UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE DIREITO

LICENCIATURA EM DIREITO

TRABALHO DE FINAL DE CURSO

A RESPONSABILIDADE LEGAL DOS BANCOS NA PREVENÇÃO E INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS EM MOÇAMBIQUE

O Discente:

Marcos Armando Nabingo

O Supervisor:

Manuel Castiano, Ph.D.

Maputo, 14 de Fevereiro de 2025

Marcos Armando Nabingo

A RESPONSABILIDADE LEGAL DOS BANCOS NA PREVENÇÃO E INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS EM MOÇAMBIQUE

LICENCIATURA EM DIREITO

TRABALHO FINAL DE CURSO A SER APRESENTADO À FACULDADE DE DIREITO DA UNIVERSIDADE EDUARDO MONDLANE PARA A OBTENÇÃO DO GRAU DE LICENCIATURA EM DIREITO

O Discente:

Marcos Armando Nabingo

O Supervisor:

Manuel Castiano, Ph.D.

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE DIREITO

Maputo, Fevereiro de 2025

DECLARAÇÃO DE HONRA

Eu, Marcos Armando Nabingo, declaro por minha honra que o presente trabalho é da minha autoria e orientação dos tutores, feita segundo as regras em vigor na Faculdade de Direito da Universidade Eduardo Mondlane, nunca foi anteriormente apresentado em nenhuma instituição para a obtenção de qualquer grau académico. O seu conteúdo é original e todas as fontes consultadas estão devidamente citadas no texto e nas referências bibliográficas.

Autor

Marcos Armando Nabingo

DEDICATÓRIA

Dedico este trabalho aos meus filhos Ivone e Emmanuel, por lhes ter roubado maior atenção.

AGRADECIMENTOS

A Deus pelo dom da vida que sempre tem me concedido, que ao mesmo tempo inclui saúde, bem-estar e sabedoria;

Aos meus pais Fofoana Armando Nabingo e Ivone André Quana ambos em memória, pois em vida souberam-me transmitir amor, educação, integridade que na base deles me proporcionou um desenvolvimento pessoal;

À minha esposa, Judite Justino Mabota, pelo amor, companheirismo, apoio incondicional e confiança, vai um agradecimento especial;

Aos meus irmãos e demais familiares, pelo apoio moral e companheirismo que me concedem em todos os momentos da vida;

Ao meu tutor, Doutor Manuel Castiano, a minha profunda e especial gratidão por ter-me concedido disponibilidade, sabedoria e objectividade nos ensinamentos constantes em todo o percurso de orientação científica desta monografia;

A todos docentes do curso de licenciatura, que souberam conceder o seu saber para fazer de mim o estudante que sou;

Aos meus colegas da turma 2019, pelos momentos que partilhamos colhendo ensinamentos de forma recíproca, em especial ao drs. Manecas Chiziane, Edmilson Taula, Momed Madogy Curantilal e Quisito Ferro, por me terem incentivado a não desistir quando eclodiu a Covid19, pois foi um tempo muito complicado para mim.

ABREVIATURAS, SIGLAS E ACRÓNIMOS

Art.	Artigo
BCI	Banco Comercial e de Investimentos, SA
BIM	Banco Internacional de Moçambique, SA.
GAFI	Grupo de Acção Financeira Internacional
SERNIC	Serviço Nacional de Investigação Criminal
TDIC	Teoria da Detecção e Investigação Criminal
TIC	Tecnologias de Informação e Comunicação
UEM	Universidade Eduardo Mondlane
UIT	União Internacional de Telecomunicações

RESUMO

Com o avanço das tecnologias digitais, o sistema bancário tem enfrentado desafios crescentes no combate aos crimes cibernéticos. Este trabalho analisa a responsabilidade legal dos bancos na prevenção e investigação de delitos cibernéticos, destacando o papel das instituições financeiras na protecção de dados e na segurança das transacções digitais. A pesquisa explora a legislação pertinente, como a Lei 3/2017 de 9 de Janeiro e as normas internacionais de segurança bancária, além de discutir os mecanismos de defesa utilizados pelas instituições, como sistemas de monitoramento e criptografia. Também são analisados os esforços de colaboração entre bancos, autoridades reguladoras e órgãos de segurança pública na investigação de fraudes cibernéticas. Através da revisão da doutrina e estudo de casos, o trabalho propõe soluções para fortalecer a actuação dos bancos no combate aos crimes cibernéticos, sugerindo melhorias nas práticas e regulamentações existentes. O estudo busca, ainda, reflectir sobre a responsabilidade compartilhada entre as partes envolvidas para garantir um ambiente seguro para as transacções financeiras digitais.

