

Crimes informáticos no ordenamento jurídico moçambicano

Computer crimes in the mozambican legal system

Delitos informáticos en el sistema jurídico mozambiqueño

Raúl de miguel benjamim jofrisse nhamitambo¹

RESUMO

A presente pesquisa tem por fim abordar sobre os crimes informáticos ou cibernéticos em Moçambique. Tendo em vista as mudanças paradigmáticas promovidas pela globalização e dos avanços da tecnologia, com o uso da internet tornou-se um ambiente facilitador para a prática da violência no seio virtual. A sociedade da informação viabilizou diversas mudanças técnicas e sociais, criando uma comunicação global e instantânea, facilitando a comunicação em diferentes áreas. Fez-se uma análise sobre as TIC's e o Direito, apresentando seus principais aspectos, a análise terminológica e conceito crime informático ou cibernético, bem como a classificação dos crimes informáticos ou cibernéticos e os sujeitos ativos e passivos. A prática deste tipo de crime aumentou com as habilidades que a internet brinda aos seus utilizadores (anonimato, simplicidade, agilidade de comunicação, facilidade de partilha de dados transfronteiriços e potencial para conquistar o público-alvo). O ciberespaço tornou-se assim um instrumento para utilizadores "de bem", como para sujeitos que se aproveitam das benesses da rede universal de informação tendo em vista a execução dos mais diversos tipos de crime. Nesta lógica, há a necessidade da justiça entrar em acção e dar soluções para os problemas vigentes procurando aplicar uma lei que se revele atual.

¹ Doutor em Ciências Jurídicas, pela Universidade Para La Cooperación Internacional México (UCIMEXICO) – México (2020); Mestre em Assessoria Jurídica de Empresas, pela Universidad a Distancia de Madrid (UDIMA) - Madrid (2016); Licenciado Ciências Jurídicas e Investigação Criminal, pelo extinto Instituto Superior de Ciências e Tecnologia Alberto Chipande (ISCTAC) – Beira (2011); Advogado e Membro da Ordem dos Advogados de Moçambique (desde Abril de 2018); Professor Auxiliar de Direito das Tecnologias de Informação e Comunicações (Direito das TIC's) – na Universidade Joaquim Chissano (UJC) – Maputo (desde Fevereiro de 2020), no Curso de Licenciatura em Engenharia de Tecnologias e Sistemas de Informação; Professor Auxiliar de Direito Administrativo e Noções de Direito Administrativo – na Universidade Pedagógica de Maputo (UP - Maputo), nos Cursos de Licenciaturas em Gestão de Recursos Humanos e Gestão Pública e Educacional; Técnico Superior de Assistência Jurídica – Gabinete Jurídico (UP - Maputo); Docente Universitário de Introdução ao Direito, Direito Administrativo I e II e, Direito de Trabalho, nos Cursos de Licenciatura em Direito, Contabilidade e Auditoria e, Administração Pública e Autárquica – no Instituto Superior Maria Mãe de África (ISMMA); Professor Auxiliar no Instituto Superior de Contabilidade e Auditoria de Moçambique (ISCAM), leccionando a disciplina Complementos de Fiscalidade no Curso de Mestrado em Auditoria; Autor, Revisor, Avaliador Externo e Parecista na Revista Científica Multidisciplinar O Saber (desde II Semestre de 2024); Autor, Avaliador e Parecista na Revista Multidisciplinar RECIMA21 (desde I Semestre de 2025) e na Revista Internacional Consinter de Direito (Conselho Internacional de Estudos Contemporâneos em Pós-Graduação – CONSINTER), desde II Semestre de 2025 e Organizador da Editora Científica Digital (Desde I Semestre de 2025). Matola – Maputo.

ORCID: 0009-0006-4118-1970. nhamitambo@gmail.com. (+258) 872058783/847417800.

Palavras-chave: Crimes informáticos ou cibernéticos; ciberespaço; problemas vigentes.

ABSTRACT

The purpose of this research is to address computer or cyber crimes in Mozambique. In view of the paradigmatic changes promoted by globalization and advances in technology, the use of the internet has become an environment that facilitates the practice of violence in the virtual world. The information society has enabled several technical and social changes, creating global and instant communication, facilitating communication in different areas. An analysis was made on ICTs and Law, presenting their main aspects, the terminological analysis and concept of computer or cyber crime, as well as the classification of computer or cyber crimes and active and passive subjects. The practice of this type of crime has increased with the capabilities that the Internet offers its users (anonymity, simplicity, agility of communication, ease of sharing cross-border data and potential to reach the target audience). Cyberspace has thus become an instrument for "good" users, as well as for individuals who take advantage of the benefits of the universal information network with a view to carrying out the most diverse types of crime. In this logic, there is a need for justice to take action and provide solutions to current problems, seeking to apply a law that is up to date.

Keywords: Computer or cybercrimes; cyberspace; current problems.

RESUMEN

El propósito de esta investigación es abordar los delitos informáticos o cibernéticos en Mozambique. Ante los cambios paradigmáticos promovidos por la globalización y los avances tecnológicos, el uso de internet se ha convertido en un entorno que facilita la práctica de la violencia en el mundo virtual. La sociedad de la información ha permitido diversos cambios técnicos y sociales, creando una comunicación global e instantánea, facilitando la comunicación en diferentes ámbitos. Se realizó un análisis sobre las TIC y el Derecho, presentando sus principales aspectos, el análisis terminológico y concepto de delito informático o cibernético, así como la clasificación de los delitos informáticos o cibernéticos y los sujetos activos y pasivos. La práctica de este tipo de delitos ha aumentado con las capacidades que ofrece Internet a sus usuarios (anonimato, sencillez, agilidad de comunicación, facilidad para compartir datos transfronterizos y potencial para llegar al público objetivo). El ciberespacio se ha convertido así en un instrumento tanto para los "buenos" usuarios como para los particulares que aprovechan los beneficios de la red universal de información para cometer los más diversos tipos de delitos. En esta lógica, existe la necesidad de que la justicia actúe y aporte soluciones a los problemas actuales, buscando aplicar un derecho actualizado.

