CAPÍTULO 9

ANÁLISE DAS NOVAS TECNOLOGIAS NA INVESTIGACAO CRIMINAL EM MOÇAMBIQUE

https://doi.org/10.22533/at.ed.874192527109

Elísio Marcos Domingos João

RESUMO: Este artigo tem como tema a analise das novas tecnologias na investigação criminal em moçambique que pretende abordar como as novas tecnologias podem contribuir para a busca da verdade material e responsabilização dos criminosos assim como as dificuldades na investigação criminal com base nas novas tecnologias no ordenamento jurídico moçambicano. Para o presente artigo científico quanto a metodologia recorremos a uma pesquisa qualitativa é um tipo de pesquisa que utiliza uma busca de revisão bibliográfica em livros e artigos já publicados que abordam o tema em discussão.

PALAVRAS-CHAVES: Novas Tecnologias, Investigação Criminal, Moçambique.

Analysis of New Technologies in Criminal Investigation in Mozambique

ABSTRACT: This article analyzes new technologies in criminal investigations in Mozambique, aiming to address how these technologies can contribute to the pursuit of material truth and the accountability of criminals, as well as the difficulties faced in criminal investigations based on new technologies within the Mozambican legal system. For this scientific article, we used a qualitative research methodology, a type of research that utilizes a bibliographic review of previously published books and articles addressing the topic under discussion.

KEYWORDS: New Technologies, Criminal Investigation, Mozambique.

INTRODUÇÃO

A internet foi o início de um grande avanço dentro do contexto do mundo globalizado, onde o fácil acesso e a rapidez em busca de informação foi um dos principais fundamentos, pois basta entrar em um ***site*** e escrever o que procura para obter as informações de forma rápida, segundo Correia[1].

Tendo em vista que cada dia que se passa, mais pessoas recorrem a internet como meio de obtenção de informação, para lazer, estudos, e venda e compra de objectos. Apesar dessas facilidades, esse cenário também deixa o usuário a mercê de criminosos, que se valem desse meio para praticar os mais variados tipos de crimes.

Com o advento da internet em diversos lares e lugares, os crimes que já são tipificados pelo Código Penal passaram a ser praticados no ambiente virtual, sendo que o criminoso fica "*escondido através da rede*", dificultando a localização da autoria dos crimes.

Inúmeros são os benefícios trazidos com o surgimento da Internet, porem esse avanço esta correndo ao lado da utilização ilimitada e indiscriminada desse meio virtual, favorecendo os acontecimentos de crimes cibernéticos e assim dando alerta aos olhos de jurisdição na esfera Processual Penal.

Nesse mesmo contexto verifica-se que o Estado como protector dos direitos deve rever a questão jurídica das provas e dos meios de sua obtenção no Processo Penal Moçambicano para se adequar as inovações científicas e tecnológicas, garantindo um processo penal com resultados que cumpram com as garantias constitucionais.

As provas no processo penal são de fundamental importância para a formar a convicção do juiz, ou seja, ele são a peca chave para a sua deliberação. Portanto, se o mundo se encontra influenciado pelos efeitos virtuais, as provas obtidas por meio virtual terão de ter a mesma eficiência como qualquer outro tipo de prova vigente na nossa legislação.[2]

Segundo o relatório da PGR -2024 o crime de fraude relativo aos instrumentos e canais de pagamento electrónico em Moçambique registou, em 2024, um total de 492 casos, o maior número de processos, seguido de furto de fluido com 286, e burla informática e nas comunicações com 177, em 2024, os dados indicam que a PGR registou um total de 1.061 processos de crimes informáticos, contra 912, em 2023, o que representa um acréscimo de 149 casos, correspondente a 16,3 por cento.[3]

A obtenção de prova por meio virtual seria o meio cabal advindo do avanço tecnológico, ou seja, os crimes estão acontecendo virtualmente, então as provas

1. CORREA, Gustavo Testa. Aspectos Jurídicos da Internet. São Paulo. 2000.
2. LEONARDI, Marcel. Tutela e Privacidade na Internet, São Paulo, Saraiva, 2012, P. 38.
3. https://aimnews.org/2025/04/29/mocambique-regista-centenas-de-burlas-de-pagamentos-eletronicos/ Acessado em 25/06/2025, pelas 16 horas.

concretas, terão de vir também pelo meio virtual. Deste modo, para que essas provas, sejam colhidas de forma integral, deve-se ter materiais suficientes para a conservação e defesa das provas a fim de não serem modificadas no processo de investigação.[4]

Assim sendo, surge um questionamento: como utilizar meios adequados (equipamentos de alta tecnologia ou programas para identificar as pessoas responsáveis) para produção de provas e a eficácia do regime de produção de provas nos crimes cibernéticos no nosso ordenamento jurídico?

IMPACTOS DAS NOVAS TECNOLOGIAS NA INVESTIGAÇÃO CRIMINAL

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

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

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

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

4. COLLI, Maciel. Cibercrimes, Limites e Perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá Editora, 2010.

- Decreto nº 59/2019, de 3 de Julho, Regulamento do Sistema de Certificação Digital de Moçambique.

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

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

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

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

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

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

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

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

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

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

No âmbito desta lei, serão dados pessoais qualquer informação relativa a uma pessoa singular que possa ser identificada directa ou através da referência a um número de identificação ou a um ou mais factores específicos à mesma. Nesse contexto, esses dados têm protecção legal devidamente prevista na CRM[5] que, proíbe o acesso a arquivos, ficheiros e registos informáticos ou de bancos de dados para conhecimento de dados pessoais relativos a terceiros.

