ter como vítimas os menores de idade, este está revestido, no nosso contexto sociocultural, de um grande sentimento de reprovação.

11. Utilização de menores em pornografia (art.212 do CP)

A utilização de menor em fotografia, filme ou gravação pornográficos, independentemente do seu suporte, encontra-se prevista no art. 212 do CP, sendo a conduta do agente jurídico-penalmente relevante se o menor for usado numa fotografia nitidamente pornográfica ou se este for utilizado, a título principal ou secundário, num espectáculo de teor pornográfico.

12. Distribuição ou posse de pornografia de menores (art. 213 do CP)

A conduta de quem detém material pornográfico com o propósito de o distribuir, importar, exportar, divulgar, exibir ou ceder profissionalmente ou com finalidade de lucro, a qualquer título ou por qualquer meio, materiais, fotografia, filme ou gravação pornográfica de menores de dezoito anos, foi acolhido pelo artigo 213º, no seu número 1. O âmbito de punibilidade desta conduta passou a abranger a intenção de distribuir, divulgar, importar e exportar esses materiais, abarcando-se assim situações em que o agente age como veículo difusor de pornografia.

Consagrou-se, portanto, a punibilidade de uma conduta que constitui um crime de perigo abstracto, assim como um crime intencional, uma vez que, para a acção ser típica, exige-se a verificação dos elementos subjectivos. O que há aqui é, verdadeiramente, um "dolo específico, uma intenção de produção de resultado", cuja verificação não é necessária ao preenchimento do tipo.

5.4. Relação entre Crimes Cibernético e Crimes Informáticos no Direito Moçambicano

Os termos cibernético e informático levantam discussão doutrinal, de forma a se aferir se os dois apresentam elementos que encaixam no âmbito do objecto da tese. Nessa perspectiva, ilidimos que um depende do outro para a sua materialização. Isto é, o crime cibernético depende do crime informático para puder manifestar-se. Outrossim, pode manifestar-se o crime informático sem se verificar o cibernético.

Por crimes informáticos, nesta vertente, entendem-se aqueles praticados com recurso a um dispositivo electrónico, comummente denominado computador, sem que este esteja conectado à internet e mesmo estando, não se tenha perpetrado no ambiente cibernético e nem para o efeito se tenha utilizado a internet.

Os crimes cibernéticos, por sua vez, são os praticados e perpetrados no ambiente cibernético, ou melhor, na internet, ainda que o objecto mediato esteja fora do ambiente cibernético.

No nosso entendimento, o tratamento destes crimes na legislação penal moçambicana é indistintível, apesar de, em alguns momentos, o legislador referir-se especialmente aos crimes cibernéticos, mas em todos os casos correlaciona-os directamente com os crimes informáticos.

Neste contexto, podemos observar o crime de distribuição ou posse de pornografia de menores, previsto no art. 213.° do CP, o qual pode manifestar-se pela divulgação de conteúdo com recurso à internet, assim como a partilha, a exibição, a cedência, importação, exportação ou distribuição do material pornográfico de menores e bem assim o aliciamento destes menores. Sucedendo também com o crime de difamação previsto no art. 233.° do CP, quando se refere, essencialmente, no seu n.° 1 " (…) aos outros meios de publicação da difamação" que pode ser o ambiente cibernético. O mesmo sucede no crime de devassa da vida privada, previsto no art. 252.° do CP, e o crime de violação de correspondência ou de comunicações, previsto no art. 253.° do CP, quando "o meio utilizado para o efeito tenha sido informático ou ainda no ambiente cibernético".

No mesmo âmbito, pode se referir o caso do crime de base de dados automatizados, conforme o art. 254. ° do CP, onde com recurso aos "meios informáticos e à internet", o agente cria, mantem ou utiliza ficheiro automatizado de dados individualmente identificáveis e relativos às convicções políticas, filosóficas ou ideológicas, à fé religiosa, à filiação partidária ou sindical e à vida privada de outrem". O mesmo sucede com o crime de acesso ilegítimo (n.° 2 do art. 256. ° do CP) "ao dispositivo informático alheio com a finalidade de tomar conhecimento de certa informação ou objecto de natureza privada, ou seja, que não sejam públicos".

O mesmo acontece com o crime de Gravações ilícitas (art. 257. ° do Cp) nas circunstâncias em que o agente "gravar palavras proferidas por outra pessoa e não destinadas ao público, mesmo que lhe sejam dirigidas, e/ou utilizar ou permitir que se utilizem as gravações anteriores, mesmo que licitamente produzidas, quando seja contra vontade do ofendido e fora dos casos permitidos por lei".

Ao crime de apropriação ilegítima de coisa alheia (n.° 1 do art. 272. ° do Cp), aplicando-se para quem, ilegitimamente, se apropriar de coisa alheia que tenha entrado na sua posse ou detenção por efeito de força natural, erro, caso fortuito ou por qualquer maneira independente da sua vontade. Podemos levantar a situação em que uma pessoa transfere por erro, um valor

pelo meio bancário (principalmente aos novos serviços bancários das operadoras móveis, como M-pesa, M-kesh e, E-mola), com recurso a um dispositivo electrónico e o receptor se apodera da coisa recebido por erro ou por qualquer maneira independente da sua vontade.

Ao crime de burla informática (art. 289. ° do CP), onde o agente causa a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de "programa informático", utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, com intenção de obter para si ou para terceiro enriquecimento ilegítimo. Neste tipo de crime, apesar de o legislador não dizer directamente que o meio poderá ser a internet, ainda assim, tais actos podem ser realizados com recurso à internet, interferindo no tratamento de dados de uma outra pessoa que também esteja conectada à rede mundial de computadores, ou ainda comandando o dispositivo alheio remotamente pela internet.

Ao crime de fraude relativa aos instrumentos e canais de pagamento electrónico (art. 294 do CP), onde, no n.º 2 do referido artigo, considera-se instrumento de pagamento electrónico o dispositivo ou registo electrónico que permite ao utilizador transferir fundos ou pagar a um beneficiário, enquadrando-se nos sistemas de pagamento virtuais, tal seja para as compras *online*, os serviços bancários online, e demais que hajam de aparecer conforme a evolução tecnológica.

Ao crime de falsidade informática (art. 336. ° do CP), onde o agente poderá modificar, apagar ou suprimir de forma intencional e ilegítima dados informáticos, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se o fossem, seja recorrendo à internet ou executando of-line em um dispositivo informático. Ou ainda, com a prática de tais acções, o agente importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado.

Ao crime de interferência em dados (art. 337.º CP), onde o agente altera, deteriora, inutiliza, apaga, suprime, destrui ou, de qualquer forma, altera dados informáticos, ou mediante a introdução ou transmissão de dados informáticos ou, por qualquer outra forma, instalando vulnerabilidades, interfere no funcionamento de sistema informático, causando intencionalmente dano.

Ao crime de interferência em sistemas (art. 338.º do CP), no qual, o agente encrava, impede, interrompe ou perturba gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento,

impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, sem que para tal tenha havido permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele. Ou no crime de uso abusivo de dispositivos (art. 339.º do CP) para a obtenção dos anteriores resultados, de forma ilegítima produzir, vender, distribuir, importar ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizada.

5.5. Sujeitos Processuais no Âmbito dos Crimes Cibernéticos em Moçambique.

Os sujeitos processuais no âmbito do Direito Processual Penal "*são pessoas ou entidades titulares de direitos e deveres processuais, que através de actos processuais, conformam a tramitação do processo penal".* Com efeito, o processo penal deve ser instaurado pelo **Ministério Público (MP)** ou determinados órgãos titulares da acusação; ocorrer perante um **tribunal**; contra certa pessoa (**o arguido**), pressupondo a existência de um **ofendido**, que poderá se constituir em **assistente.** Assim, são **sujeitos processuais,** designadamente: *O Ministério Público e o Serviço Nacional de Investigação Criminal, o Arguido e seu defensor, o ofendido e os assistentes, o Tribunal – Juiz Penal* ([636]).

Os sujeitos processuais se distinguem de **participantes processuais,** que compreendem as **testemunhas, declarantes, peritos e intérpretes.** Os participantes processuais intervêm no processo quando tal seja necessário, sobretudo no âmbito da produção da prova. O processo penal é concebível sem a actuação dos participantes processuais, embora com maior o menor grau de dificuldade de prova ([637]).

5.5.1. O Ministério Público

O Ministério Público (MP) constitui uma magistratura hierarquicamente organizada, subordinada ao Procurador-Geral da República (Cfr. artigo 234 da CRM conjugado com o artigo 1 n°1 da Lei n° 1/2022 de 12 de Janeiro que aprova a Lei orgânica do MP). Trata-se de uma magistratura de carreira com reconhecimento constitucional, composta por magistrados togados, não eleita com um estatuto próprio de magistratura.

([636]) CUNA, Ribeiro José (2014), *Direito processual Penal.* Maputo: Escolar Editora, p. 123
([637]) CUNA, Ribeiro José (2014), *Direito processual Penal.* Maputo: Escolar Editora, p. 123

Enquanto os juízes são titulares de um órgão de soberania – os tribunais ([638]), os magistrados do MP produzem decisões de colaboração com o tribunal, não sendo considerados órgãos de soberania. O MP não declara o direito aplicável, apenas o propõe e o defende. Quem aplica o direito e daí tira consequências é o Tribunal ([639]).

O MP tem várias funções importantes, desde logo: (a) representar o Estado junto dos tribunais; (b) defender os interesses que a lei determina; (c) controlar a legalidade; (d) controlar o prazo das detenções; (e) **dirigir a instrução preparatória dos processos-crime; (f) exercer a acção penal;** (g) assegurar a defesa dos interesses dos menores, ausentes e incapazes (Cfr. artigo 235 da CRM conjugado com o artigo 1 n°2 da Lei n° 1/2022 de 12 de Janeiro que aprova a Lei orgânica do MP). Isto quer dizer que o MP tem poderes e responsabilidades muito amplas, **que não se limitam à acção penal.** No Caso da acção penal, o MP tem um monopólio que só é mitigado por dois regimes: (1) o regime dos crimes semipúblicos e (2) o regime dos crimes particulares e através do controlo que o assistente pode fazer quanto a promoção ou não promoção do processo (Cfr por exemplo, o artigo 277 do CP) ([640]).

5.5.2. O Serviço Nacional de Investigação Criminal (SERNIC)

Entre as funções que a Constituição impõe ao Ministério Público destaca-se a função de exercício da acção penal que corresponde a um número diverso de competências, das quais se destaca a de *dirigir a instrução preparatória dos processos-crime e deduzir a acusação.* Para cumprir esta tarefa, o Ministério Público é assistido pelo **Serviço Nacional de Investigação Criminal** (**SERNIC),** que *é um Serviço Público de investigação criminal de natureza paramilitar, auxiliar da administração da justiça, dotado de autonomia administrativa, técnica e táctica, sem prejuízo da tutela pelo Ministro que superintende a área da ordem, segurança e tranquilidade públicas, em matéria que não afecta a sua autonomia (Cfr. artigo 3 n°1 da Lei n°2/2017 de o9 de Janeiro).* Enquanto o MP é um sujeito processual, o SERNIC é apenas uma entidade coadjuvante, que não tem poderes autónomos.

O SERNIC actua sob a directa orientação e dependência funcional do Ministério Público (Vide o artigo 10 da Lei nº 2/2017 de 9 de Janeiro, conjugado com o artigo 308 do CPP). Ou

[638] Cfr. Artigo 133 da CRM

([639]) Cfr. PINTO, Frederico Costa (2017), *Direito processual penal, in*, http://ae.fd.unl.pt/wp-content/uploads/2019/10/Direito-Processual-Penal-Anonimo.pdf p. 81, acesso, 17-05-2022.

([640]) Cfr. PINTO, Frederico Costa (2017), *Direito processual penal, in*, http://ae.fd.unl.pt/wp-content/uploads/2019/10/Direito-Processual-Penal-Anonimo.pdf p. 82, acesso, 17-05-2022.

seja, os agentes do Serviço Nacional de Investigação Criminal actuam sob directa orientação e na dependência funcional do Ministério Público, tão – só com vista e no que concerne à realização das finalidades do processo penal (GONÇALVES: 1999, p. 182). Analisando ao disposto no artigo 10 da Lei nº 2/2017 de 9 de Janeiro, conjugado com os artigos 308, 315, 316 e 317 todos do CPP, podemos concluir que o legislador processual penal Moçambicano ***optou pelo sistema de dependência funcional do Serviço Nacional de Investigação Criminal ao Ministério Público,*** que se pode analisar sob ponto de vista jurídico-funcional e sob ponto de vista jurídico-organizacional.