Palabras clave: Delitos informáticos o cibernéticos; ciberespacio; problemas actuales.

INTRODUÇÃO

No presente trabalho abordaremos sobre os crimes informáticos ou cibernéticos em Moçambique.

Partindo da premissa de que o Direito acompanha o facto social e que o anonimato influencia no cometimento de actos ilícitos, surge a intervenção do Direito, visando, ao mínimo, reduzir a incidência destas práticas. Pois, concomitantemente, ascende o problema relacionado à ausência de punição para quem cometeu a conduta considerada típica, ilícita e culpável, gerando por consequência uma instabilidade jurídica. Por isso, é necessário a análise da dilação probatória, cuja identificação do agente activo é complexa devido ao anonimato concedido pela rede.

Diante da relevância social e complexidade do tema, não há possibilidade de esgotar o assunto, no entanto, o objectivo é incitar a discussão e analisar referências que constatem, ou não, melhorias e esclarecimentos sobre o assunto. Para tanto, quanto à metodologia, foi utilizado o método dedutivo como forma de abordagem da pesquisa e o procedimento empregado como técnica foi a revisão de literatura – doutrina, jurisprudência, artigos científicos e legislação – de modo a se ter uma percepção real e conclusão geral sobre o tema.

O crescente acesso aos serviços das TIC, incluindo a Internet, é também acompanhado de crescentes vulnerabilidades a que o cidadão está sujeito e com isto também o crescimento dos crimes cibernéticos. O Governo de Moçambique está também plenamente consciente da ameaça e dos efeitos negativos do crime informático ou cibernético sobre a sua Nação e por isso tem sido feito esforços para garantir que hajam instrumentos que possam proteger o cidadão e penalizar os que cometem estes crimes com recurso as TIC's. Estes esforços incluem:

- ✧ O Código Penal, aprovado pela Lei n.º 24/2019, publicada no dia 24 em Dezembro de 2019, que cobre os Crimes informáticos, a saber: Pornografia de menor (artigo 211), Utilização de menores em pornografia (artigo 212), Distribuição ou posse de pornografia de menores (artigo 213), Devassa da vida privada (artigo 252), Violação de correspondência ou de comunicações (artigo 253), Base de dados automatizada (artigo 254), Acesso ilegítimo (artigo 256), Gravações ilícitas (artigo 257), Furto de fluidos (artigo 276), Burla informática e nas comunicações (artigo 289), Fraudes relativas aos instrumentos e canais de pagamento electrónico (artigo 294), Abuso de meios de pagamento electrónicos (artigo 295), Falsidade informática (artigo 336), Interferência em dados (artigo 337), Interferência em sistemas (artigo 338), Uso abusivo de dispositivos (artigo

339), Instigação pública a um crime (artigo 345), Apologia pública ao crime (artigo 346), Publicidade da decisão condenatória (artigo 448);

- ✧ A Lei 3/2017, a Lei das Transacções Electrónicas, promulgada em Janeiro de 2017, que visa proteger os consumidores e regular o uso de sistemas electrónicos no governo, sector privado e sociedade civil;
- ✧ Regulamento de controlo de Tráfego de Telecomunicações, Decreto n.º 75/214, de 12 de Dezembro;
- ✧ Regulamento de Registo de Cartões SIM, Decreto 18/2015;
- ✧ Lei de Telecomunicações, Lei n.º 4/2016, de 3 de Junho.

Segundo Nhamitambo (2025), Crime ou delito é o facto voluntário declarado punível pela lei penal, nos termos do art. 1 do CP.

Segundo Marques e Martins (2000, p.493) citado por Nhamitambo (2025), "crime informático é todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é o alvo desse acto."

EMBASSAMENTO TEÓRICO

Internet e o Direito: Contextualização e Aspectos Importantes

O acesso à internet, como Direito Fundamental, decorre dos valores da dignidade humana e da cidadania, assegurados constitucionalmente. “Na actualidade, o papel da Internet estende-se para além de um simples meio de comunicação, porquanto passou a fazer parte da própria vida em sociedade como facilitador e mantedor de relações humanas.” (PIMENTEL; CARDOSO, 2015, p. 48).

Assim, a ordem jurídica e a normativa constitucional garantem o direito fundamental à informação e liberdade de expressão, hiper dimensionados pelo uso da internet, novas tecnologias e desenvolvimento da informática.

No contexto da globalização, a internet tornou-se o principal meio de comunicação e informação. Está presente, de cordo com Sorg et.al (2019, p. 9), em quase todas as actividades da vida

privada. A quantidade e diversidade de informações que se pode acessar e compartilhar, a facilidade de comunicação, possibilita compartilhar mensagens e postar opiniões, produzindo uma nova forma de organizar a informação e comunicação.

Nesta nova perspectiva, computadores, smartphones, tablets, GPS, câmeras digitais, e outros dispositivos eletrônicos são utilizados em crimes e ações ilegais. A disseminação das tecnologias e dos recursos eletrônicos “não estão sendo apenas empregados pelas empresas, mas também sendo mais utilizados na prática de diversos crimes” (CAIADO, CAIADO, 2018, p. 10). No mesmo sentido: Praticamente todas as pessoas físicas e jurídicas, de uma forma ou de outra, interagem no ciberespaço, pois a Internet se tornou indispensável em nossas vidas, possibilitando inúmeras facilidades que se estendem de simples contatos sociais até operações bancárias. Porém, justamente por se expandir por praticamente todas as residências, empresas e órgãos públicos, seu livre acesso resulta em problemas ligados à segurança desse sistema, sobretudo quando se trata de operações que envolvam informações que não sejam públicas, tais como dados sigilosos, informações pessoais e bancárias (GIMENES, 2013).