Palavras-chave: *responsabilidade legal, bancos, crimes cibernéticos, prevenção e investigação.*

ABSTRACT

With the advancement of digital technologies, the banking system faces growing challenges in combating cybercrimes. This paper analyzes the legal responsibility of banks in preventing and investigating cybercrimes, highlighting the role of financial institutions in data protection and the security of digital transactions. The research explores relevant legislation, such as the Law 3/2017 of 9 of January, and international banking security standards, in addition to discussing the defense mechanisms used by institutions, such as monitoring systems and encryption. It also examines the collaboration efforts between banks, regulatory authorities, and public security agencies in investigating cyber frauds. Through a review of the literature and case studies, the paper proposes solutions to strengthen the role of banks in combating cybercrimes, suggesting improvements in existing practices and regulations. The study also reflects on the shared responsibility among the involved parties to ensure a secure environment for digital financial transactions.

Keywords: *legal responsibility, banks, cybercrimes, prevention and investigation.*

ÍNDICE

DECLARAÇÃO DE HONRA i
DEDICATÓRIA ii
AGRADECIMENTOS iii
ABREVIATURAS, SIGLAS E ACRÓNIMOS iv
RESUMO v
ABSTRACT vi
INTRODUÇÃO 1
Contextualização 1
Problema da pesquisa 4
Hipóteses 5
Justificativa 5
Objectivos 6
Geral **6**
Específicos **6**
Metodologia 6
Revisão Bibliográfica **6**
Análise documental **7**
Método de análise dos dados **7**
Estrutura do Trabalho 7
CAPÍTULO I: CRIMES CIBERNÉTICOS NO SECTOR BANCÁRIO 9
1.1. Conceito de crime e Cibercrime 9
1.2. Tipologias de Crimes Cibernéticos 11
1.3 A Segurança Cibernética 14
1.4 A prevenção do crime cibernético. 17
CAPÍTULO II: ANÁLISE JURÍDICA DAS LEIS RELEVANTES NO CONTEXTO DA RESPONSABILIDADE LEGAL DOS BANCOS EM CRIMES CIBERNÉTICOS 18
2.1. A Lei das Transacções Electrónicas (Lei n.º 3/2017 de 9 de Janeiro) 18
2.2. Lei de Supervisão Bancária (Lei n.º 20/2020, de 31 de Dezembro) 20
2.2.1. Pontos Positivos **20**
2.2.2. Lacunas Jurídicas **21**
CAPÍTULO III: RESPONSABILIDADE LEGAL DOS BANCOS NA PREVENÇÃO DE CRIMES CIBERNÉTICOS 22
3.1. Definição da Responsabilidade Legal 22
3.1.1. A responsabilidade dos Bancos **22**
3.1.2 O Risco associado a actividade bancária **23**

3.1.3 Risco de Tecnologia de Informação (TI)**.....24**
3.2. Responsabilidade Civil dos Bancos na Prevenção e investigação do Cibercrime 26
3.2.2. Limites à responsabilidade dos bancos.**.....30**
3.3. Responsabilidade Criminal dos Bancos como Pessoas Colectivas.....32
3.3.1. Conceito de pessoa colectiva 32
3.3.2. Fundamentos da Responsabilidade Criminal das pessoas colectivas.....32
3.3.3. Critérios Para Estabelecer a Responsabilidade Criminal das pessoas colectivas.....34
3.3.4. Sanções Penais Aplicáveis às Pessoas Colectivas 35
3.3.5. Eficácia da Responsabilidade Criminal das Pessoas Colectivas na Prevenção de crimes 36
3.3.6. Análise comparativa das Leis 35/2014 e 24/2019 de 24 de Dezembro 36
3.4. Desafios na Investigação de Crimes Cibernéticos no Sector Bancário.....39
3.4.1. A Prevenção dos ataques cibernéticos**.....39**
3.4.2. A Investigação do Cibercrime **.....39**
CONCLUSÃO 41
RECOMENDAÇÕES.....42
REFERÊNCIA BIBLIOGRÁFICA.....43

INTRODUÇÃO

A ascensão das tecnologias digitais revolucionou os sistemas financeiros em escala global, promovendo avanços significativos na prestação de serviços bancários. Contudo, esse progresso trouxe consigo um aumento exponencial dos riscos associados aos crimes cibernéticos, os quais se tornaram uma ameaça substancial à segurança econômica e à estabilidade do sector financeiro. Em Moçambique, o ambiente digital dos bancos tem sido alvo recorrente de actividades ilícitas como fraudes, acessos não autorizados e roubo de informações sensíveis, desafiando não apenas as instituições financeiras, mas também o aparato legislativo e regulatório[1].

Nas últimas décadas, a internet transformou profundamente o funcionamento da sociedade, especialmente no sector financeiro. A integração das Tecnologias de Informação e Comunicação (TIC) permitiu a automação de processos bancários e a criação de novas formas de interação entre os bancos e os clientes. Segundo Castells, a revolução digital criou uma "sociedade em rede", onde as transações financeiras e os serviços bancários dependem fortemente da conectividade digital[2].