Assim, **sob ponto de vista jurídico-funcional**, a direcção da instrução preparatória cabe ao Ministério Público, a quem será prestado pelas autoridades e agentes policiais todo ao auxílio que para esse fim necessitar; isto é, para efeitos da instrução preparatória o princípio geral será o da *actuação subordinada dos agentes do* Serviço Nacional de Investigação Criminal *ao Ministério Público.* A subordinação do Serviço Nacional de Investigação Criminal ao Ministério Público traduz-se na possibilidade de o Ministério Público emitir orientações e ordens, estando o Serviço Nacional de Investigação Criminal obrigado a cumpri-las. Do conjunto dos poderes que o Ministério Público possui, que o permitem influenciar a actuação do Serviço Nacional de Investigação Criminal na actividade produzida por este, destacam-se *o poder de orientação ou direcção, o poder de controlo e o poder de fiscalização.*

Quanto ao poder de orientação ou direcção **(**Vide o artigo 4 alínea e) da Lei nº 1/2022 de 12 de Janeiro conjugado com o artigo 10 da Lei nº 2/2017 de 9 de Janeiro***):*** o Ministério Público pode conformar a actividade do Serviço Nacional de Investigação Criminal através de emissão de orientações e ordens. O poder de orientação não dá campo ao Serviço Nacional de investigação Criminal de modo que esta faça a sua apreciação valorativa a estes comandos, pois tudo deve ser feito na estreita linha de orientação. Os comandos que o Serviço Nacional de investigação Criminal recebe do Ministério Público dizem respeito as questões ligadas aos direitos dos arguidos, a legalidade das buscas e capturas, os prazos de prisão preventiva, realização de diligências, etc. O poder de orientação pressupõe para que se efective que a ele esteja conexos outros poderes instrumentais em relação ao poder de emitir esses comandos. Entre os outros poderes instrumentais, está o ***poder de informação***, o ***poder de avocação***. Ocorre avocação quando o Ministério Público decide assumir na sua titularidade quanto ao caso concreto ou delegado ao Serviço Nacional de investigação Criminal.

No que tange ao poder de fiscalização **(**Vide o artigo 4 alínea m) da Lei nº 1/2022 de 12 de Janeiro: este poder traduz-se na fiscalização de âmbito restrito do MP aos actos praticados

pelo Serviço Nacional de Investigação Criminal, sem, no entanto ter a possibilidade de sancioná-la. Este se diferencia do poder de controlo na medida em que abrange apenas os actos concretos, ao passo que o poder de controlo é mais abrangente.

Relativamente ao poder de Controlo (Vide o artigo 4 alínea g) da Lei nº 1/2022 de 12 de Janeiro)**:** este consiste num poder autónomo que ultrapassa o restrito esquema de relacionamento, mas que com ela é conexo, visto que visa suprir a falta de garantia decorrente da solução em favor da dependência funcional e de supremacia sem hierarquia. O poder de controlo é geral sobre a administração da justiça no seu todo, ao passo que o poder de fiscalização é específico que cabe ao Ministério Público quanto a um concreto acto processual penal.

Deste modo, a forma mais genérica que surge em termos de relacionamento entre o Ministério Publico e o Serviço Nacional de Investigação Criminal é no âmbito da coadjuvação para finalidades processuais penais. Portanto, *sob ponto de vista jurídico – funcional*, o Serviço Nacional de Investigação Criminal é apenas um órgão auxiliar (Vide artigo 3 nº1 da Lei nº 2/2017 de 9 de Janeiro) do Ministério Público, enquanto e só actuante com vista à realização das finalidades processuais. Neste contexto, a maior colaboração que o Serviço Nacional de Investigação Criminal dá ao Ministério Público diz respeito aos exames dos instrumentos do crime e do local de ocorrência do facto.

Analisando o sistema de relacionamento entre o Ministério Público e o Serviço Nacional de Investigação Criminal, sob ponto de vista jurídico-organizacional podemos dizer que o Serviço Nacional de investigação criminal é colocado "na dependência funcional, dentro do processo, das autoridades judiciárias, persistindo, porém, a dependência organizativa, administrativa e disciplinar face ao executivo" (GONÇALVES: 1999, p.182). O Serviço Nacional de Investigação Criminal no exercício das competências penais actua sob a responsabilidade do Ministério Público, criando-se entre eles uma relação de supremacia sem hierarquia que consiste no reconhecimento de um poder de orientação do Ministério Público sobre o Serviço Nacional de Investigação Criminal (vide artigo 10 da Lei nº 2/2017 de 9 de Janeiro).

Mas também os agentes do Serviço Nacional de Investigação Criminal estão integrados numa dependência hierárquica do Director-geral do Serviço Nacional de Investigação criminal, nomeado por Primeiro-Ministro, sob Proposta do Ministro do Interior, residindo aí o poder disciplinar orgânico e administrativo (vide artigo 24 nº1 conjugado com o artigo 25 alínea o) da Lei nº 2/2017 de 9 de Janeiro). Portanto, os agentes do Serviço Nacional de Investigação

Criminal sofrem dupla subordinação, sendo uma a nível material, pois, materialmente o Serviço Nacional de Investigação Criminal subordina-se ao Ministério Público e a outra ao nível hierárquico, pois, o Serviço Nacional de Investigação criminal hierarquicamente subordinam-se ao executivo.

5.5.3. Suspeito, Arguido e seu Defensor

5.4.3.1. O Arguido

"*Assume a qualidade de **arguido** aquele contra quem for deduzida a acusação ou requerida a audiência preliminar num processo penal" (Cfr. artigo 65 n°2 do CPP). O arguido é um suspeito formalizado, que passou pela sua constituição em arguido.* A definição de arguido é de particular relevância em processo penal, tendo em conta **os efeitos de constituição** de determinada pessoa como arguido e o regime jurídico que se lhe aplica.

O formalismo exigido no interrogatório do arguido é mais complexo e dotados de maiores garantias do que o formalismo exigido para o interrogatório de uma testemunha"([641]) Cfr., os artigos 159,163, 164, 175-178; todos do CPP). Com efeito, o interrogatório do arguido exige maiores garantias, desde logo, **a presença de um advogado,** constituído ou defensor oficioso (Cfr. artigo 175 n°2 do CPP).

5.5.3.2. Distinção entre o Suspeito, o Arguido/ Réu

O arguido distingue-se do **suspeito,** pois este "*é aquele relativamente ao qual exista indício de que cometeu ou se prepara para cometer um crime ou que nele participou ou se prepara para participar (Cfr. artigo 65 n°1 CPP).*

O suspeito distingue-se do arguido pelo facto de não pesar sobre ele qualquer acusação ou existir qualquer requerimento de audiência preliminar no decurso do processo penal. Ou seja, *toda pessoa a quem recai uma investigação criminal, designa-se por suspeito até que seja deduzida a acusação, ou requerida a audiência preliminar ou ainda até que seja constituído em arguido nos casos declarados na lei (Cfr. artigo 65 n°1 e 2 conjugado com o artigo 66 n°1 ambos do CPP).* **O suspeito não é um sujeito processual.**

"*A Constituição de arguido representa (…) uma garantia da pessoa sobre quem recai a investigação ou foi deduzida a acusação, garantida de que pode defender-se, nomeadamente*

([641]) CUNA, Ribeiro José (2014), *Direito processual Penal.* Maputo: Escolar Editora, p.151

a de se fazer assistir por defensor, de audiência, de se manter em silêncio etc."([642]). Conceitualmente, o arguido distingue-se outrossim do réu, sendo este considerado como tal, *o arguido pronunciado ([643]) mediante a recepção e aceitação da acusação pelo juiz (Cfr. artigo 353 n°1 e 354 do CPP).*

5.5.3.3. O Estatuto ou Posição Processual do Arguido

O estatuto jurídico do arguido é um acervo de direitos e deveres de natureza processual. Com efeito, desde que uma pessoa adquire a qualidade de arguido é-lhe assegurado o exercício de direitos e deveres processuais, sem prejuízo da aplicação de medidas de coacção e de garantia patrimonial e da efectivação de diligências probatórias (Cfr. artigo 68 n°1 do CPP).

Os direitos e deveres processuais do arguido constam do artigo 69 do CPP, com o destaque para o **direito de escolher o defensor ou solicitar ao juiz que lhe nomeie um (Cfr. artigo 69 n°1 alínea d) do CPP).**

5.5.3.4. O Defensor

O defensor é um *órgão autónomo de administração da justiça, que colabora com o tribunal para a descoberta da verdade e realização do direito, actuando exclusivamente em favor do arguido ([644]).* Em processo penal existe uma admissibilidade geral da defesa, uma vez que tanto a CRM no artigo 62 n°2, como o Código de processo penal no artigo 70 n°1 permitem que o arguido possa escolher livremente o seu defensor e constitui-lo em qualquer altura do processo através de mandato forense.

No entanto, a defesa, sendo admissível de forma geral, em qualquer altura do processo, *ela é necessária e obrigatória em certos casos prevista na lei.* Com efeito, *é obrigatória a assistência do defensor* (Cfr. artigo 72 n°1 do CPP):

(a) No primeiro interrogatório judicial do arguido;

(b) Na audiência preliminar e na audiência de julgamento, salvo se tratando-se de processo que não possa dar lugar a aplicação da pena de prisão ou de medida de segurança de internamento;

([642]) SILVA, Germano Marques Da (2010), *curso de processo penal I – noções gerais, elemento do processo penal,* 6ª Edição, Revista e actualizada, VERBO, Edição Babel, Lisboa, p. 319, *Apud,* CUNA, Ribeiro José (2014), *Direito processual Penal.* Maputo: Escolar Editora, p. 152.
([643]) Cfr. CUNA, Ribeiro José (2014), *Direito processual Penal.* Maputo: Escolar Editora, p.152.
([644]) Cfr. CUNA, Ribeiro José (2014), *Direito processual Penal.* Maputo: Escolar Editora, p.173

(c) em qualquer acto processual, sempre que o arguido for cego, surdo, mudo, desconhecedor da língua portuguesa, menor de 21 anos ou suscitar a questão da sua inimputabilidade ou imputabilidade diminuída;
(d) nos recursos ordinários e extraordinários; (e) nos casos de declarações para memória futura (artigo 318 e 340 do CPP); e nos demais casos que a lei determinar.

Dada a importância da obrigatoriedade de assistência do defensor, constitui nulidade insanável, a ausência do arguido ou do seu defensor, nos casos em que a lei exigir a respectiva comparência (Cfr. artigo 135 alínea c) do CPP).

5.5.3.5. O Ofendido, o Lesado e o Assistente

5.5.3.5.1. Distinção entre Ofendido, Lesado e o Assistente

> **"***O assistente distingue-se processualmente do ofendido e do lesado. O ofendido não é sujeito processual, salvo se se constituir em assistente; o lesado, enquanto tal, nunca pode constituir-se assistente, mas apenas parte civil para efeitos de deduzir pedido de indemnização civil, mas sendo aquele que sofreu danos com o crime, pode coincidir e coincide muitas vezes com o ofendido, e, por isso, pode também constituir-se assistente, não por ser lesado, mais por ser ofendido"([645]).*

O ofendido é o titular do bem jurídico lesado ou posto em perigo e, torna-se sujeito processual, depois de se constituir em assistente. Note-se que a figura do ofendido e do assistente nem sempre tem de coincidir, pois o ofendido não é o único a poder constituir-se assistente.

5.5.3.5.2. Constituição de Assistente e sua Posição Jurídica no Processo Penal.

(A) - Legitimidade para Constituição de Assistente

Podem constituir-se assistentes no processo penal, além das pessoas a quem as leis especiais conferirem esse direito (Cfr. artigo 76 do CPP):

(a) O ofendido – considerando-se como tal o titular de interesses que a lei especialmente quis proteger com a incriminação, desde que maior de 16 anos;

([645])SILVA, Germano Marques Da (2010), *curso de processo penal I – noções gerais, elemento do processo penal,* 6ª Edição, Revista e actualizada, VERBO, Edição Babel, Lisboa, p. 355, *Apud,* CUNA, Ribeiro José (2014), *Direito processual Penal.* Maputo: Escolar Editora, pp. 184-185.

(b) A pessoa cuja queixa ou acusação particular depender o procedimento criminal;

(c) Se o ofendido morrer sem ter renunciado a queixa, o cônjuge sobrevivo não separado judicialmente de pessoas e bens, os descentes, os adoptados e a pessoa a que com o ofendido vivesse em condições análogas às de cônjuge ou na falta deles, os ascendentes, os irmãos e os seus descendentes e os adoptantes, salvo se algumas destas pessoas tiverem comparticipado no crime;

(d) Se o ofendido for incapaz, o seu representante legal e as pessoas indicadas na lei processual (o cônjuge sobrevivo não separado judicialmente de pessoas e bens, os descentes, os adoptados e a pessoa a que com o ofendido vivesse em condições análogas às de cônjuge ou na falta deles, os ascendentes, os irmãos e os seus descendentes e os adoptantes, salvo se algumas destas pessoas tivem comparticipado no crime);

(e) Qualquer pessoa nos crimes de tráfico de pessoas, rapto, sequestro, abuso sexual de menores, pornografia e prostituição de menores, de terrorismo ou outro tipo de criminalidade organizada ou associação criminosa, falsificação de moeda, notas de banco e títulos do Estado, de passagem de moeda falsa, de contrabando, tráfico de produtos e espécies da fauna e flora proibidos, de dano contra o meio ambiente e poluição, de corrupção, peculato, suborno, concussão, branqueamento de capitais, fraude em concurso de fornecimento de obras, bens e serviços pelo Estado e enriquecimento ilícito.

(B) - Regime da Constituição de Assistente

O regime jurídico da constituição em assistente encontra-se fixado no artigo 77 do CPP. A **regra geral (artigo 77 n°2 do CPP),** é a de que "*o assistente pode intervir em qualquer altura do processo, aceitando-o no estado em que se encontrar, desde que o requeira ao juiz até cinco (5) dias antes do início da audiência de julgamento.* Esta regra geral, só se aplica se não houver lei espacial sobre a oportunidade de constituição em assistente.

A regra geral de constituição de assistente não se aplica ao denunciante, que goza de um regime especial. Com efeito,

> "*o denunciante pode declarar, na denúncia, que deseja constituir-se assistente. Tratando-se de crime cujo procedimento depende da acusação particular, a declaração é obrigatória, devendo neste acaso, a autoridade judiciária ou órgão dos serviços de investigação criminal a quem a denúncia for feita verbalmente advertir ao denunciante da obrigatoriedade de constituição de assistente e dos procedimentos a*

observar, sem prejuízo, de o MP finda a instrução notificar ao denunciante para se constituir assistente e deduzir a acusação no prazo de 5 dias (Cfr. 289 n°4 conjugado com o artigo 330 n°4 ambos do CPP do CPP).