Devido à insegurança jurídica que é causada no âmbito digital e o receio social em todo o mundo, surge a necessidade de atualizar a legislação e métodos mais rigorosos de fiscalização, visando otimização dos meios de busca do agente. A internet criou um novo paradigma, não apenas para a melhoria da qualidade de vida, mas atualmente representa um meio facilitador das práticas criminosas.

Caiado, Caiado (2018, p.10), explica que, com esse novo paradigma, o desenvolvimento da tecnologia melhora o padrão de vida, contudo, ao mesmo tempo, aumenta exponencial e proporcionalmente, a consecução de diferentes práticas criminosas, “entre elas a criação de um dos crimes mais infame da sociedade moderna: a pornografia infanto-juvenil, e facilitando também o acesso a ele e a distribuição de material a este relacionado.”

Os crimes praticados nos meios digitais tomaram enormes proporções com o advento da sociedade digital e representam um enorme desafio a devida identificação e persecução da pena. Assim sendo, é preciso destacar que: O acesso às novas tecnologias em um mundo cada vez mais conectado têm garantido diversos avanços nas relações sociais e econômicas. Entretanto, toda essa tecnologia também pode ser utilizada para a prática de crimes. Os crimes cibernéticos são uma realidade, várias espécies de crimes se originaram e outros já conhecidos ganharam uma nova roupagem diante do avanço tecnológico (ARAÚJO, 2018, p. 90).

Assim, surge com o estabelecimento da internet novas situações sociais, políticas, econômicas e, conseqüentemente, novas questões jurídicas. Nas palavras de Reale (2010, p. 2), o Direito é “um facto ou fenómeno social; não existe senão na sociedade e não pode ser concebido fora dela. Uma das características da realidade jurídica é, como se vê, a sua socialidade, a sua qualidade de ser social.”

Por conseguinte, o Direito precisa ser adaptado às novas realidades. “Tem se, então, no Direito Penal a ultima ratio para inibição ou punição da realização de um determinado facto ou acto humano não tolerado pela sociedade em certa época.” (SANTOS, 2018, p. 159). Desta feita, com os benefícios da internet, novos riscos surgiram. Com a inclusão digital: [...] disseminaram-se novas formas de assédio pessoal e abuso de crianças e adolescentes, e a privacidade dos indivíduos fica cada vez mais em xeque. A Internet tornou-se palco de cibercrimes, de práticas de censura de conteúdo em massa e de vigilância e espionagem ilegais realizadas por Estados nacionais. Suas ferramentas passaram a ser usadas por grupos que promovem violações de direitos humanos e exploram a fragilidade de serviços e infraestruturas públicos, inclusive ataques cibernéticos a sistemas militares (SORJ et al; 2018, p. 9).

No mesmo compasso da evolução tecnológica, abre-se espaço para os crimes virtuais, os quais vêm acarretando diversos prejuízos à sociedade. Como salienta Maues, Duarte e Cardoso (2018, p. 170), a imaterialidade da internet propicia a ausência de limites espaciais e temporais; seu amplo e genérico acesso “alavanca riscos oriundos da vulnerabilidade do meio digital, sendo assim, quanto maior a utilização da internet nas interações humanas, mais se potencializa a tendência de surgimento de problemas legais, inclusive, o nascimento de novos tipos de crimes.”

Como explica Spinieli (2018, p. 206), foi a partir do grande levante de invasões aos computadores mundiais que trouxe para o Estado a responsabilidade única de vigiar e, ao mesmo tempo, garantir a protecção dos bens jurídicos relevantes para o meio social que se encontrava em risco, além de punir aquele que transgredisse tais valores.

A evolução levou-nos à era cibernética, com vantagens e desvantagens “que essa evolução tecnológica pode proporcionar. Tem havido, em todo o mundo, a criação de novos crimes cibernéticos, decorrentes da necessidade de ordenar, disciplinar e limitar o uso indevido da moderna e avançada tecnologia cibernética.” (BITENCOURT, 2018, p. 554).

A internet, associada à disseminação das tecnologias da informação e comunicação, é um novo caminho para a prática de crimes já previstos na norma penal incriminadora, sendo necessário que a legislação seja adaptada aos crimes cometidos por meio virtual.

RESULTADOS E DISCUSSÃO

Crime Informático

Segundo Marques e Martins (2000, p.493), citado por Nhamitambo (2025), "crime informático é todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é o alvo desse acto."

Embora não exista uma definição específica de “Crime Informático”, vários doutrinários abordam sobre o assunto e se têm esforçado por elucidar um conceito claro e conciso sobre o crime da nova era.

Segundo Perez (2003), expressa em sentido amplo que o crime informático, é: “qualquer conduta criminógena ou criminosa que na sua realização faz uso da tecnologia eletrónica como método, meio ou fim e que, de forma”.

Em sentido estrito, Crime Informático é qualquer ato criminoso em que os computadores, as suas técnicas e funções desempenham um papel comométodo, meio ou fim.”

RODRÍGUEZ, define o Crime Informático como: “a execução de uma acção que, reunidas as características que delimitam o conceito de crime, se realiza através de um computador e/ou elemento telemático, ou que viole os direitos do proprietário de um elemento informático, seja hardware ou software.”