Investigação para prova digital

Nos crimes virtuais, os meios de prova desempenham um papel crucial na investigação, julgamento e punição dos infractores. No entanto, a natureza digital desses delitos apresenta desafios únicos para a colecta, autenticação e apresentação de evidências em tribunal, segundo OLIVEIRA[6].

Um dos principais meios de prova em casos de crimes cibernéticos são os registros electrónicos, que incluem *logs* de servidor, registros de actividade de rede, históricos de navegação na web e comunicações electrónicas. Esses registros podem fornecer informações essenciais sobre as acções dos suspeitos *online*, incluindo actividades fraudulentas, invasões de sistemas e transferências ilegais de dados.[7]

Além dos registros electrónicos, as evidências digitais podem incluir arquivos de mídia, como fotos, vídeos e áudios, mensagens de texto, *e-mails*, documentos electrónicos e registros de transacções financeiras. A autenticidade e integridade dessas evidências são fundamentais para sua admissibilidade em tribunal, exigindo métodos robustos de preservação e análise forense digital, afirma SODRÉ[8].

No entanto, a colecta e preservação adequadas das evidências digitais podem ser desafiadoras devido à sua natureza volátil e facilmente manipulável. Alterações inadvertidas nos dados electrónicos podem comprometer sua credibilidade e utilidade como prova, destacando a importância de protocolos claros de manuseio e cadeia de custódia para garantir a integridade das evidências.[9]

5. Cfr. nº 3, artigo 71, Constituição da República de Moçambique.
6. OLIVEIRA, Lais. Crimes Cibernéticos e a Legislação Brasileira. 2020
7. LÔ, Willian Andrade. A (in) eficácia da produção de provas oriundas do ambiente digital em face aos crimes cibernéticos. 2022.
8. SODRÉ, Ludmilla Gonçalo da Silva. As dificuldades na colheita de elementos de autoria e materialidade delitiva dos Crimes Cibernéticos. 2022.
9. Idem

Além das evidências técnicas, depoimentos de testemunhas e especialistas em computação forense também podem fornecer informações valiosas sobre a natureza e a extensão dos crimes cibernéticos. Esses especialistas podem explicar as complexidades técnicas envolvidas nos ataques cibernéticos, identificar vulnerabilidades em sistemas de segurança e ajudar a reconstruir eventos digitais para apresentar um caso convincente em tribunal.

É importante ressaltar que a admissibilidade das evidências digitais em tribunal depende não apenas de sua autenticidade e integridade, mas também da conformidade com os padrões legais de colecta e apresentação de provas, de acordo com LÔ[10]. Isso inclui considerações sobre a privacidade e os direitos constitucionais dos indivíduos, bem como as leis e regulamentos específicos que regem a obtenção e utilização de dados electrónicos.

CONCLUSÃO

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

O actual cenário legislativo do cibercrime é composto por dispositivos que prevêem e punem infracções criminais cometidas por via das redes de conexão, porém, esse cenário precisa de ser melhorado, através da criação de legislação específica para crimes cibernéticos. Após análise e estudo do panorama penal em que está circunscrita a prova digital, chega-se à conclusão que 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. Moçambique aderiu, mas não ratificou a Convenção de Budapeste, que facilitaria

10. LÔ, Willian Andrade. A (in) eficácia da produção de provas oriundas do ambiente digital em face aos crimes cibernéticos. 2022.

a cooperação internacional e a recolha de obtenção de prova digital e enfrentamos ainda dificuldades como a Falta de equipamento tecnológico adequado para os profissionais de justiça criminal bem como a falta de pessoal qualificado em matéria de criminalidade informática.

RECOMENDAÇÕES

Do exposto recomenda-se:

- Criação de uma lei específica e interna sobre crimes cibernéticos onde se estabelece a prova digital e os 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.
- Ratificação da Convenção de Budapeste, que facilitaria a cooperação internacional e a recolha de obtenção de prova digital, buscando inspiração no direito comparado de países como Portugal e Brasil.
- Investir em equipamentos tecnológico adequado para os profissionais de justiça criminal para melhor produção de provas nos crimes cibernéticos e a descoberta da verdade material.
- Investir em formação contínua do pessoal do SERNIC (Serviço Nacional de Investigação Criminal) em matéria de crimes cibernéticos.

REFERÊNCIAS

1. Doutrina

CORREA, Gustavo Testa. Aspectos Jurídico da Internet. São Paulo: Saraiva, 2002.

COLLI, Maciel. Cibercrimes, Limites e Perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá Editora, 2010.

LÔ, Willian Andrade. A (in) eficácia da produção de provas oriundas do ambiente digital em face aos crimes cibernéticos. 2022.

LEONARDI, Marcel. Tutela e Privacidade na Internet, São Paulo, Saraiva, 2012.

SODRÉ, Ludmilla Gonçalo da Silva. As dificuldades na colheita de elementos de autoria e materialidade delitiva dos Crimes Cibernéticos. 2022.

OLIVEIRA, Lais. Crimes Cibernéticos e a Legislação Brasileira. 2020.

2. Legislação usada

Constituição da República de Mocambique-2004- Publicada no Boletim da República, 1 Série, número 51 de 22 de Dezembro de 2004- actualizada pela Lei 1/2018 de 12 de Junho.

Código Penal da República de Moçambique aprovado pela Lei número 24/2019 de 24 de Dezembro, Boletim da República, I série, número 5.

Código de Processo Penal da República de Moçambique aprovado pela Lei número 25/2019 de 26 de Dezembro no Boletim da República, I Série, número 249.

Lei nº 3/2017, de 19 de Janeiro – Lei das Transacções Electrónicas.