(C) - O Estatuto Híbrido do Assistente (ou Posição Processual).

O Estatuto do assistente é considerado híbrido, pelo facto de subordinar-se ao Ministério Público e em alguns casos gozar de autonomia para praticar actos por si mesmo ainda que não esteja alinhado com o MP. Com efeito, o artigo 78 n°1 do CPP, estabelece que "***o assistente tem a posição de colaborador do Ministério Público, a cuja actividade subordina a sua intervenção no processo, salvas as excepções da lei".***

Ora, acontece que as excepções da lei referidas no artigo 78 n°1 do CPP, são todos casos em que o assistente tem autonomia para praticar actos por si mesmo, ainda que isso vá contra a posição do Ministério Público (por exemplo, há casos em que o MP abstém-se de acusar e o assistente deduz a acusação particular). Assim, sendo a lei diz que o assistente subordina a sua actividade ao Ministério Público, e depois em muitos casos ele tem uma intervenção autónoma, o que lhe permite actuar isoladamente e controlar os actos do Ministério Público.

5.5.3.6. O Tribunal: o Juiz Penal

Os tribunais judiciais são os órgãos competentes para decidir as causas penais e aplicar penas e medidas de segurança criminais. As decisões dos tribunais são de cumprimento obrigatório para todos os cidadãos e demais pessoas jurídicas e prevalecem sobre as de outras autoridades (artigo 15 n°3 do CPP).

No exercício das suas funções, os tribunais têm direito a ser coadjuvados por **outras autoridades e entidades públicas e privadas**; a colaboração solicitada prefere a qualquer outro serviço (Cfr. artigo 15 n°1 e 2 do PP). Constituem autoridades judiciárias, o Juiz, o Juiz de Instrução Criminal e o Ministério Público, cada um relativamente aos actos processuais que cabem nas suas competências (Cfr. artigo 17 do CPP).

No exercício da função jurisdicional, vigora o **princípio do juiz natural,** segundo o qual, *"nenhuma causa poderá ser subtraída ao tribunal cuja competência esteja fixada em lei anterior" (artigo 16 do CPP).* Ou seja, do princípio do juiz natural ou do juiz legal resulta o "direito fundamental dos cidadãos a que uma causa seja jugada por um tribunal previsto como

competente por lei anterior, e não ad hoc criado ou tido como competente[646]", sendo através deste princípio que se salvaguarda a necessária garantia dos direitos da pessoa, em termos de ser julgado por um tribunal independente e imparcial e, dessa forma assegurar-se a confiança da comunidade na administração da justiça.

O **princípio do juiz natural** ou do juiz legal encontra-se consagrado no Pacto Internacional dos Direitos Civis e Políticos, ao dispor que todas as pessoas têm o direito a que a sua causa seja ouvida equitativa e publicamente por um tribunal competente ([647]), independente, imparcial e na carta Africana dos Direitos do Homem e dos Povos, que se refere ao direito a ser julgado em tempo razoável por um tribunal imparcial([648]). No entanto, é de referir que o princípio do juiz natural não impede que a lei preveja especialmente os casos de desaforamento ([649]).

Portanto, o **princípio do juiz natural** proíbe é a criação, posterior de um juiz para conhecer de um certo, ou então a determinação arbitrária ou discricionária do juiz competente, tendo assim por finalidade estabelecer uma organização fixa dos tribunais ([650]).

5.6. A Actuação da Administração da Justiça Moçambicana no Combate aos Crimes Cibernéticos

As tecnologias de informação e comunicação alavancam o desenvolvimento dos Estados. A tecnologia digital é usada para a prática de actos criminais que se apresentam como uma tipologia de crime transnacional em expansão, ocorrendo no ciberespaço, sem fronteiras. A internet tem sido usada, com frequência, para efectuar operações bancárias, compras, entre outras, criando uma maior exposição e ambiente favorável às actividades ilícitas on-line, com a incidência para a fraude ou burlas, usando meios informáticos e de comunicações, bem como a desinformação digital, criando por via dos meios digitais, novas oportunidades para as mais variadas formas de criminalidade.

Moçambique, a par de outros Estados, não está imune a ataques aos seus sistemas informáticos, com todos os prejuízos em termos de segurança e funcionamento normal de instituições públicas e privadas. Nesse corolário, os órgãos da Administração da Justiça

([646]) DIAS, Jorge de Figueiredo, ***Direito Processual Penal***, 1°. Volume, 1.ª Edição – 1974, Reimpressão, Coimbra, 2004, pág. 322
([647]) Artigo 14 n°1 da Resolução n°5/91 de 12 de Dezembro, que ractifica o Pacto Internacional Sobre os Direitos civis e políticos, adoptado pela Assembleia Geral das Nações Unida, em 16 de Dezembro de 1966.
([648]) Artigo n°7 alínea d) da carta Africana dos Direitos do Homem e dos Povos, ratificada por Moçambique através da resolução n° 8/88 de 25 de Agosto
([649]) Cfr. artigo 37 da LOJ – Lei n° 24/2007, de 20 de Agosto – Lei de organização judiciária.
([650]) CUNA, Ribeiro José, ***lições de Direito Processual Penal,*** Escolar Editora, Maputo, 2004, pag 213.

moçambicana, a semelhança de outras instituições da Administração Pública de outros Estados, nem sempre encontram uma resposta atempada de investimentos para responder as exigências do desenvolvimento tecnológico que o mundo tem vindo a registar. Sendo assim, as dificuldades de natureza adversas (técnicas e financeiras) que estas instituições encaram, têm vindo a contribuir negativamente para o acompanhamento e esclarecimento pleno dos crimes cometidos em meios digitais.

De acordo com o Ministério Publico, nos últimos anos, os crimes cibernéticos têm crescido a cada dia, em Moçambique, os criminosos tem vindo a sofisticar, cada vez mais a sua forma de actuação, sendo tarefa primordial do Sistema da Administração da Justiça prevenir e combater esta criminalidade. A eficiência nessa acção passa pela adopção de medidas legislativas eficazes, bem como de políticas e estratégias consistentes.

O aumento gradual dos crimes cibernéticos tem vindo a preocupar os órgãos da Administração da Justiça, o que exige estratégias vista a mitigação desta realidade. A título ilustrativo, em 2018 foram tramitados 357 processos[651] relacionados com crimes cibernéticos e em 2019 os números subiram para 509 processos, um aumento em 152 processos, o correspondente a 42,68%. De igual modo, em 2020 foram tramitados 692 processos, o que representa um aumento em 133 processos, o correspondente a 36%[652]. Em "2021 foram registados 393 processos, contra 692, de igual período anterior (2020), o que significa um decréscimo de 299, correspondente a 43,2%"[653]. Ainda em conformidade com o informe do Ministério Público, "as Procuradorias Provinciais da República – em Gaza, Maputo e Tete foram as que registaram maior número, com 64, 44 e 43, respectivamente. As Procuradorias Provinciais da República – em Cabo Delgado, Manica e Sofala, com 13, 20 e 26, são as que registaram menor número de processos. Os tipos legais de crime mais registados foram - fraudes relativas aos instrumentos e canais de pagamento electrónico, com 214, e burla informática e nas comunicações, com 70 processos" [654].

Ainda na mesma senda, "em 2022, foi registado um ataque cibernético, que afectou o normal funcionamento de várias instituições do Estado (Serviço Nacional de Migração, Instituto Nacional de Gestão e Redução de Riscos de Desastres, Direcção Nacional de Identificação Civil e Administração Nacional de Estradas), cujo processo encontra-se em instrução preparatória. A tendência da ocorrência de crimes informáticos manteve-se crescente,

[651] MOÇAMBIQUE, PROCURADORIA-GERAL DA República, ***ob. cit***.
[652]PROCURADORIA-GERAL DA REPúBLICA, ***obb. Cit.*** 2020.
[653] Idem , 2022, p. 53.
[654] Ibidem, pp.53-54.

tendo sido registados 560 processos, contra 393 (em 2021)[655]. "Foram concluídos 456, tendo recaído despacho de acusação em 267 e 189 arquivados. A Cidade de Maputo, com 81, e as Províncias de Manica e Gaza, com 74 e 67 processos, respectivamente, foram as que apresentaram maior registo. Portanto, continuam frequentes os crimes de fraudes relativas aos instrumentos e canais de pagamento electrónico, com 251, seguida da burla informática e nas comunicações, com 139, e furto de fluidos, com 74 "[656].

Reconhecendo o aumento e a sofisticação da criminalidade cibernética em Moçambique, ressalta-nos afirmar que embora a recente reforma da legislação penal tenha trazido inovações na criminalidade informática, entretanto, a dinâmica desta criminalidade impõe a aprovação de uma lei específica que contemple outras manifestações do cibercrime e estabeleça, na componente processual, medidas especiais de recolha, conservação e manutenção da prova, bem como de análise forense, prevenção de perdas, maneio de incidentes e avaliação de risco, assegurando, assim, uma investigação profícua. Outrossim, é essencial potenciar a área das tecnologias de informação e comunicação, com pessoal especializado, impondo-se, assim, a formação de peritos informáticos para auxiliarem na investigação, sobretudo, na recolha e tratamento de prova digital ou electrónica. "A adesão de Moçambique à Convenção de Budapeste sobre o Cibercrime contribuiria para facilitar a cooperação internacional, nesta matéria, pois estamos em face de criminalidade organizada, com natureza transnacional"[657].

Avaliando pela sofisticação e o *modus operandi* dos autores, somos de entendimento que a qualificação de magistrados e investigadores, bem como o apetrechamento em meios tecnológicos adequados, de modo a assegurar a recolha de elementos indiciários do crime e a identificação dos infractores, é uma estratégia a tomar em consideração, pela velocidade de actuação dos infractores.

Uma das principais medidas para a prevenção e combate à criminalidade informática é a actualização permanente do nosso quadro legislativo, de modo a acompanhar a evolução deste tipo de criminalidade e os instrumentos jurídicos internacionais sobre a matéria.

O Código Penal moçambicano não dispõe de condutas específicas relacionadas a tipos penais exclusivos aos crimes cibernéticos, deixando criminalmente impunes situações tais como acesso ilegítimo; intercepção ilegítima; interferência em dados; danos relativos a programas ou outros dados informáticos; sabotagem informática, etc.

---

[655] Idem, 2023, p.35.
[656] Ibidem, p.35.
[657] Procuradoria-Geral da República, ***ob, cit***., 2023, p.36.

É de concordar com o MP quando alude que a natureza instável, dispersa e imaterial que caracteriza a prova digital exige da investigação maior atenção com a sua recolha, de forma a garantir a sua integridade e força probatória em juízo. As especificidades técnicas que caracterizam a criminalidade informática exigem reconhecimento de procedimentos de investigação distintos.

Um dos maiores desafios dos órgãos de Administração da Justiça em Moçambique consiste em ter profissionais dotados de conhecimentos específicos sobre a matéria e com meios técnicos a altura da sofisticação dos criminosos. E, por outro lado, os crimes cibernéticos, muitas vezes, transcendem o ordenamento jurídico moçambicano, uma vez que o praticante de tais crimes nem sempre se encontra no território nacional, o que exige das autoridades judiciais a cooperações internacionais e ratificação de convenções de prevenção e combate ao cibercrime, de modo a terem acesso a colaboração com os países dos criminosos para a recolha de informações que permitam o esclarecimento de tais crimes e com vista a sua responsabilização.

Neste contexto, importa afirmar que as especificidades tecnológicas, o carácter transaccional, a dificuldade na identificação dos seus agentes e os efeitos dos crimes informáticos tornam a sua investigação ainda mais complexa e um desafio acrescido para o Ministério Público, facto que exige deste Órgão, formações sobre o cibercrime, incluindo matérias de segurança informática e cooperação jurídica e judiciária. Como corolário, há necessidade de o Governo priorizar, nos seus investimentos, esta matéria, em meios técnicos, materiais e humanos, de modo a criar segurança tanto para os utentes assim como para os prestadores dos serviços; investimento que deve também abranger aos órgãos da administração da justiça, para que estes estejam a altura de esclarecer delitos cometidos por meio destas plataformas digitais.

5.7. Segurança Cibernética no Contexto Moçambicano

A ideia do presente tópico é trazer um breve mapeamento sobre os problemas da segurança cibernética em Moçambique. Problemas acentuados pela existência de vulnerabilidades e/ou ameaças que afectam a segurança de diferentes actores no ciberespaço e do próprio ciberespaço[658]. Nesse sentido, Najah argumenta que:

[658] O ciberespaço é "o ambiente criado pelo uso da eletroeletrónica e do espectro eletromagnético, no qual ocorre a criação, armazenamento, processamento, transmissão de informações e comunicações em redes analógicas e digitais mais ou menos interconectadas (Kuehl, D. 2009. Cyberpower and National Security, Ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz. Center for Technology and National Security Policy, National

> "O ciberespaço é formado pela união dos componentes físicos e virtuais". O autor define o ciberespaço "como interação dinâmica entre três camadas. A primeira é a camada física, incluindo elementos materiais tais como satélites, cabos submarinos, data centers, telefonia fixa/móvel etc. A segunda camada é a das aplicações, a qual inclui os sistemas operacionais, protocolos, códigos, aplicações, bases de dados etc. A camada virtual permite a utilização da infraestrutura física, mas também a produção e circulação de conteúdos produzidos. A terceira camada é chamada de cognitiva. Para o autor, é a camada individual e coletiva que reúne o universo das duas camadas anteriores, possibilitando assim que as informações sejam produzidas, redes sociais sejam criadas e discussões e trocas de dados ocorram em tempo real" [659].