Características dos Crimes Informáticos

As pessoas que cometem tais crimes têm determinadas características que não apresentam o denominador comum dos criminosos. Ou seja, os sujeitos activos têm a capacidade de lidar

com sistemas informáticos e, em geral, por causa da sua situação de emprego se encontram em locais estratégicos onde é tratada informações sensíveis; ou são qualificados na utilização dos sistemas informatizados, ainda que, em muitos casos, não realizem actividades que facilitam a prática deste tipo de crime.

Segundo o TELLEZ, os crimes informáticos apresentam os seguintes principais características:

- a) São crimes que apresentam condutas criminosas de colarinho branco, desde que apenas um certo número de pessoas com determinados conhecimentos (em neste caso os técnicos) podem cometê-los.
- b) São acções ocupacionais, pois são frequentemente realizadas quando o assunto é trabalho.
- c) São acções de oportunidade porque aproveitam uma oportunidade criada ou altamente intensificadas no campo das funções e organizações do sistema tecnológico e económico.
- d) Provocam graves prejuízos económicos, pois produzem quase sempre "lucros" de mais de cinco dígitos para quem os obtém.
- e) Oferecem facilidades de tempo e espaço, pois podem ser praticadas em milésimos de segundo e sem a necessária presença física.
- f) Há muitos casos e poucas denúncias, por falta de regulamentação jurídica a nível internacional.
- g) São muito sofisticados e relativamente comuns no campo militar.
- h) Apresentam grandes dificuldades de verificação, devido à sua natureza técnico.
- i) A maioria deles é maliciosa ou intencional, embora também existam muitos de natureza negligente ou imprudente.
- j) Oferecem facilidades aos menores para a sua comissão.

k) Tendem a proliferar cada vez mais, pelo que exigem acções urgentes, regulamentação jurídica na esfera internacional.

Classificação dos crimes Informáticos ou Virtuais

Várias são as classificações doutrinárias sobre os crimes informáticos ou virtuais. Duas categorias são utilizadas: a dos crimes informáticos próprios ou puros e a dos crimes informáticos impróprios ou impuros.

Barreto e Brasil (2016, p.17) conceituam crime virtual próprio como aqueles em que o dispositivo informatizado e/ou seu conteúdo é o alvo dos criminosos - os sistemas informatizados, bancos de dados, arquivos ou terminais (computadores, smartphones, tablets) são atacados por criminosos, normalmente após a identificação de vulnerabilidades, seja por meio de programas maliciosos ou por engenharia social (golpista engana a vítima, fazendo com que forneça informações pessoais e/ou estratégicas).

Para Albuquerque (2006, p.168), os crimes virtuais impuros “diriam respeito aos crimes em que os recursos informáticos constituem o meio de execução, tendo como objecto bens jurídicos que já são protegidos por tipos penais existentes”. Na sociedade da informação, a incidência de ilícitos penais “têm por objecto material ou meio de execução o objecto tecnológico informático: hardware, software, redes, etc.

Crimes informáticos puros, segundo Amabélia Chuquela, são aqueles em que a utilização do sistema informático é o meio necessariamente utilizado para a prática delitiva.

Crimes Informáticos impuros, segundo Amabélia Chuquela, são aqueles em que a utilização do sistema informático trata-se apenas de um novo *modus operandi*. Ou seja, são aqueles em que a utilização do sistema informático é o meio necessariamente utilizado para a prática delitiva.

Nucci (2017, p. 131), explica que o sujeito activo (autor ou agente) é “a pessoa que pratica a conduta descrita pelo tipo penal”. Ou seja, é quem realiza a acção ou omissão típica, nos delitos dolosos ou culposos. Apenas pode ser sujeito activo a pessoa humana, e não animais ou coisas. O sujeito passivo do delito, conforme Nucci (2017, p. 134), é o titular do bem jurídico protegido pelo tipo penal incriminador, lesado ou ameaçado de lesão. Podem figurar como sujeitos passivos – vítimas, ofendidos, a pessoa física ou o indivíduo, mesmo incapaz, o conjunto de indivíduos, a pessoa jurídica, a coletividade, o Estado ou a comunidade internacional, de acordo com a natureza do delito.

Nos crimes virtuais, no polo activo, portanto, é muito comum associarem os hackers à figura dos criminosos da internet, porém, hacker é apenas uma expressão dada, dentre muitas outras, para caracterizar uma pessoa que possui muito conhecimento no meio informático e que invade sistemas, só que não necessariamente visa o ilícito.

De acordo com Assunção (2017, p. 33), o termo hacker, desde as décadas de 1970 e 1980, serve para designar “fuçadores”. Com o passar do tempo, foi utilizado pela mídia para nomear invasores de sistemas, até hoje esse termo é utilizado de forma peculiar: designa um garoto de doze anos que acciona o computador da escola para mudar sua nota ou um fraudador que engana pessoas, enviando-lhes e-mail para para capturar senhas de acesso.

Por isso, há várias outras designações para diferenciar os autores dos crimes praticados, como por exemplo, a figura dos crackers, que são aqueles que necessariamente utilizam do seu conhecimento para o mal, obtendo vantagens ilícitas, através de danificação de sistemas, usurpação de senhas, dados, documentos, entre outros. De forma genérica, é a “denominação para alguém que possui uma grande habilidade em computação. Cracker, black-hat ou script kiddie, neste ambiente, denomina aqueles hackers que têm como hobby atacar computadores. Portanto, a palavra hacker é gênero, e cracker, espécie.” (GIMENES, 2013).