Assim, segundo Cepik et al, "a segurança cibernética é obtida por meio de actividades e medidas preventivas, de redução de vulnerabilidades, bem como por meio de acções dissuasórias e/ou coercitivas, que visam a neutralizar ameaças e a proteger o espaço cibernético"[660]. Concretamente trata-se da segurança dos desenvolvedores, provedores, usuários, infra-estrutura, acervos informacionais e comunicações[661].

A internet é considerada sinónimo de ciberespaço, com a evolução das comunicações mundiais e o avanço da digitalização. Na verdade, como explica Canabarro *et al*, "o ciberespaço é anterior ao surgimento da internet. Ou seja, quando novas tecnologias da Era Digital superarem a configuração actual da internet, o ciberespaço continuará existindo. Enquanto componente decisivo do ciberespaço, a internet pode ser definida como "a estrutura internacional das redes de computadores digitais interligados via cabos submarinos, fibra óptica e satélite".

Em conformidade com Leal, "a internet também se caracteriza pelo uso de protocolos comuns para as comunicações e aplicações, principalmente o TCP-IP (*Transmission Control Protocol – Internet Protocol)"*[662].

A segurança cibernética é obtida por meio de actividades e medidas preventivas, de redução de vulnerabilidades, bem como por meio de acções dissuasórias e/ou coercitivas, que visam a neutralizar ameaças e a proteger o espaço cibernético. Concretamente, trata-se da

---

Defense University, USA, p. 39-40. Apud CEPIK, Marco Aurélio Chaves; et al. Revista Carta Internacional. Associação Brasileira de Relações Internacionais, Belo Horizonte, V.16, n.3, e1130, 2021, DOI: 10.21530/ci.v16n3.2021.1130,ISSN2526-9038, p.7 (7-25).

[659] Najah, R. 2020. Le cyberespace africain: un état des lieux. Disponível em: www. policycenter.ma/opinion/le-cyberespace-africain-un-etat-des-lieux#.X2BMHpNKjGI. Acesso em: 1 de junho de 2020. Apud CEPIK, Marco Aurélio Chaves; et al. Revista Carta Internacional. Associação Brasileira de Relações Internacionais, Belo Horizonte, V.16, n.3, e1130, 2021, DOI: 10.21530/ci.v16n3.2021.1130,ISSN2526-9038, p.5 (5-25).

[660] CEPIK, Marco Aurélio Chaves; et al, ***Revista Carta Internacional. Associação Brasileira de Relações Internacionais***, Belo Horizonte, V.16, n.3, e1130, 2021, DOI: 10.21530/ci.v16n3.2021.1130,ISSN2526-9038, p.3 (3-25).

[661] Ibidem, p.7 (7-25).

[662]Ibidem, p.7 (7-25).

segurança dos desenvolvimentistas, provedores, usuários, infra-estrutura, acervos informacionais e comunicações[663]. De tudo isso, leva-nos a um entendimento de que segurança cibernética é um processo interactivo e dinâmico, não um dado fixo no tempo e no espaço.

Conforme Cepik *et al*[664], "Em 2019, Moçambique contava com 6.523.613 usuários de internet. Cerca de 20,9% de uma população total de mais de 30 milhões. A maioria dos usuários no País tem acessado a internet por meio de telefonia celular, como ocorre em outros países do Sul Global. Segundo o Instituto Nacional de Estatísticas (INE), em Dezembro de 2018, havia 14 milhões de assinantes de telefonia móvel no País[665]. O adensamento digital traz oportunidades de desenvolvimento, mas também vulnerabilidades do e no ciberespaço. Instituo Nacional de Governo Electrónico (INAGE), mostra que "2018, Moçambique registou mais de 1,5 milhão de ataques por mês, dos quais 90% ataques não-direccionados, principalmente phishing, *spam* e malware (vírus, worms, trojans e bots). Mas órgãos governamentais e universidades sofreram ataques tipo DDoS (negação de serviços) *e web defacement*. Ainda em 2019 e 2020, além do aumento de ataques não-direccionados, foram detectados ataques persistentes, incluindo ransomware, spyware e quebras de chaves criptográficas, em redes governamentais, empresas e no sistema financeiro"[666].

Os ataques cibernéticos constituem um problema que preocupa as sociedades em todo mundo, principalmente no espaço cibernético moçambicano, que se mostra vulnerável pelos ataques cibernéticos. Essa preposição vem sendo referenciado pelo Kshetri, ao destacar que "ataques cibernéticos causam bilhões de dólares de prejuízo para as economias africanas anualmente. Muitos ataques são originados em outros países, inclusive da própria África"[667]. Nisso, autores como Broadhurst[668] exortam a necessidade de cooperação multilateral e multissectorial para lidar com o problema. Conforme o Cepik et al, "em 2012, com apoio da União Europeia e da *International Telecommunication Union (ITU), a South African Development Community* (SADC) adoptou um modelo legal harmonizado para a caracterização de crimes cibernéticos, no âmbito do projecto Support for Harmonization of the ICT Policies in Sub-Saharan Africa (HIPSSA2)"[669]. Entretanto, African Union-Symantec destaca que "em

[663] Ibidem, p.7 (7-25).
[664] Ibidim, p.3 (3-25).
[665] Ibidem, p.3 (3-25).
[666] CEPIK, Marco Aurélio Chav, ibidem , ***ob. cit***. p.3 (4-25).
[667] ibidem, p.4 (4-25).
[668] ibidem, p.4 (4-25).
[669] Ibidem, p.4 (4-25).

2016, apenas 11 dos 54 países africanos possuíam leis contra crimes cibernéticos"[670]. Enquanto isso, "Moçambique assinou, em 2018, a Convenção da União Africana sobre Segurança Cibernética e Protecção de Dados Pessoais[671].

Em conformidade com International Telecommunication Union (ITU), ainda em 2018, Moçambique obteve um escore de 0,158 no *Global Cybersecurity Index* (GSI), ocupando a posição número 26 entre 42 países da África e a posição 132 entre 175 países no mundo[672]. Um dos indicadores que compõe o pilar organizacional do GSI é a existência de documentos formais de estratégia.

[670] ibidem, p.4 (4-25).
[671] ibidem, p.4 (4-25).
[672] ibidem, p.4 (4-25).

CAPÍTULO VI- ANÁLISE, INTERPRETAÇÃO E DISCUSSÃO DOS RESULTADOS

Para a análise, interpretação e discussão dos resultados fizemos uso de dois métodos: *(a) a triangulação teórica e (b) a triangulação de localização*. A **triangulação de teorias** consistiu no uso de várias estruturas ou perspectivas teóricas. O estudo usou uma série de teorias para avaliar seus dados e comparar seus resultados extraídos de diferentes perspectivas. Esse método ajudou na descoberta de várias facetas ou explicações para o fenómeno do cibercrime, enriquecendo e aprofundando a análise. **A triangulação de localização** consistiu no estudo do cibercrime no direito comparado. Esse método facilitou a localização de elementos gerais ou específicos do cibercrime no direito comparado face a globalização, para subsumi-los no contexto moçambicano.

6.1. Análise e Interpretação dos Dados (sobre o Cibercrime)

Do ponto de vista da triangulação teórica, a criminalidade informática apresenta dois sentidos: sentido amplo e sentido estrito. Nessa perspectiva, SILVA, dissertando sobre este assunto, afirma que "em sentido amplo, a criminalidade informática engloba toda actividade criminosa realizada por computadores ou meios de tecnologia da informação"[673]. Em sentido estrito, a criminalidade de informação engloba os crimes, que de acordo com SIMAS "o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital". Dessa forma, SIMAS definiu o cibercrime como sendo "as infracções penais praticadas no âmbito digital ou que estejam envolvidos com a informação digital, mediante as condutas atentatórias aos direitos fundamentais, de pessoas físicas e pessoas jurídicas através dos mais diversos meios e dispositivos conectados à internet, tais como computadores, celulares e outro"[674].

No nosso entendimento, a informática pode ser um instrumento de práticas de crimes tradicionais, isto é, que não necessitam de suporte informático para serem realizados, nem sendo parte legal. Nesse corolário, podemos citar crimes cometidos contra a honra e a dignidade da pessoa humana, que podem ser cometidos com recurso em meio informático para divulgação

[673] SILVA, Paulo Quintiliano da, ***Dos Crimes Cibernéticos e seus efeitos internacionais***. Procedings of the Firts International Conference on Forensic Computer Science Inv estigation (ICoFCS´2006)/ Departamento de Polícia Federal (ed.) Brasília, Brazil, 2006,124 pp.- ISSN 19180-1114. Apud SOBRINHO, Jéssica R. Nunes; et.al, ob. cit. p. 3.

[674] SIMAS, Diana Viveiros de, ***O cibercrime***. 2014. 168f. Dissertação (Mestrado em Ciências Jurídicoob.citForenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa, 2014. Disponível em: http://hdl.handle.net/10437/5815. Acesso em: 18 maio 2021. Apud SOBRINHO ….. ibidem, p. 3

(e-mail, whatsap e outros). Outros casos que se podem inferir são situações em que a informática surge como "elemento integrador, isto é, podendo o bem jurídico protegido não ser unicamente com a informática, como é o caso de crimes contra *softwares* em que o bem jurídico protegido é autoral. Nisso, ilidimos que Cibercrimes são os delitos penais cometidos por meio digital ou que estejam envolvidos com a informação digital.

Os crimes informáticos reflectem novos interesses, essencialmente no âmbito social a serem protegidos pelo Estado. Nessa perspectiva, há toda uma necessidade pela tutela penal de bens jurídicos emergentes, oriundos de avanços tecnológicos. Por isso, este nosso entendimento pode ser harmonizado com o enfoque de VIANA, quando alude que "as novas tecnologias proporcionaram inúmeros avanços à colectividade, sendo que as pessoas estão cada vez mais conectadas nas "redes" e as informações em geral passaram a ser mais valiosas, tanto para o indivíduo, quanto para as empresas e entidades governamentais. Contudo, noutra perspectiva, verifica-se que, em grande proporção, a informática passou a ser utilizada como um meio ao cometimento de crimes, além de fazer surgir novas condutas relacionadas à invasão de dispositivos electrónicos, o que, em tese, implica a violação de bens jurídicos individuais ou colectivos" [675].

É certo que o bem jurídico em questão é a segurança informática. Dai que em uma abordagem constitucional da segurança informática, é possível vislumbrar que há uma preocupação com **a protecção de dados pessoais** constantes de registos informáticos, as condições de acesso aos bancos de dados, de constituição e utilização por autoridades públicas e entidades privadas destes bancos de dados ou de suportes informáticos. No nosso entender, os crimes cibernéticos violam bens jurídicos garantidos pela Constituição da República de Moçambique, desde logo: a intimidade, a liberdade de expressão, a privacidade, entre outros de suma importância.

A necessidade de evitar confusão na divisão da jurisdição, de modo a determinar, face a um caso concreto, qual o tribunal que, atento sua espécie, o referido caso concreto deve ser entregue e, por acréscimo, dentre os tribunais da mesma espécie, qual em concreto deve ser chamado a conhecer do caso, leva a que seja necessário regulamentar através da lei, de forma geral e abstracta, o âmbito de actuação de cada tribunal, permitindo o diferimento de cada caso de natureza penal a um único tribunal.

[675] VIANA, Lucas Freitas, .

A partir do estudo do cibercrime no direito comparado, é possível fazer a triangulação dos dados do cibercrime no brasil, Portugal e Espanha, sem descurar das convenções internacionais sobre o cibercrime.

No Brasil, existem, hoje, algumas políticas públicas implementadas em atenção aos Cibercrimes, como por exemplo "a Estratégia Nacional de Segurança Cibernética – E-Ciber – aprovada somente em fevereiro de 2020, porém eleita pelo Gabinete de Segurança Institucional da Presidência da República, em janeiro de 2019, como o primeiro módulo da ENSI (Estratégia Nacional de Segurança da Informação), esta elaborada a partir do Decreto nº 9637, de 26 de dezembro de 2018, para implementação da Política Nacional de Segurança da Informação. Existem, no Brasil, órgãos que actuam no combate ao cibercrime, desde logo: o Ministério público, as delegacias especializadas em cibercrime entre outros órgãos". Com efeito, foi com a promulgação da Lei 12735/12, que ficou estabelecida a criação nos órgãos da polícia judiciária, de departamentos e grupos especializados na actuação contra cibercrimes.

Ainda no âmbito do direito comparado, a legislação Espanhola refere-se aos tratados europeus e convenções assinados em matéria do cibercrime da seguinte forma: "Conclusões do Conselho de 26 de Abril de 2010 sobre Plano de Acção Contra o Cibercrime" e "Conclusões da Presidência sobre a Conferência de Cibercrime que teve lugar a 12-13 de Abril 2011 em Budapeste"[676].

Já em Portugal, a partir de 1991, como apregoa Vidigal[677], foram criadas regras especificas relativas ao cibercrime, tendo sido produzida a Lei da Criminalidade Informática, Lei 109/91, de 17 de Agosto. Posteriormente foi criada a Lei do Cibercrime, Lei 109/2009, de 15 de Setembro. Esta nova lei " (…) estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa"[678].

---

[676] VIDIGAL, Inês Maria Andrade, apud VIDIGAL, Inês Maria Andrade, As Políticas de Combate a Cibercrime na Europa, Dissertação de Mestrado em Políticas Europeias, Instituto de Geografia e Ordenamento Territorial, Universidade de Lisboa, 2012, p.67.

[677] VIDIGAL, Inês Maria Andrade, ibidem, p. 92.

[678] BDJUR (2011) ***Código do direito de autores e dos direitos conexos,*** Almedina, pp. 151- 166. Apud VDIGAL, Inês Maria Andrade, ***ob., cit.,*** p. 92.

A Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais ("CUACPDP") disciplina, no seu capítulo III, a matéria relativa a "*Promoção da Cibersegurança e a Luta contra o Cibercrime*".

6.2. Discussão dos Resultados sobre Cibercrimes e sua Repercussão no Direito Penal Moçambicano.

O estudo teve como pergunta de partida a seguinte: *até que ponto o quadro jurídico-penal moçambicano tutela, cabalmente, os crimes cibernéticos?* Para responder à esta pergunta, avançamos com as seguintes hipóteses: (a) Moçambique tutela cabalmente os crimes cibernéticos, pois ratificou todas convenções internacionais sobre o cibercrime e tipificou totalmente toda a espécie dos cibercrimes. (b) Moçambique ainda não tutelou cabalmente os crimes cibernéticos, pois ainda não ratificou todas as convenções internacionais sobre o cibercrime e tipificou parcialmente os cibercrimes.

Moçambique não ratificou a convenção de Budapeste sobre cibercrime, mas ratificou através da resolução n° 5/2019 de 20 de Junho a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais. As previsões constitucionais referenciadas no art. 71 da CRM servem apenas para ilustrar que existe, certamente, uma preocupação constitucional com os aspectos elementares nos quais a segurança informática objectiva proteger; ainda que não trate explicitamente da questão em debate - o bem jurídico protegido pelos crimes cibernéticos.

As preocupações com a segurança cibernética vêm se avolumando desde que o país decidiu enveredar pela massificação do uso das TIC`s, quando o Governo aprovou a primeira Política de Informática, através da Resolução número 28/2000, de 12 de Dezembro, que 18 anos depois foi revista e aprovada sob a nova perspectiva de Política para a Sociedade da Informação, através da Resolução nº 17/2018, de 21 de Junho. Com efeito, o Governo de Moçambique tem a questão da segurança cibernética como uma das suas prioridades. Nisso, por Resolução n.º 69/2021 de 31 de Dezembro, o Governo Moçambicano aprovou a Política de Segurança Cibernética e Estratégia da sua Implementação, com vista a adequá-la aos instrumentos orientadores e aos desafios impostos pelo crescente progresso das Tecnologias de Informação e Comunicação (TIC's).

A Política de Segurança Cibernética é um instrumento, parte da materialização da Política para a Sociedade de Informação, aprovada por Resolução n.º 17/2018, de 21 de Junho,

que visa orientar os esforços de Moçambique na resolução dos novos problemas trazidos pela revolução tecnológica, que passa por acções que garantam: (a) a regulamentação de funcionamento do espaço cibernético; (b) o desenvolvimento de capacidade institucional e operacional em matéria de segurança cibernética; (c) a protecção de infra-estruturas críticas e activos de informação; (d) O ordenamento da coordenação e colaboração institucional em matéria de segurança cibernética; (e) a promoção de boas práticas no uso das TIC's.

Para além da Política de Segurança Cibernética e da Política Informática, existe uma série de outros instrumentos orientadores e regulatórios do sector das TIC`s que foram sendo aprovados e implementados pelo Governo ao longo dos últimos anos, dos quais se destacam - a Política para a Sociedade da Informação, a Lei de Transacções Electrónicas, Lei n.º 3/2017, de 9 de Janeiro, a Lei de Telecomunicações,[679] Lei n.º 4/2016, de 3 de Junho, o Regulamento do Quadro de Interoperabilidade de Governo Electrónico, o Decreto nº 67/2017, de 1 de Dezembro[680], o Regulamento de Segurança de Redes de Telecomunicações, Decreto n.º 62/2019, de 1 de Agosto[681], o Regulamento do Sistema de Certificação Digital de Moçambique, Decreto n 59/2019, de 1 de Dezembro, o Regulamento do Domínio[682] ".mz", Decreto n.º 82/2020, de 10 de Setembro, a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais, Resolução n.º 5/2019, de 20 de Junho e as recentes[683] iniciativas legislativas referentes ao Código Penal, que, de um modo geral, permitiram dar cobertura universal aos crimes de natureza informática no país[684].

O Código Penal moçambicano aprovado pela Lei n.º 24/2019, de 24 de Dezembro, nas disposições gerais contempla o princípio da territorialidade (artigo 4) e, factos praticados fora do território nacional (artigo 5), consentâneos com o artigo 22 da Convenção de Budapeste; prevê infracções contra a confidencialidade de sistemas informáticos, integridade e disponibilidade de sistemas informáticos e dados informáticos: os crimes de "devassa da vida privada" (art. 252), "base de dados automatizada" (art. 254), "acesso Ilegítimo" (art. 256), "gravações ilícitas" (art. 257), "burla informática e nas comunicações" (art. 289), "fraudes relativas aos instrumentos e canais de pagamento electrónico" (art. 294);

---

679 Cfr., Lei n.º 3/2017, de 9 de Janeiro***, aprova a Lei de Transacções Electrónicas***,

680 Cfr., O Regulamento do Quadro de Interoperabilidade de Governo Electrónico (Decreto n 67/2017, de 1 de Dezembro).

681 Cfr., Decreto n.º 62/2019 de 1 de Agosto***, aprova o Regulamento de Segurança de Redes de Telecomunicações***

682 Cfr., Resolução n.º 5/2019 de 20 de Junho, ***rectifica a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais*** *in* Boletim da República.

683 Cfr., Resolução n.º 5/2019 de 20 de Junho, ***rectifica a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais***.

684 Cfr., Resolução 69/2021 de 31 de Dezembro.

Chama-se também à colação de determinadas formas de cometimento dos crimes de "difamação" (art. 233) e "injúria" (art. 234), na parte em que a Lei se refere à «qualquer outro meio de publicação»; a secção do CP respeitante à "falsidade informática e crimes conexos", nos quais se incluem os crimes de "falsidade informática" (art. 336), "interferência em dados" (art. 337), "interferência em sistemas" (art. 338), "uso abusivo de dispositivos" (art. 339). Inclui, igualmente, infracções relacionadas aos conteúdos sobre: pornografia de menores (artigo 2011); utilização de menores em pornografia (artigo 212), distribuição ou posse de pornografia de menores (artigo 213 do CP). Finalmente, estabelece formas de responsabilidade e sanções e responsabilidade das pessoas colectivas em conformidade com os artigos 11 e 12 da Convenção de Budapeste.

Destaca-se que no âmbito dos crimes informáticos é extremamente difícil indicar o exacto momento da prática do acto ilícito, para que seja aplicada a consequente sanção penal. Isto porque, no meio informático existe uma dissociação temporal, pois é possível programar a execução de um crime informático no tempo, ou seja, o acto ilícito pode ser executado meses após a sua programação, devido o facto de todo computador possuir um relógio interno. O nosso Código Penal adoptou a teoria da actividade para descrever o momento do crime. Assim sendo, a prática de um crime ocorre no momento da acção ou omissão, independentemente do momento do resultado (art. 2 do CP). Em matéria do local e momento da prática do cibercrime é necessário a aplicação de alguns princípios do Código Penal, mais precisamente quanto a territorialidade (art. 4 do CP), extraterritorialidade (art. 5 do CP), nacionalidade, defesa (art.2 do CPP) e representação (art. 7 do CPP).

Tendo em conta a doutrina dominante sobre a competência territorial para julgar os crimes cibernéticos, entendemos que a teoria do resultado com relação ao lugar da prática do crime cibernético mostra-se mais ajustada. Deste modo, sugerimos que de *iure condendo,* **seja adoptada a teoria do resultado com relação ao lugar da prática do crime cibernético. Assim, a competência para julgar um crime cibernético, seria o local onde se encontre o computador violado, pois nesse local é onde houve a consumação do crime.**

Em conformidade com o artigo 15 da Convenção de Budapeste sobre o cibercrime, o Código de Processo Penal (CPP) moçambicano, aprovado pela Lei n° 25/2019 de 26 de Dezembro, prevê princípios fundamentais e garantias do processo penal, designadamente: direito fundamental de presunção de inocência (artigo 3); proibição de provas obtidas por meios ilícitos (artigo 4); princípio do contraditório (artigo 5); direitos da pessoa detida (artigo 6); direito a defensor (artigo 7); e dever de fundamentação (artigo 8).

Ainda o CPP permite o recurso às escutas telefónicas (artigos 222 e 225), como meios de obtenção de prova, na criminalidade informática, em conformidade com o artigo 21 da Convenção de Budapeste sobre o cibercrime. A escuta, considerado meio especial de obtenção da prova, "consiste na intercepção e a gravação de conversas ou comunicações telefónicas, acto coordenado ou autorizado por despacho do juiz competente…" (art. 222 e ss). Nisso, aquele que interceder as comunicações sem que para tal seja autorizado (…), comete a infracção de intercepção ilegal das comunicações (…)", punível nos termos do art. 64.º da Lei n.º 8/2004, de 21 de Julho (Lei das Telecomunicações).

O CPP moçambicano prevê outros meios de obtenção da prova, em conforme, desde logo: (a) os exames, "realizados em pessoas, lugares das coisas, inspecção dos vestígios que possa ter deixado o crime e todos os indícios relativos ao modo como e lugar onde foi praticado, as pessoas que o cometeram ou sobre as quais foi cometido" (art. 206.º e ss.); (b) revistas e buscas, nos casos em que haja indícios de que alguém oculta na sua pessoa quaisquer objectos relacionados com um crime ou que possa servir de prova (art. 209.º e ss.); (c) as apreensões dos objectos que tiverem servido ou estivessem destinados a servir a prática de um crime (art. 213.º e ss.)

A Lei de Cooperação Internacional de Moçambique (Lei n°21/2019 de 11 de Novembro) tem disposições relativas ao pedido de extradição de Moçambique para outros Estados (artigos 32 -68). Prevê no artigo 157 a possibilidade do auxílio mútuo em matéria de *interceptação de dados de conteúdo,* conforme o artigo 34 da Convenção de Budapeste sobre o cibercrime.

No mesmo sentido o artigo 25 n°2 da Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais, rectificada pela Resolução n.º 5/2019, de 20 de Junho, insta que "cada Estado-parte deve adoptar medidas legislativas e ou regulamentares que julgar necessárias para conferir `as responsabilidades específicas às instituições – quer as instituições existentes quer novas – assim como os funcionários destas instituições que forem designados, a fim de lhes conferir autoridade estatutária e a capacidade legal de agir em todos os aspectos da aplicação à cibersegurança não se limitando a dar respostas aos incidentes nestes domínio, coordenação e cooperação em matéria da justiça, investigação forense, julgamentos, etc.", directriz que encontra acolhimento no estabelecido, no que tange às competências do SERNIC, preceituados na alínea g) do artigo 6 e alínea c) do n.º 1 do artigo 7, ambos da Lei que cria o SERNIC, **(**Lei n.º 2/2017 de 9 de Janeiro**),** que atribuem a este organismo poderes

funcionais para investigar crimes informáticos e estabelecer ligações com a INTERPOL no que à cooperação judiciária diz respeito.

Comparando o quadro jurídico-penal moçambicano com as convenções internacionais sobre o cibercrime, constatam-se algumas lacunas, desde logo: *(a) a legislação moçambicana ainda não contempla disposições específicas da prova digital no âmbito dos meios de obtenção de prova, como seja a conservação expedita de dados informáticos; pesquisa de dados informáticos; apresentação de dados informáticos e injunção para a apresentação ou concessão de acesso de dados, o que dificulta as investigações; (b) não ratificação ainda da convenção de Budapeste, que facilitaria a cooperação internacional e a recolha de obtenção de prova digital.*

Ainda, existem condutas atípicas que não podem ser punidas em decorrência do princípio da legalidade, sendo insuficientes para combater os crimes cibernéticos a aplicação das legislações vigentes. Dentre as condutas atípicas destaca-se: (i) danos relativos a programas ou outros dados informáticos; (ii) sabotagem informática; (iii) reprodução ilegítima de programa protegido; dentre outras condutas atípicas.

Os crimes cibernéticos ocorrem no mundo inteiro, sem respeitarem fronteiras, por isso, o Moçambique deve adoptar a legislação específica sobre o cibercrime e aderir a tratados internacionais, *máxime,* a Convenção de Budapeste sobre o cibercrime.

CONSIDERAÇÕES FINAIS

Moçambique, como Estado Democrático e Social de Direito, não pode ser dissociada a tutela penal de um pressuposto bem jurídico, sendo que somente será considerada legítima, sob a óptica constitucional, quando for socialmente necessária, ou seja, quando imprescindível para assegurar as condições de vida, desenvolvimento e paz social, haja vista o fundamento maior da liberdade e da dignidade da pessoa humana. Nesse corolário, o Direito sobressalta-nos a ideia de adaptação social, de interacção e pacificação das relações do homem consigo próprio e com o meio em que vive; dai que, a natureza do Direito Penal está intrinsecamente ligada à existência de violência e de excessos que gravemente ofendem o convívio social.

A criminalidade é um fenómeno social normal, pois ocorre em todas as sociedades constituídas por seres humanos. O objectivo do Direito Penal é a tutela subsidiária (de "ultima ratio") de bens jurídicos com dignidade penal. É importante sublinhar, que a realidade do crime depende da reacção social, quer pelas instâncias formais (legislador, polícia, Ministério Público, Juiz), quer pelas instâncias informais (família, escolas, igrejas, clubes, vizinhos).