Moisés Cassanti (2014, p. 2) traz uma distinção entre os conceitos de hacker e cracker. Embora ambos sejam termos que se referem a experts em computadores, a principal diferença está na forma como cada um utiliza esse conhecimento: Apesar do termo hacker sempre aparecer associado a roubo de dados e invasão de sistemas, no entendimento de especialistas em computação, os verdadeiros criminosos são designados como crackers. A palavra deriva do verbo em inglês “to crack”, que significa quebrar. Entre as acções, estão a prática de quebra de sistemas

de segurança, códigos de criptografia e senhas de acesso a redes, de forma ilegal e com a intenção de invadir e sabotar para fins criminosos. O termo hacker, por sua vez, serve para designar um programador com amplo conhecimento sobre sistemas, mas sem a intenção de causar danos. Inclusive, a habilidade para lidar com sistemas e programações, muitas vezes, é utilizada pela própria polícia em investigações ou até mesmo no desenvolvimento de softwares com o intuito de limar brechas de segurança, criar novas funcionalidades ou adaptar as antigas.

Desta forma, a “questão da segurança no ciberespaço não é de interesse apenas das pessoas físicas ou das empresas, sendo altamente relevante para órgãos públicos, para agentes políticos e para o próprio Estado.” (GIMENES, 2013). Qualquer pessoa pode ser sujeito passivo, até mesmo empresas e instituições, e, devido às técnicas dos cibercriminosos acabam tendo suas informações e bens violados.

O Bem Jurídico Protegido nos Crimes Informáticos

A questão relativa ao bem jurídico protegido suscita um dos problemas que mais dúvidas se levantam nos crimes de dano em geral, e nos crimes de dano informáticos em particular.

O bem jurídico protegido em geral é informação, mas é considerada de diferentes formas, quer como valor económico, como valor intrínseco da pessoa, pela sua fluidez e tráfego legal e, finalmente, pelos sistemas que o processam ou automatizam; o que são equivalentes aos bens jurídicos protegidos tradicionais, tais como:

- a) Os activos no caso do vasto leque de burlas informáticas e da manipulações de dados a que dá origem.
- b) A confidencialidade, a privacidade e a confidencialidade dos dados, no caso de ciberataques à esfera da privacidade em geral, especialmente no caso das bases de dados.
- c) A segurança ou fiabilidade do tráfego jurídico e/ou probatório, no caso de falsificações de dados ou documentos comprovativos através de cientistas da computação.

d) O direito de propriedade, neste caso sobre a informação ou sobre o elementos físicos e materiais de um sistema informático, que são afetados por danos e pelo chamado terrorismo informático.

Portanto, o bem jurídico protegido está sujeito à confidencialidade, integridade, disponibilidade de informação e sistemas de computador onde é armazenado ou transferido.

Numa outra perspectiva doutrinária, assume-se que a emergente Sociedade da informação torna absolutamente necessária a incorporação de valores intangíveis e a própria informação como bens jurídicos de protecção, tendo em conta as diferenças que existem, por exemplo, entre propriedade tangível e intangível.

Isto porque, na opinião de Palazzi, a informação não pode ser tratada da mesma forma, da mesma forma que a legislação vigente se aplica aos bens tangíveis², embora. Estes bens têm um valor intrínseco partilhado, que é a sua valorização económico, é por isso que a informação e outros bens intangíveis são objectos de propriedade, que é constitucionalmente protegida. Em suma, a protecção da informação como bem jurídico protegido deve ter sempre em conta o princípio da necessária protecção dos bens jurídicos que indicie que a penalização de a conduta desenvolve-se dentro da estrutura do princípio do “dano” ou da “nocividade”.

Assim, uma conduta só pode ser punida quando for completamente incompatível com os pressupostos de uma vida pacífica, livre e partilhada materialmente seguro.

O interesse social digno de a protecção criminal seria: Informação - armazenada, tratada e transmitida através sistemas informáticos - sem prejuízo de que dele derivem ou tragam consigo um leque extensos bens jurídicos protegidos e salvaguardados pela lei e legislação do cada país.

² Bens tangíveis são objetos físicos, ou seja, que possuem substância material e podem ser tocados. São bens que podem ser vistos, sentidos e percebidos pelos sentidos, ao contrário dos bens intangíveis, que são imateriais. Exemplos de bens tangíveis incluem imóveis, veículos, equipamentos, móveis e mercadorias.

Tipo Legal de Crimes Informáticos e Suas características

MORRAIS (2015), citado por Nhamitambo (2025), afirma que:

“As tecnologias de informação e comunicação para além de permitir o intercâmbio de dados e informações que concretizam desde relacionamentos interpessoais até acordos comerciais envolvendo movimentações financeiras vultosas, criaram novos tipos de delitos, que são os crimes cibernéticos. Porém, recorrendo na análise conceitual, trazemos aspectos comuns em relação ao conceito do crime cibernético. Nesse corolário, podemos ilidir que os crimes cibernéticos comportam-se como uma acção ou omissão típica, ilícita, culposa e punível nos termos da lei penal e caracterizados pela utilização do computador (instrumento típico do crime) e da internet para a prática de actos delituosos, como sejam”, nos termos da Lei nº 24/2019, de 24 de Dezembro (que aprova o Código Penal):

Pornografia de menor (artigo 211), é caracterizado por representação visualmente de um menor ou pessoa aparentando ser menor envolvido em comportamento sexualmente explícito por meio de suporte ou plataforma.

Utilização de menores em pornografia (artigo 212), é caracterizado pelo uso de menor de 18 anos em fotografia, filme ou gravação pornográficos, independentemente do seu suporte, ou o aliciar para esse fim; ou em espectáculo pornográfico ou o aliciar para esse fim. Cujas molduras penais variam de 1 a 5 anos de prisão maior. E, de 12 anos, cuja moldura penal varia de 2 a 8 anos de prisão maior.