Estamos perante a Revolução tecnológica, nova era, a era tecnológica, a digital, na qual a nova sociedade da informação depara-se com uma explosão da comunicação, era de consumo, e, actualmente, um dos grandes combates do Direito é garantir aos usuários a protecção no ambiente virtual. Por isso, é importante a prevenção e cuidado sobre como é divulgado e exposto informações pessoais, pois, por mais simples e inocente pareça ser, a mesma pode usada de diferentes formas para obter dados que possibilitam os crimes cibernéticos. É fundamental obtermos conhecimento sobre quais os crimes mais comuns cometidos por esses infractores e as leis que buscam conferir protecção jurídica às pessoas expostas a esses delitos.

O sistema jurídico português exerceu uma significativa influência no desenvolvimento do Direito Penal moçambicano, devido ao passado histórico e à relação colonial entre Portugal e Moçambique. Durante o período colonial, que durou até a independência de Moçambique, em 1975, o sistema jurídico português foi aplicado no País. Assim, como resultado, o Direito Penal moçambicano foi inicialmente moldado pelo sistema jurídico português, que se baseia no sistema romano-germânico. Várias leis portuguesas foram adoptadas em Moçambique e serviram como a base para o Código Penal e outras legislações penais moçambicanas, como foi o caso do Código Penal aprovado pelo Decreto de 16 de Setembro de 1886. Após a independência, Moçambique passou a adoptar um sistema jurídico próprio. Mas a influência do Direito Penal português permaneceu presente. Embora o País tenha feito esforços para

desenvolver sua legislação penal de acordo com as necessidades e realidades locais (a titulo ilustrativo, o Código Penal aprovado pela Lei nº 35/2014, de 31 de Dezembro), posteriormente, revogado pela Lei nº 24/2019, de 24 de Dezembro, que aprova o novo Código Penal vigente, e a Lei nº 25/2019, de 26 de Dezembro, que aprova o novo Código do Processo Penal, demais legislação complementar (Código de Execução de Penas, aprovado pela Lei nº 26/2019, de 27 de Dezembro), muitos princípios e conceitos jurídicos do sistema português ainda são reconhecidos e aplicados em Moçambique.

De facto, o Código Penal, aprovado pela Lei nº 35/2014, de 31 de Dezembro (ora revogado), trouxe grandes inovações ao introduzir novos tipos legais de crimes (inclusive trouxe inovações na criminalidade informática, como se pode depreender no título III daquele dispositivo legal, do art. 316 a 326), alterações na redacção e nas modularas penais e incorporação de matérias que constavam da legislação avulsa. Esta adoptou o movimento da descriminalização e a preferência por penas não privativas de liberdade à pena de prisão, passando a situar no Homem a sua dimensão máxima. Entretanto, por razões de fundo, traduzidas na limitação à abordagem dos seus valores axiológicos e a necessidade de tratamento jurídico particular, nomeadamente em sede de articulação entre normas substantivas e processuais específicas, passaram a justificar a afectação sistemática dos lapsos e omissões por uma vicissitude legal.

Em relação ao Código Penal vigente (Aprovado pela Lei nº 24/2019, de 24 de Dezembro), prevê infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos[685]; contempla também infracções relacionadas com computadores[686] assim como infracções relacionadas com o conteúdo[687]. No nosso entendimento, o tratamento destes crimes na legislação penal moçambicana é indistintível, apesar de, em alguns momentos, o legislador referir especialmente aos crimes cibernéticos, mas em todos os casos correlaciona-os directamente com os crimes informáticos. A título ilustrativo, é o caso do crime de base de dados automatizados, conforme o art. 254. ° do CP, onde com recurso aos "meios informáticos e à internet", o agente cria, mantem ou utiliza ficheiro automatizado de dados individualmente identificáveis e relativos às convicções políticas,

[685] Acesso ilegítimo (artigo 256º); Intercepção ilegítima (artigo 256, nº 2); Violação de correspondência ou de comunicações (artigo 253º); Interferência em dados (artigo 337º); Interferência em sistemas (artigo 338º) e Uso abusivo de dispositivos (artigo 339º).
[686] Falsidade informática (artigo 336º) e Burla informática e nas comunicações (artigo 289º)
[687] Pornografia de menores (artigo 211º); Utilização de menores em pornografia (artigo 212º); Distribuição ou posse de pornografia de menores (artigo 213º)

filosóficas ou ideológicas, à fé religiosa, à filiação partidária ou sindical e à vida privada de outrem". O mesmo sucede com o crime de acesso ilegítimo (n.° 2 do art. 256. ° do CP) "ao dispositivo informático alheio com a finalidade de tomar conhecimento de certa informação ou objecto de natureza privada, ou seja, que não sejam públicos", entre outros casos previstos no CP.

Tendo em revista o Código Penal vigente, sobressalta-nos que não dispõe de condutas específicas relacionadas a tipos penais exclusivos aos crimes cibernéticos, deixando criminalmente impunes situações tais como *intercepção ilegítima; interferência em dados; danos relativos a programas ou outros dados informáticos; sabotagem informática, etc*.

Outrossim, Moçambique ainda não está preparada para garantir a segurança jurídica necessária para a sociedade mediante os ataques dos criminosos no âmbito virtual. Nisso, há uma insuficiência ou ausência de norma penal, tipificando, de forma precisa, os crimes digitais, o que limita a função punitiva estatal, uma vez que influência na sensação de insegurança e impunidade, com repercussão negativa para a sociedade e, em especial, para a comunidade internacional, que há mais de uma década vem chamando a atenção para a necessidade e urgência de controlo e prevenção de condutas delituosas no ciberespaço: 1. a legislação moçambicana ainda não contempla Disposições Específicas da prova digital no âmbito dos meios de obtenção de prova como sejam a conservação expedita de dados informáticos; Pesquisa de dados informáticos, Apreensão de dados informáticos e Injunção para apresentação ou concessão do acesso a dados, o que dificulta as investigações; 2. Moçambique ainda não ratificou a Convenção de Budapeste, que facilitaria a cooperação internacional e a recolha de obtenção de prova digital; 3. Falta de equipamento tecnológico adequado para os profissionais de justiça criminal bem como a falta de pessoal qualificado em matéria de criminalidade informática. Desse modo, a legislação moçambicana tem dificuldade em acompanhar a evolução tecnológica, pois a cada dia surge um novo delito nesse ambiente, do qual o legislador não é capaz de caminhar em paralelo com essas evoluções, e consequentemente os crimes virtuais não recebem as devidas punições, deixando a sensação de impunidade.

Está evidente pelos informes do MP, há aumento e a sofisticação da criminalidade cibernética em Moçambique. Nesse corolário, ressalta-nos afirmar que embora a recente reforma da legislação penal tenha trazido inovações na criminalidade informática, a dinâmica desta criminalidade impõe a aprovação de uma lei específica que contemple outras manifestações do cibercrime e estabeleça, na componente processual, medidas especiais de recolha, conservação e manutenção da prova, bem como de análise forense, prevenção de

perdas, maneio de incidentes e avaliação de risco, assegurando, assim, uma investigação profícua. Neste contexto, é essencial potenciar a área das tecnologias de informação e comunicação, com pessoal especializado, impondo-se, assim, a formação de peritos informáticos para auxiliarem na investigação, sobretudo, na recolha e tratamento de prova digital ou electrónica.

A adesão de Moçambique à Convenção de Budapeste sobre o Cibercrime contribuiria para a facilitação da cooperação internacional, nesta matéria, pois estamos em face de criminalidade organizada, com natureza transnacional. De facto, há necessidade de o processo penal acompanhar novas exigências da sociedade, trazendo soluções concretas dos problemas básicos do Direito Processual Penal. Nesse corolário, a efetivação do processo penal visa essencialmente a realização da justiça e a descoberta da verdade material, a protecção dos direitos fundamentais e o restabelecimento da paz jurídica, através da aplicação de uma sanção penal ao arguido que violou específicos bens jurídicos protegidos pelo Direito Penal.

Na esfera penal moçambicana, é fundamental que sejam criados mecanismos específicos para combater com mais eficiência e mais eficácia os crimes cibernéticos. Para o efeito, o ordenamento jurídico deve acompanhar os avanços dos delitos cibernéticos potenciando as áreas das tecnologias de informação e comunicação, com pessoal especializado, impondo-se, assim, a formação de peritos informáticos para auxiliarem na investigação, sobretudo, na recolha e tratamento de prova digital ou electrónica. Outrossim, uma das principais medidas para a prevenção e combate à criminalidade informática é a actualização permanente do nosso quadro legislativo, de modo a acompanhar a evolução deste tipo de criminalidade e os instrumentos jurídicos internacionais sobre a matéria.

Ressalta-nos concluir que as dificuldades de natureza técnicas e financeiras, encaradas pelas instituições públicas e privadas, têm vindo a contribuir para o enfraquecimento, o acompanhamento e esclarecimento pleno dos crimes cometidos em meios digitais. Consequentemente, o País (Moçambique, a par de outros Estados) continuará vulnerável aos ataques nos seus sistemas informáticos, pondo em causa a segurança e funcionamento normal dessas instituições. Nessa senda, há necessidade de o Governo priorizar nos seus investimentos nesta matéria, meios técnicos, materiais e humanos de modo a criar segurança tanto para os utentes assim como para os prestadores dos serviços, investimento este que deve também abranger aos órgãos da administração da justiça para que estes estejam a altura de esclarecer delitos cometidos por meio destas plataformas digitais. A formação deve ter como base o cibercrime, incluindo matérias de segurança informática e cooperação jurídica e judiciária.

Na mesma perspectiva, é necessário tomar uma estratégia tendo em atenção a velocidade de actuação dos infractores, o carácter transaccional e a complexidade dos delitos virtuais, como qualificar magistrados e investigadores, bem como o seu apetrechamento em meios tecnológicos adequados.

O cibercrime desafia os valores fundamentais que o mundo defende, se tivermos em consideração ao Direito Comparado: direitos humanos, democracia e o Estado de Direito. O aumento da importância e da utilização das tecnologias de informação e comunicação em todos os domínios do comércio global e da sociedade revela-se o grande motivo para o combate ao cibercrime, exigindo uma regulação multidisciplinar. Um ataque a determinada empresa ou instituição pública pode implicar, além de prejuízos monetários muito significativos, o acesso a dados confidenciais. Além disso, este tipo de ataques favorece a perda de confiança dos clientes nas empresas e dos cidadãos nos governos que os representam, o que pode levar à descredibilização de empresas e governos, à perda de poder das empresas no mercado global e de influência de Estados em assuntos maiores de política internacional.

Buscando experiências no âmbito do Direito Comparado, somos de sugerir que o Estado Moçambicano formule estratégias no sector da educação, mas virada para utilizadores da internet. Isto por que a educação dos utilizadores da internet reduz o número de potenciais alvos de ataques cibernéticos. Os utilizadores podem ser educados através de campanhas públicas, aulas em escolas, bibliotecas, centros de informação e universidades, assim como através de parcerias público-privadas. Uma condição importante para uma educação eficiente – que poderá ser desenvolvida como estratégia de informação – será uma comunicação aberta e rigorosa sobre as últimas ameaças de cibercrimes por parte dos Estados e do sector privado (empresas, etc.).

Quanto às investigações policiais de cibercrimes, se o criminoso e a vítima estão localizados em países diferentes, o sucesso das investigações depende da cooperação entre as autoridades policiais de todos os países afectados. A soberania nacional não permite investigações dentro do território de diferentes países sem a permissão das autoridades locais. As investigações de cibercrime precisam do apoio e do envolvimento das autoridades de todos os países envolvidos.

Tendo em conta a doutrina dominante sobre a competência territorial para julgar os crimes cibernéticos, entendemos que a teoria do resultado com relação ao lugar da prática do crime cibernético mostra-se menos ajustada. Assim, sugere-se que de *iure condendo,* seja adoptada a teoria do resultado com relação ao lugar da prática do crime cibernético. Assim, a

competência para julgar um crime cibernético, seria o local onde se encontre o computador violado, pois nesse local é onde houve a consumação do crime.

Portanto, ressalta-nos afirmar que a criminalidade informática enquadra-se em uma área específica de incriminação penal, podendo, com os instrumentos do Direito Penal clássico, dar-se um estudo contínuo dessa área específica da incriminação. Partindo desse pressuposto, o legislador penal pátrio deverá considerar a criação de um Direito Penal informático, como uma disciplina jurídico-penal autónoma, como tem acontecido em outros ordenamentos jurídicos onde ocorre autonomização, do mesmo modo - um Direito Penal patrimonial, um Direito Penal dos crimes contra a vida, um Direito Penal dos crimes contra a integridade física, e assim sucessivamente. Ou seja, teríamos uma parte especial com diferentes e autónomas áreas ou zonas de incriminação.

REFERÊNCIAS BIBLIOGRÁFICAS

Os Documentos Legislativos.

- MOÇAMBIQUE, República de. *Constituição da República de Moçambique* (2004), que inclui a Lei de Revisão Pontual da Constituição (Lei nº 1/2018, de 12 de Junho, publicado no Boletim da República, 1ª Série – nº 115, 2º Suplemento, de 12 de Junho de 2018.

- _____ *Código Civil* (CC), O Código Civil de 1966, aprovado como Código Civil português, pelo Dec – Lei nº 47344, de 25 de Novembro de 1966 e extensivas as províncias ultramarinas pela Portaria nº 22 869, de 4 de Setembro de 1967.

- _____*Código do Processo Civil* (CPC), ora, aprovado pelo Decreto-lei nº 44.129, de 28 de Dezembro de 1961, tornado extensivo ao Ultramar pela Portaria nº 19305, de 30 de Julho de 1962, e entrou em vigor a 1 de Janeiro de 1963. Foi revisto pelo Decreto-Lei nº 1/2005, de 27 de Dezembro, publicado no Boletim da República, 1ª Série – nº 51, 5º Suplemento, de 27 de Dezembro de 2005, posteriormente alguns artigos sofrem alterações por força do Decreto-Lei nº 1/2009, de 24 de Abril, Publicado no Boletim da República, 1ª Série, nº 16, 3º Suplemento, 24 de Abril de 2009.

- _____ *Código Penal* (CP), O Código Penal de 1886, ora vigente, foi aprovado pelo Decreto de 10 de Setembro de 1886, revogado pela Lei nº 35/2014, de 31 de Dezembro, posteriormente revogada pela Lei nº 24/2019, de 24 de Dezembro, que aprova o CP Vigente, publicada no Boletim da República, 1ª Série, nº 249, de 26 de Dezembro de 2019.
- _____*Código do Processo Penal* (CPP), ora vigente foi aprovado pelo Decreto nº 16489 de 15 de Fevereiro de 1929 e mandado a vigorar na então colónia de Moçambique, pela Portaria nº 19271, de 24 de Janeiro de 1931, revisto pela Lei nº 25/2019 de 26 de Dezembro, publicada no Boletim da República, 1ª Série, nº 248, de 26 de Dezembro de 2019.
- _____ Lei n.º 3/2017, de 9 de Janeiro, *aprova a Lei de Transacções Electrónicas*, *in* Boletim da República, I Série, número 212 de 9 de Janeiro.

- _____, Lei n.º 4/2016, de 3 de Junho, *aprova a lei das Telecomunicações in* Boletim da República, I Série, número 118 de 3 de Junho.

- _____, Decreto n.º 62/2019 de 1 de Agosto, *aprova o Regulamento de Segurança de Redes de Telecomunicações in* Boletim da República.
- _____, o Regulamento do Quadro de Interoperabilidade de Governo Electrónico, o Decreto n 67/2017, de 1 de Dezembro.

- _____, Resolução n.º 5/2019 de 20 de Junho, *rectifica a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais in* Boletim da República.

- _____, Resolução 69/2021 de 31 de Dezembro, ***aprova a***

política de segurança cibernética e a estratégia de sua implementação, *in* Boletim da República, I série, número 253 de 31 de Dezembro.

II. Doutrina/Livros/Monografias e diversas obras.

- APPHIAH, Kwame Anthony, ***Na casa d*e ***meu pai: a África na filosofia da cultura,*** Contraponto, Rio de Janeiro, 1997**.**

- ALVIM, Carreira, ***Teoria Geral do Processo***, revista, ampliada e actualizada, Editora Forense, Rio de Janeiro, 2009. p. 260.
- ATHENIENSE, Alexandre. **Crimes virtuais*: crimes vigentes e soluções projectos de lei***. 2000.
- ANDERSON, Benedict. ***Nação e consciência nacional***, Companhia das Letras, São Paulo, 2008.
- ANTUNES, Maria João, Direito Processual Penal, 3ª Ed., Coimbra Editora, Lisboa, 2004.
- ASCENSÃO, José Oliveira, O Direito, Introdução e Teoria Geral, 10ª Ed., Editora Coimbra, Coimbra, 1997.
- ALBERGARIA, Jason, ***Criminologia Teórica e Prática***, 2ª Ed. Aide Editora, Rio de Janeiro, 1988.
- BARREIROS, José António. As instituições criminais em Portugal no século XIX: subsídios para sua a história. Análise Social. Lisboa, vol. XVI, 1980.
- BARROSO, Sérgio Luís, Furto De Uso, 1ª Edição, Editora Atlas, Brasil, 2011.
- BARATTA, Alessandro, ***Criminologia Crítica e Crítica do Direito Penal: Introdução à Sociologia do Direito Penal***, Editora Revan, Rio de Janeiro.
- BELLUCCI, Beluce, ***Economia contemporânea em Moçambique: sociedade linhageira,***
- ***Colonialismo, socialismo, liberalismo,*** EDUCAM, Rio de Janeiro, 2007.
- BELEZA, Teresa Pizarro, ***Direito Penal***, Vol. I, 2ª Ed. Revista e actualizada, Associação Académica da Faculdade de Direito Lisboa, Lisboa, 1998.
- BETTS, Raymond F, ***A dominação europeia: método e instituições***. Boahen, A. Adu. (Coord.) História Geral da África. África sob dominação colonial 1800-1935. Vol. VII. São Paulo: Ática UNESCO, 1991.
- BITTENCOURT, Cezar Roberto, ***Tratado de Direito Penal***. Vol. I, Saraiva, São Paulo, 2003.
- BOXER, Charles, O império colonial português, S/Ed. Edições 70, Lisboa, 1999.
- CAPEZ, Fernando, Curso de Direito Penal. 15ª Ed., Saraiva Editora, São Paulo, 2011.
- CARLOS, Soares, ***Uma visão panorâmica sobre o sistema cibernético e suas políticas***, Vol. III, Atlas Editora, Brasil, 2011.
- CAVALEIRO, Manuel de Ferreira, ***Lições do Direito Penal***, 4° Ed., Almeida Editora, Lisboa, 1982.
- CABETTE, Eduardo Luiz Santos, ***Direito penal parte especial***, S/Ed. Saraiva, São Paulo, 2012.
- CABAÇO, José Luís, ***Moçambique: Identidade, colonialismo e libertação***, Editora UNESP, São Paulo, 2009.
- CARVALHO, Americo Taipa de Direito Penal 2ª Ed. Coimbra Editora, Coimbra.

- CALENDO, André Jaime, ***Lei de Terras Anotada e Comentada***, S/Ed. CFJJ, Maputo, 2005.
- CISTAC, Gilles Et. Al, ***Contributo Para o Debate Sobre a Revisão Constitucional***, Faculdade de Direito da UEM, Maputo, 2004.
- COTA, Gonçalves, ***Projecto Definitivo do Código Penal dos Indígenas da colónia de Moçambique,*** Imprensa Nacional de Moçambique, Lourenço Marques, 1946.
- COVANE, Luís António, ***As relações económicas entre Moçambique e a África do Sul, 1850-1964: acordos e regulamentos principais***, Núcleo Editorial da Universidade Eduardo Mondlane. Maputo, 1989.
- CORREIA, Eduardo, ***Direito Criminal***, Vol. I S/Ed. Reimpressão, Almedina, Coimbra, 2001.
- COSTA, José de Faria, ***Noções Fundamentais de Direito Penal***, 3ª Ed. Coimbra Editora, Coimbra, 2012.
- CRUZ, Sebastião, ***Direito Romano***, 4ª Ed, Coimbra, 1986.
- CUNHA, Rogério Sanches, ***Manual de Direito Penal,*** V.1, 3ª Ed, Editora Jus Podvm, Salvador, 2015.
- CUNHA, Jorge, ***Dicionário da Língua Portuguesa e seu elucidário***, 12ª edição, Portugal, 2009.
- DAVID, René, ***Os Grandes Sistemas de Direito Contemporâneo***, 2.ª Ed., Editora Meridiano, Lda., Lisboa, 1978.
- _____, Os grandes sistemas do direito contemporâneo, 4ª Ed. Martins Fontes, São Paulo, 2002.
- DIAS, Jorge de Figueiredo, Direito penal Português, 3° Ed., Coimbra, Lisboa, 2001.
- _____, ***Direito penal: parte geral***, 2ª edição, Coimbra Editora, 2007.
- _____, Direito Penal, Tomo II, 2ª Ed. Coimbra Editora, Coimbra, 2012
- DIAS, Donaldo de Souza; SILVA, Mónica Ferreira da, Como escrever uma monografia: manual de elaboração com exemplares e exercícios, 1. ed. São Paulo: Atlas, 2010.
- DOTTI, René Ariel, Curso de direito penal: parte geral, 3ª. ed., rev., atual. e ampl, Editora Forense, Rio de Janeiro 2010.
- ESTEFAM, André, Direito Penal, 7ª Ed., Editora Saraiva, São Paulo, 2018.
- FRAGOSO, Heleno Cláudio, Lições de Direito Penal: parte geral, Rio de Janeiro, Forense, 2006.
- FERREIRA, Manuel Cavaleiro De Direito Penal Português, Parte Geral I, 2ª Edição, Editorial Verbo, Lisboa/São Paulo, 1982
- FERNANDES, Valter, Criminologia Integrada. 2ª Ed. Editora dos Tribunais, São Paulo, 2002, p. 378
- FIORILLO, Celso António Pacheco. Crimes no meio ambiente digital. 1 Ed. São Paulo: Saraiva, 2013.

- GIL, António edição, editora Atlas, São Paulo-Brasil, 2008. Carlos, *Métodos e técnicas de pesquisa social*, 6ª
- GOUVEIA, Jorge Bacelar, Direito constitucional de Moçambique, ASPRINT Editora, 2015.
- GREGO, Rogério, Curso de Direito Penal Parte Especial, Vol. II, 6ª Ed, Revista, Niteroi- Editora Impetus Ltda, 2009.
- HEDGES, David. História de Moçambique: Moçambique no auge do colonialismo, UEM, Maputo, 2004.
- HUNGRIA, Nelson, FRAGOSO, Heleno Cláudio, Comentários ao Código Penal, 4ª Edição, Lisboa.
- JESUS, Damásio, Direito Penal: Parte Geral, 36ª Ed., Editora Saraiva, São Paulo, 2015.
- JORGE, Wiliam Wanderley. Curso de Direito Penal: Parte Geral, Volume 1, Editora Forense, Rio de Janeiro. 1986.
- JOLO, Ana Flavia, Evolução Histórica do Direito Penal, São Paulo.
- KISSINGER, Henry, ***Ordem mundial***. Tradução Cláudio Figueiredo. 1. ed. Rio de Janeiro: Objectiva, 2015.
- MACIE, Albano, **Direito Penal I,** Topográfica Editora, Maputo, 2018.
- MAUS, Victor. **A Aplicabilidade da Lei das Contravenções Penais no Ordenamento Jurídico Contemporâneo**, Santa Cruz do Sul, 2017.
- MACAGNO, Lorenzo. **Outros muçulmanos: Islão e narrativas coloniais**, Imprensa de Ciências Sociais, Lisboa, 2006.
- MANDARINO, Rafael, ***Segurança e defesa do espaço cibernético brasileiro***, Recife: CUBZAC, 2010.
- MARCOS, Rui Manuel de Figueiredo, A história do Direito e o seu ensino na Escola de Coimbra.
- MARCONI, Mariana de Andrade De; LAKATOS, Eva Maria, Técnicas de Pesquisa: panejamento e execução de pesquisas, amostragens e técnicas de pesquisas, elaboração e interpretação de dados, 2ª edição, Editora Atlas, São Paulo: 1998.
- _____, Fundamentos de Metodologia Científica, 5ª Edição, Editora Atlas, São Paulo-Brasil, 2003.

- MARQUES, José Frederico. "Elementos de Direito Processual Penal". Campinas: Bookseller, 1997. Vols. I e II.
- MATUSSE, R.,. ***História da Informática em Moçambique***, Mozambique Acácia Advisory Committee Secretariat. Universidade Eduardo Mondlane, Maputo, 2003.
- MENDES, João de Castro, Direito Comparado, S/Ed. Associação Académica da Faculdade de Direito de Lisboa, Lisboa, 1982.
- MEHMERI, Adilson. Noções Básicas de Direito Penal, São Paulo, Saraiva, 2000.
- MIRABETE, Júlio Fabbrini; FABBRINI, Renato, Manual de Direito Penal-Parte Especial, Tomo II, 28ª Ed, Atlas Editora, São-Paulo, 2011.
- MIRANDA, Jorge; Manual de Direito Constitucional, Tomo IV, 4.ª Edição, Coimbra Editora, 2008.
- MOSSIM, Heráclito Antônio, Compêndio de Processo Penal, Manole, São Paulo, 2010.
- MUBARAK, Rizuane, Direito Penal e Criminalística: Da teoria universal as realidade nacional, S/Ed, Escolar Editora, 2016.