Distribuição ou posse de pornografia de menores (artigo 213), é caracterizado pela distribuição, importação, exportação, divulgação, exibição ou cedência profissionalmente ou com finalidade de lucro, a qualquer título ou por qualquer meio, materiais de fotografia, filme ou gravação pornográfica de menores de dezoito anos; a mera partilha, exibição, cedência, importação, exportação ou distribuição do material, quando não tem os fins lucrativos ou profissional, independentemente do suporte ou

plataforma, adquirir, detiver ou conservar os materiais referidos anteriormente, ainda que para uso pessoal. Cujas tentativas são puníveis.

Devassa da vida privada (artigo 252), é caracterizado pela interceptação, gravação, registro, utilização, transmissão ou divulgação de conversa, comunicação telefónica, imagem, fotografia, vídeo, áudio, facturação detalhada, mensagens de correio electrónico, de rede social ou de outra plataforma de transmissão de dados; captação, por fotografar, filmar, manipular, registar ou divulgar imagem das pessoas ou de objectos ou espaços íntimos; observar ou escutar às ocultas pessoas que se encontrem em lugar privado; ou divulgar factos relativos à vida privada ou a doença grave de outra pessoa – este último, não é punível quando for praticado como meio adequado para realizar um interesse público legítimo e relevante. E, É punido com pena de prisão até 1 ano e multa correspondente, quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual.

Violação de correspondência ou de comunicações (artigo 253), é caracterizado pela intromissão no conteúdo de telecomunicação ou dele tomar conhecimento, sem consentimento, cuja pena de prisão vai até 1 ano e multa correspondente. e, pela divulgação do conteúdo de cartas, encomendas, escritos fechados, ou conteúdos de telecomunicações, pena varia de 6 meses a 1 ano de prisão e multa correspondente.

Base de dados automatizada (artigo 254), é caracterizado por criar, manter ou utilizar 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, sem o devido consentimento, ou fora dos casos estabelecidos na lei e punível com a pena de prisão até 2 anos e multa correspondente.

Acesso ilegítimo (artigo 256), é caracterizado por invadir um dispositivo alheio, fixo ou móvel, ligado ou não à rede de computadores, com o fim de obter informação não pública de correio ou comunicações electrónicas privadas, acesso a dados privados, segredos comerciais ou industriais, informações sigilosas ou o acesso remoto não autorizado do dispositivo, sem permissão legal ou sem para tanto estar autorizado pelo

proprietário, por outro titular do direito do sistema ou de parte dele e punível com prisão de 1 a 2 anos e multa até 1 ano. E, ilegítimamente, 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 anteriormente em relação aos factos e a moldura penal.

O procedimento criminal depende de queixa, po se tratar de um crime particular.

Gravações ilícitas (atigo 257), é caracterizado por gravar palavras proferidas por outra pessoa e não destinadas ao público, mesmo que lhe sejam dirigidas; utilizar ou permitir que se utilizem as gravações descritas anteriormente, mesmo que licitamente produzidas, contra vontade e fora dos casos permitidos por lei, cuja moldura penal seja de pena de prisão até 1 ano e multa correspondente.

Furto de fluidos (artigo 276), é caracterizado por subtrair, para consumo pessoal ou de terceiro, sinal de telefone, rádio, televisão, internet, dados de voz, imagem, vídeo ou outros bens imateriais com valor económico, por qualquer meio, é punido com pena de prisão até 1 ano, se pena mais grave não couber. A tentativa é punível.

Burla informática e nas comunicações (artigo 289), é caracterizado por causar 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 e; causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios 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, e é punido com pena de prisão até 3 anos ou com pena de multa.

Fraudes relativas aos instrumentos e canais de pagamento electrónico (artigo 294), é caracterizado por falsificar um instrumento ou canal de pagamento electrónico; aceder ilegalmente a um sistema de pagamento electrónico, mediante a violação indevida dos mecanismos de segurança; instalar objectos que afectem o funcionamento do canal ou sistema de pagamento electrónico, visando obter, adulterar ou destruir dados ou informações; apropriar-se ilicitamente de um instrumento de pagamento electrónico de outrem, incluindo o correspondente código secreto; possuir, detiver, importar, exportar, receber, transportar, vender ou transferir para terceiros instrumentos de pagamento electrónicos obtidos indevidamente ou que tenham sido objecto de contrafacção ou falsificação; e criar programas informáticos, instrumentos, objectos e outros meios preparados deliberadamente para a prática de infracções relacionadas com instrumentos de pagamento electrónicos; e é punido com pena de prisão de 1 a 3 anos e multa até 1 ano. E, quando as acções descritas anteriormente 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 prisão até 5 anos e multa até 1 ano.

E, por importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento sobre o qual tenha sido praticada qualquer das acções previstas no número 2, é punido com a pena de prisão até 5 anos.

Instrumento de pagamento electrónico é o dispositivo ou registo electrónico que permite ao utilizador transferir fundos ou pagar a um beneficiário.

Abuso de meios de pagamento electrónicos (artigo 295), caracterizado pelo abusando da possibilidade conferida pela posse de meios de pagamento electrónicos levar o emitente a fazer um pagamento ou causar prejuízo a este ou a terceiro, é punido com as penas de furto.

Falsidade informática (artigo 336), caracterizado por introduzir, 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; por actuar 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 anteriormente 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. e é punido com a pena de prisão de 1 a 5 anos e multa até 1 ano. E, por último, por importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções mencionadas anteriormente, é punido com a pena de prisão de 2 a 8 anos.

Interferência em dados (artigo 337), caracterizado por alterar, deteriorar, inutilizar, apagar, suprimir, destruir ou, de qualquer forma, alterar dados informáticos e; mediante a introdução ou transmissão de dados informáticos ou, por qualquer outra forma, instalando vulnerabilidades, interferir no funcionamento de sistema informático, causando intencionalmente dano a alguém, e é punido com a pena de prisão de 1 a 2 anos e multa correspondente.

Interferência em sistemas (artigo 338), caracterizado por alterar, deteriorar, inutilizar, apagar, suprimir, destruir ou, de qualquer forma, alterar dados informáticos e; mediante a introdução ou transmissão de dados informáticos ou, por qualquer outra forma, instalando vulnerabilidades, interferir no funcionamento de sistema informático, causando intencionalmente dano a alguém. E, é punido com a pena de prisão de 1 a 2 anos e multa correspondente.

Uso abusivo de dispositivos (artigo 339), caracterizado por 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 autorizadas, sem legitimidade e é punido com a pena de prisão de 1 a 2 anos.

Instigação pública a um crime (artigo 345), caracterizado por divulgar por escrito ou qualquer outro meio, provocar ou incitar à prática de um crime determinado, em reunião

pública, através de meio de comunicação social, e é punido com pena de prisão de 1 a 3 anos ou com pena de multa até 2 anos, se pena mais grave lhe não couber por força de outra disposição legal; por motivações religiosas, instigar outrem ou participar em actos de violência e perturbação da ordem pública, é punido com pena de prisão de 1 a 5 anos.

A pena não pode ser superior à prevista para o facto ilícito típico praticado.

Apologia pública ao crime (artigo 346), caracterizado por divulgar por escrito ou qualquer outro meio, recompensar ou louvar outra pessoa por ter praticado um crime, de forma adequada a criar perigo da prática de outro crime da mesma espécie, em reunião pública, através de meio de comunicação social, é punido com pena de prisão até 6 meses e multa correspondente, se pena mais grave lhe não couber por força de outra disposição legal.

A pena não pode ser superior à prevista para o facto ilícito típico praticado.

Publicidade da decisão condenatória (artigo 448), caracterizado por existência de decisão condenatória nos crimes previstos no Capítulo II da Lei n° 24/2019, de 24 de Dezembro (que aprova o Código Penal), relativamente à Corrupção e Crimes Conexos deve, ser dada publicidade em meio de comunicação social a determinar pelo tribunal, bem como através da afixação de edital, dela constando a identificação do servidor público, os elementos da infracção, as sanções aplicadas e a sua duração. 2. A publicidade da decisão condenatória é efectivada a expensas do condenado e no local de exercício da actividade, por período não inferior a 30 dias, por forma bem visível ao público.

Autoria do Crime

Para ZACARIAS (2016), citado por Nhamitambo (2025), 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. Há casos em que o criminoso, se faz passar por outra pessoa, mediante o uso indevido de suas senhas pessoais. E

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. 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 de determinada acção criminosa realizada em um serviço de Internet esta postulado na Lei de Revisão do Código Penal aprovadas pelo Parlamento em Julho de 2019.

Sujeito activo

É aquele que pratica o crime informático.

Sujeito passivo

O sujeito passivo pode ser uma pessoa colectiva pública ou privada, pessoa singular, a qual incide os actos praticado pelo sujeito activo. É a vítima.

Materialização do crime cibernético

Segundo Nhamitambo (2025), de modo geral, pode-se dizer que as evidências dos crimes cibernéticos são extremamente voláteis. 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 pena.

Conforme o COSTA (2016), citado por Nhamitambo (2025), as evidências dos crimes cibernéticos, em um computador, podem ser classificadas como evidências do usuário e evidências do sistema”. 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 produzidas pelo sistema operacional, em função da acção do sujeito activo.

Para MORRAIS (2015), “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”. E, diz também que, 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 ou até mitiga-los.

Conceito de crime

Segundo Nhamitambo (2025), Crime ou delito é todo o acontecimento, feita de forma voluntária em que a própria lei criminal diz tratar - se de crime. Nos termos do art. 1 da Lei nº 24/2019, de 24 de Dezembro, que aprova o Código Penal.

E, de salientar que existem crimes públicos (por exemplo: crimes informáticos), crimes semi - públicos (por exemplo: furto) e crime particular (por exemplo: crimes de injúria, difamação).

Evolução Legislativa em Materia de Crimes Informáticos ou Cibernéticos

Neste contexto, aumentou o uso da internet e, como consequência, o número de golpes virtuais. De acordo com Cadoso (2020), a criminalidade cibernética existe há tempos, no entanto, o avanço e a facilidade da utilização da internet e dos recursos tecnológicos compõe um ambiente atrativo para exploração de crimes.

Característica do agente criminoso

O agente é inteligente, culto, alfabetizado, possui um bom conhecimento em informática, utilizando subrefúgio como provedores alienígenas, identificadores (IPs) falsos, locais públicos de acesso à internet conhecidos como lan houses, alterações de IP na mudança de provedores.

Ao quebrar uma barreira de protecção digital, aquele programa torna - se vulnerável e obsoleto.

O agente criminoso, ao superar os bloqueios contra condutas proibidas, terá redução de tempo de exploração para tal conduta até que novos mecanismos impeçam a sua prática.

Sua identidade

Pelo novo *modus operandi*, o crime informático é sempre praticado por meio de um computador ou aparelho ligado a rede. Isto torna ainda mais difícil a identificação do infractor. Estamos perante um sujeito virtual comandado por um sujeito real.

CONCLUSÃO

De concluir que com a tipificação dos crimes informáticos em 2014, Moçambique hoje esta a caminhar a passos de camaleão. Havendo, atualmente necessidade de o legislador aprimorar aprovar a lei cibernética e que a mesma venha espelhar a realidade do dia-a-dia. O crime informático ou cibernético é cometido por meio das TIC's, atendendo a evolução no cenário da informação e tecnologia.