- MUCHANG, José, ***Internet em Moçambique,*** Centro de Informática Universidade Eduardo Mondlane (CIUEM) – Maputo, Moçambique, 2006.
- NETO, Filomeno, A política de segurança cibernética no actual espaço entre as nações, 2ª Edição, Amanhecer, Lisboa, 2003.
- NEWITT, Malyn. História de Moçambique, Publicações Europa América, Lisboa, 1997.
- NORONHA, E. Magalhães, Direito Penal: Introdução e Parte Geral, 36ª edição, Saraiva, São Paulo 2001.
- OLIVEIRA Martins, J. P. O Brasil e as colónias portuguesas. 5 ed. Lisboa: Parceria António Maria Pereira Lived, 1920.
- PAUL, Leandro, Noções Sobre História do Direito Clássico e Moçambicano, S/Ed. Edições FDS, Maputo.
- PALMA, Maria Fernanda, Direito Constitucional Penal, 1ª edição, Almedina, 2011.
- PINHEIRO, E. P. Crimes virtuais: uma análise da criminalidade informática e da resposta estatal.
- PRODANOV, Cleber Cristiano, e Ernani Cesar de Freitas. **Metodologia do Trabalho Científico - Métodos e Técnicas da Pesquisa e do Trabalho Académico,** 2ª edição. Rio Grande do Sul: ASPEUR, 2013.
- QUEIROZ, Paulo, ***Direito penal***, 4ª edição, Lumen Juris Editora, 2008.
- RAMOS, Santa Taciana Carrillo; NARANJO, Ernan Santiensteban, **Metodologia da Investigação Científica**, Escolar Editora, Lisboa, 2014.
- ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. 1. Ed. São Paulo: Memória Jurídica, 2004.
- SANTOS, Maria Emília Madeira, **A África e a instalação do sistema colonial (c. 1885-1930): III Reunião Internacional de História de África**, Centro de Estudos de História e Cartografia Antiga, Lisboa, 2000.
- SERRA, Carlos, História de Moçambique, Livraria Universitária, Maputo, 2000.
- SERRAO, Joaquim Veretissimo, História de Portugal, Vol I, 2ª edição, Editorial Verbo, Lisboa, 1990.
- SILVA, Nuno J. ESPINOSA Gomes da, História do, Direito Português – Fontes de Direito, 3ª Ed. Fundação Calouste Gulbekian, Lisboa, 2000.
- SILVA, Germano Marques Da, Direito Penal Português, 2ª Edição, Editora Verbo, São Paulo, 2001.
- SILVA, Fernando, Direito, Penal Especial: Crimes contra as pessoas, 2ª Ed. (revista e actualizada), Quid Juris sociedade editora, Lisboa, 2008.
- SILVA, Germano Marques, Direito Pena Português III, Vol. I, 2° Ed., Coimbra editora, Lisboa, 2008.
- SCHWARCZ, Lilia K. Moritz, Usos e abusos da mestiçagem e da raça no Brasil: uma história das teorias em finais do século XIX, Afro-Ásia, 1996.
- SOUTO, Amélia Neves de, Caetano e o ocaso do Império: Administração e Guerra Colonial em Moçambique durante o Marcelismo (1968 – 1974), Edições Afrontamento, Porto, 2007.

- SOUSA. Elísio de, Código Penal Moçambicano Anotado e Comentado, 2a Ed, Escolar Editora.
- TORRES, Adelino, **O Império Português entre o Real e o Imaginário**, S/Ed., Esher, Lisboa, 1991.
- THOMAZ, Fernanda. **Codificação dos costumes: Gonçalves Cota e os códigos jurídicos para os africanos de Moçambique**, 2012.
- TAVORA, Nestor; ALENCAR, Rosmar Rodrigues, Curso de Direito Processual Penal, Jus Podivm, Salvador, 2012.
- TRUJILLO, Ferrari A, ***Metodologia da ciência***, 3ª edição, editora Kennedy, Rio de Janeiro, 1974.
- VAZ, Ma ria João. **Crime e sociedade: Portugal na segunda metade do século XIX**. Oeiras: Celta Editora, 1998.
- WIEACKER, Franz, **História do Direito Privado Moderno**, 2.ª Ed., Fundação Calouste Gulbenkian, Lisboa, 1980.
- ZEFFARONI, Eugenio Raul; PIERAGELI, Jose henrique, **Manual de direito penal parte especial,** 2a Ed, São Paulo 1999.

III. Dissertações /Teses.

- MARCELINO, H, Dimensão de Defesa e Segurança Cibernética, Caso de Moçambique". (Dissertação de mestrado), Instituto Superior de Estudos de Defesa "Armando Emílio Guebuza" – Maputo, Moçambique. 2014.
- MENDES, Paulo de Sousa, As proibições de prova no processo penal. Apud RIBEIRO, Maria da Conceição Fernandes. Cibercrime e a prova digital. Dissertaçâo de Mestrado em Ciências Jurídico-Forenses. Instituto Superior Bissaya Barreto, Coimbra, 2015. p.41. disponível no Repositorio Comum: https://comum.rcaap.pt/bitstream/10400.26/28946/1/Cibercrime%20e%20Prova%20Digital.pdf, acessado no dia 29 de dezembro de 2023.
- NETO, João Araujo Monteiro. Aspectos Constitucionais e Legais do Crime Electrónico. Dissertaçáo de Mestrado em Direito Constitucional. Fundaçáo Edon Queiroz, Universidade de Fortaleza – Unifor. Centro de Ciências Jurídicas. Programa de Pós Graduaçáo em Direito Constitucional. Fortaleza – Ceará, 2008. Disponível em https://egov.ufsc.br/portal/sites/default/files/cp055676.pdf, acessado em 28 de Dezembro de 2023.
- PADILHA, Palma, Crimes Digitais e sua Tipicidade no Direito Penal, Monografia de Graduação, Faculdade Baiana de Direito, Salvador, Barasil, 2012.
- PEREIRA, Rui Mateus, Conhecer para Dominar: o Desenvolvimento do Conhecimento Antropológico na Política Colonial Portuguesa em Moçambique, 1926-1959. Tese de Doutorado. Lisboa: Universidade Nova de Lisboa, 2005.

- RIBEIRO, Maria da Conceição Fernandes. Cibercrime e a prova digital. Dissertaçâo de Mestrado em Ciências Jurídico-Forenses. Instituto Superior Bissaya Barreto, Coimbra, 2015. P.14. disponível no Repositorio Comum: https://comum.rcaap.pt/bitstream/10400.26/28946/1/Cibercrime%20e%20Prova%20Digital.pdf, acessado no dia 29 de dezembro de 2023.

- SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos, CYBERWAR: O fenómeno, as tecnologias e os actores, p. 5. RIBEIRO, Maria da Conceição Fernandes. **Cibercrime e a prova digital.** Dissertaçâo de Mestrado em Ciências Jurídico-Forenses. Instituto Superior Bissaya Barreto, Coimbra, 2015. p.16. disponível no Repositorio Comum: https://comum.rcaap.pt/bitstream/10400.26/28946/1/Cibercrime%20e%20Prova%20Digital.pdf, acessado no dia 29 de dezembro de 2023.

- SALES, Marcos Levy Gondim. **A comprovação da materialidade e da autoria nos crimes virtuais.** Monografia apresentada na Faculdade de Direito da Universidade Federal do Ceará, Fortaleza, 2013.

- SANTOS, Letícia Dutra de Oliveira, **Políticas Públicas de Educação Digital: Prevenção e Combate aos Crimes Cibernéticos,** Monografia apresentada na UniEvangélica, para obtenção de grau de Bacharel em Direito, Anápolis, 2020.

- THOMAZ, Fernanda do Nascimento, ***Casaco que se despe pelas costas: a formação da justiça colonial e a (re)ação dos africanos no norte de Moçambique, 1894-c.1940.*** Tese de Doutorado. Niterói: Universidade Federal Fluminense. 2012.

- VIDIGAL, Inês Maria Andrade, **As Políticas de Combate a Cibercrime na Europa**, Dissertação de Mestrado em Políticas Europeias, Instituto de Geografia e Ordenamento Territorial, Universidade de Lisboa, 2012.

iv. Artigos, Revistas, Períodicos e outras Publicações electrónicas.

- ALMEIDA, Jéssica de Jesus ; et. al. Crimes Cibernéticos, In Caderno de Graduaçáo, Ciências Humanas e Sociais Unit | Aracaju | v. 2 | n.3 | p. 215-236 | Março 2015 | periodicos.set.edu.br.
- BARBOSA, Caroline Ap. Sales. Teoria Geral da Prova no Direito Processual penal Brasileiro. disponível no https://www.jusbrasil.com.br/artigos/teoria-geral-da-prova-no-direito-processual-penal-brasileiro/337514638, acessado no dia 30 de Dezembro de 2023.
- CARNEIRO, Márcio Rodrigo de Freitas. Perícia de Informática nos Crimes Cibernéticos, pp. 36-37 (33-53). In EMAG- Escola de Magistrados da Justiça Federal da 3ª Região. Caderno de estudos (1- 354) Investigação e prova nos crimes cibernéticos. TRF3, São Paulo 2017.
- CAGLIARI, José Francisco. Prova em Processo Penal – SP, disponível em https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_publicacao_divulgacao/doc_gra_dout_crim/crime%2038.pdf, acessado no 3 de Janeiro de 2024.
- CEPIK, Marco Aurélio Chaves; et al. Revista Carta Internacional. Associação Brasileira de Relações Internacionais, Belo Horizonte, V.16, n.3, e1130, 2021, DOI: 10.21530/ci.v16n3.2021.1130,ISSN2526-9038.
- COELHO, António Manuel Mendes. Meios de prova e meios de obtenção de prova, Fórum de Investigação Criminal, organizado pelo Comando de Polícia de Aveiro da PSP a 26 de Outubro de 2006, no Centro Multimeios de Espinho. In Revista

VerboJurídico, disponível em .www.verbojuridico.pt/.eu/.net/.org/.com. Acesso a 14 de Dezembro de 2023.

- COSTA, Marcelo António Sampaio Lemos. Computação Forense. p. 26, Disponível no www.estantevirtual.com.br/b/marcelo-sampaio-lemos-costa/computação-forense/593469987. Acessado no dia 20 de Julho de 2017.
- Conselho da Europa. Convenção sobre o Cibercrime. Budapeste, 23 de de Novembro de 2001, disponível em: https://rm.coe.int/16802fa428. Acessado nos dias 17 de Dezembro de 2023.
- DANIEL, Rogério de Carvalho Veiga; et al. Função Simbólica do Direito Penal e o Princípio da Intervenção Minima. Programa de Apoio à Iniciação Científica – PAIC. 2013-2014. In cadernopaic.fae.edu.
- FREITAS, Lucas. Segurança Jurídica como um bem jurídico-penal. Disponível no https://www.jusbrasil.com.br/artigos/a-seguranca-informatica-como-um-bem-juridico-penal/1661329789. Acessado no dia 26 de Dezembro de 2023.
- Instituto Brasileiro de Ciências Criminais (IBCCRIM), disponível no https://ibccrim.org.br/notícias/exibir/2845/. Acessado nos dias 25 de Dezembro de 2023.
- MOORE, Susan. Gartner prevê que gastos mundiais com segurança e gerenciamento de riscos excederão US $150 bilhões em 2021 (tradução livre). Gartner Group, 17/05/2021. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwidesecurity-a.... Acesso em 03/09/2022.
- MIRANDA, Bruno Silvão, Os bens jurídicos Tutelados pelos Crimes Informáticos na Legislação Brasileira, Centro Universitário FG – Artigo Científico, Guanambi, BA, Brasil, 2021.
- ORRIGO, Gabriel Marcos Archanjo; et al. Crimes Cinbernéticos: uma abordagem jurídica sobre os crimes realizados no âmbito virtual .Jus.com.br, 2015. Disponivel em: https//jus.com. br/artigos/4358/crimes-cibernéticos-abordagem jurídica-sobre-os-crimes-realizados-no-ambito-virtual. Acessado no dia 13 de Janero de 2024.
- PACHECO, Gisele Freitas. Crimes virtuais e a legislação penal brasileira,. Revista Electrónica de Ciências Jurídicas. 2018.
- PINTO, Samara Silva. Dos Crimes Virtuais, da Obtenção das Provas e as Tendências Jurídicas decorrentes da Evolução Tecnológica. Instituto Brasileiro de Direito Público - IDP, Brasília-DF. Disponível no https://www.idp.edu.br Acessado no dia 3 de Janeiro de 2024.
- RAMOS, Alícia Castro; et al. A Fragilidade do Ordenamento Jurídico Quanto ao Cibercrime: criminosos por trás de uma tela, Vítimas expostas em suas vidas. Revista da Humanidade, Ciências e Educação – REASE, São Paulo (SP), p.8.n.11. nov. 2022. ISSN-2675 – 3375
- RONCADA, Rodiner. A prova da materialidade delitiva nos crimes cibernéticos p.p. 175 (1-354) in EMAG- Escola de Magistrados da Justiça Federal da 3ª Região. Caderno de estudos: Investigação e prova nos crimes cibernéticos. TRF3, São Paulo 2017.
- SILVA, R. G. Crimes da Informática. Editora: CopyMarket.com, 2000.
- SOBRINHO, Jéssica Rafaela Nunes; et.al. OS SUJEITOS ATIVOS NO CIBERCRIME E A RESPONSABILIDADE PENAL DO OFENSOR. REVISTA CIENTÍFICA

MULTIDISCIPLINAR DO CEAP (REV. MULT. CEAP). V. 4, N. 2, JUL./DEZ. 2022, p. 2.

- VIANA, Lucas Freitas, Segurança Jurídica como um bem jurídico-penal. Disponível no https://www.jusbrasil.com.br/artigos/a-seguranca-informatica-como-um-bem-juridico-penal/1661329789. Acessado no dia 26 de Dezembro de 2023.

IV. Relatorio e outros documentos da natureza idêntica

- MOÇAMBIQUE, República de. Procuradoria-Geral da República. ***Informação Anual de 2019 do Procurador-Geral da República à Assembleia da República***, Maputo, 2020.
- _____. Procuradoria-Geral da República. ***Informação Anual de 2020 do Procurador-Geral da República à Assembleia da República***, Maputo, 2021.
- _____. Procuradoria-Geral da República. ***Informação Anual de 2021 do Procurador-Geral da República à Assembleia da República***, Maputo, 2022.
- _____. Procuradoria-Geral da República. ***Informação Anual de 2022 do Procurador-Geral da República à Assembleia da República***, Maputo, 2023.
- IESE, ***Desafios para Moçambique 2017***, Disponível em: https://www.iese.ac.mz/wp-content/uploads/2018/05/Desafios2017.pdf, acesso: 25/06/2023.