A identificação dos sujeitos ativos nos crimes informáticos é difícil, situação que se deve ao fato de que, em regra, os criminosos utilizam da rede de internet disponibilizada em espaços públicos. A transferência de dados não estaria protegida, situação que facilita a interceptação da prática delitiva, porém, dificulta a identificação dos agentes.

O combate à criminalidade digital em Moçambique perpassa não apenas a necessidade de tipificação das condutas danosas praticadas no ambiente virtual, como, também, necessita de uma política pública dirigida à educação dos usuários das redes. Além disso, é imperiosa a constante evolução das técnicas investigativas concernentes a essas práticas, assim como a remoção de barreiras legislativas concernentes à obtenção de dados dos agentes.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. Os objetos intangíveis na era da criminalidade informática. Espaço Jurídico, *Jornal of Law*, v.7, n.2, p.165-178, 2006. Disponível em: . Acesso em: 02 mar. 2021.

ARAÚJO, Fábio Lucena de. ASPECTOS JURÍDICOS NO COMBATE E PREVENÇÃO AO RANSOMWARE. In: DOMINGOS, Fernanda Teixeira Souza et al. Crimes cibernéticos:

coletânea de artigos. Brasília: MPF (Ministério Público Federal), 2018. Cap. 5. p. 90-115. Disponível em: <https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos>. Acesso em: 22 jul. 2021.

ASSUNÇÃO, Marcos Flávio Araújo. Segredos do Hacker Ético. 5. Ed. Florianópolis: Visual Books, 2014.

CAIADO, Felipe B.; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. In: DOMINGOS, Fernanda Teixeira Souza et al. Crimes cibernéticos: coletânea de artigos. Brasília: MPF (Ministério Público Federal), 2018. Cap. 1. p. 8 25. Disponível em: <https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos>. Acesso em: 22 jul. 2021.

CRESPO, Marcelo. Crimes digitais: do que estamos falando? 2015. Disponível em: <https://canalcienciascriminais.jusbrasil.com.br/noticias/199340959/crimes-digitais-do-que-estamos-falando>. Acesso em: 02 ago. 2021.

GIMENES, Emanuel Alberto Sperandio Garcia. Crimes virtuais. Revista de Doutrina: TRF4, [s. l], on line, 2013. Disponível em: https://revistadoutrina.trf4.jus.br/index.htm?https://revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html. Acesso em: 20 jul. 2021.

PIMENTEL, Alexandre Pinto; CARDOSO, Mateus Queiroz. A regulamentação do direito ao esquecimento na lei do marco civil da internet e a problemática da responsabilidade civil dos provedores. Revista da AJURIS, v. 42, n. 137, Mar., 2015.

NHAMITAMBO, Raul de Miguel Benjamim Jofrisse. ANÁLISE DA JURISPRUDÊNCIA NACIONAL E DAS LACUNAS EXISTENTES NA LEI MOÇAMBICANA EM RELAÇÃO AS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÕES: Analysis of national jurisprudence and gaps in mozambican law in relation to information and communications technologies. **RCMOS - Revista Científica Multidisciplinar O Saber**, Brasil, v. 1, n. 1, 2025. DOI: [10.51473/rcmos.v1i1.2025.972](https://doi.org/10.51473/rcmos.v1i1.2025.972). Disponível em: <https://submissoesrevistacientificaosaber.com/index.php/rcmos/article/view/972>. Acesso em: 3 maio. 2025.

SANTOS, Paulo Ernani Bergamo dos. Direito internacional e o combate à cibercriminalidade contra crianças. In: DOMINGOS, Fernanda Teixeira Souza et al. Crimes cibernéticos: coletânea de artigos. Brasília: MPF (Ministério Público Federal), 2018. Cap. 8. p. 156-183. Disponível em: <https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos>. Acesso em: 22 jul. 2021.

SORJ, Bernardo et al (org.). Sobrevivendo nas redes: guia do cidadão. São Paulo: Moderna, 2018. 82 p. Disponível em: https://crianca.mppr.mp.br/arquivos/File/publi/santillana/sobrevivendo_nas_redes_guia_2018.pdf. Acesso em: 05 jul. 2021.

SPINIELI, andré luiz pereira. Crimes informáticos: comentários ao projeto de lei nº 5.555/2013. In: DOMINGOS, Fernanda Teixeira Souza et al. Crimes cibernéticos: coletânea de artigos. Brasília: MPF (Ministério Público Federal), 2018. Cap. 10 p. 198-217. Disponível em: <https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos>. Acesso em: 22 jul. 2021.

LEGISLAÇÃO

MOÇAMBIQUE, Lei nº 24/2019, de 24 de Dezembro. Aprova a Lei de Revisão do Código Penal. Imprensa Nacional, Moçambique, MPT, 24 de Dezembro.

MOÇAMBIQUE, Lei nº 3/2017, de 9 de Janeiro. Estabelece os princípios, normas gerais e o regime jurídico das Transacções Electrónicas e do governo electrónico. Imprensa Nacional, Moçambique, MPT, 9 de Janeiro.

MOÇAMBIQUE, Lei nº 8/2004 de 21 de Julho. Aprova a Lei das Telecomunicações. Imprensa Nacional, Moçambique, MPT, 21 de Julho.

MOÇAMBIQUE, Decreto nº 75/2014 de 12 de Dezembro. Aprova o Regulamento de Controlo de Trafego de Telecomunicações. Imprensa Nacional, Moçambique, MPT, 12 de Dezembro.