Em Moçambique, o crescimento do uso da internet nas instituições financeiras tem facilitado a inclusão financeira, mas, ao mesmo tempo, tem exposto os bancos a uma série de novos riscos, incluindo os crimes cibernéticos [3].

Nesse cenário, a responsabilidade legal dos bancos adquire um papel central na proteção contra ataques cibernéticos, uma vez que essas instituições actuam como guardiãs de informações financeiras e dados pessoais dos cidadãos. A legislação moçambicana, notadamente a Lei n.º 3/2017, de 9 de Janeiro, sobre transações electrónicas, estabelece um arcabouço normativo que visa orientar a actuação das instituições financeiras na prevenção, mitigação e, quando necessário, investigação de ilícitos cibernéticos. No entanto, a efectividade dessa legislação e sua aplicação prática ainda suscitam questionamentos, sobretudo diante da crescente

[1] MATAVELE, Fernando. Criminalidade cibernética em Moçambique: Uma análise sob a perspectiva do direito penal. Revista de Estudos Jurídicos, 2019. Pg: 22.

[2] CASTELLS, Manuel. A Sociedade em Rede. São Paulo, Paz e Terra. 2009. Pag: 28

[3] NDAVUKO, Sérgio. Segurança Cibernética em Moçambique: Desafios e Perspectivas. Maputo, UEM. 2021. Pag:8

sofisticação das técnicas utilizadas por criminosos e das limitações estruturais e tecnológicas de algumas instituições bancárias no país[4].

O presente trabalho tem como objectivo central analisar as responsabilidades legais atribuídas aos bancos em Moçambique na prevenção e investigação de crimes cibernéticos, a partir de uma abordagem teórica e normativa. Para tanto, a pesquisa adopta uma metodologia qualitativa, baseada em revisão bibliográfica e análise documental de legislações nacionais, doutrinas jurídicas e relatórios de organismos nacionais e ou internacionais sobre cibersegurança e protecção de dados no sector financeiro.

A relevância desta investigação reside na possibilidade de identificar lacunas e desafios no cumprimento das responsabilidades legais pelas instituições bancárias, bem como propor reflexões críticas acerca do papel do Estado e das instituições privadas na proteção do sistema financeiro contra ameaças cibernéticas. Assim, busca-se contribuir para o aprimoramento das estratégias de combate aos crimes cibernéticos no contexto moçambicano, em conformidade com as melhores práticas internacionais e com os princípios da segurança jurídica e da eficiência institucional.

Crimes informáticos e cibernéticos são delitos em rápido crescimento. Os termos "crime informático" e "*cibercrime*", que são frequentemente sinônimos e usados de forma intercalar, referem-se a actos criminosos em uma ou mais de três categorias: uma forma tradicional de crime cometido através de redes de comunicações eletrônicas e sistemas de informação, a publicação de conteúdo ilegal em mídia eletrônica ou qualquer crime exclusivo de redes eletrônicas[5]. Assim, o nosso ordenamento jurídico usa o termo crimes informáticos conforme a secção IV, do capítulo I no título IV do CP, mas neste trabalho optamos em usar a designação *cibercrime*, uma vez que a maior parte da doutrina consultada usa esta expressão.

Contextualização

Com o rápido avanço da tecnologia e a globalização digital, os crimes cibernéticos tornaram-se uma das maiores ameaças às instituições financeiras em todo o mundo. O desenvolvimento

[4]JANUÁRIO, T., & CHONGO, D.. *Segurança cibernética no setor financeiro: Desafios e oportunidades em Moçambique*. Maputo: Editora Jurídica Moçambicana. 2021. Pg: 45.

[5] TAVARES, TDR at. All. Crimes Informáticos e Cibernéticos: Ciências Jurídicas, Vol-28, Ed-133, sem local, 2024. Pg: 3.

da internet trouxe inúmeros benefícios para o sector bancário, como a automatização de serviços e o acesso remoto a transacções. Entretanto, essa mesma inovação tecnológica tem sido explorada por criminosos para cometer fraudes e violações de segurança digital.

Em Moçambique, o uso crescente da internet nos bancos resultou em uma série de novos desafios para o sector financeiro, especialmente no que se refere à segurança cibernética. De acordo com Mucavele, embora o país tenha implementado medidas regulatórias, na Lei das transacções electrónicas, o número de ataques cibernéticos a instituições financeiras continua a crescer. Além disso, a falta de uma infra-estrutura robusta e de treinamento especializado em ciber-segurança agrava a vulnerabilidade do sistema bancário[6].

Os bancos, enquanto guardiões dos recursos financeiros de indivíduos e empresas, têm a responsabilidade não apenas de proteger esses activos, mas também de colaborar com as autoridades na prevenção e investigação de crimes cibernéticos.

Internacionalmente, o combate aos crimes cibernéticos tem sido uma prioridade para diversas organizações, como a Europol e o Grupo de Acção Financeira Internacional (GAFI), que publicam directrizes para aumentar a segurança nos sistemas financeiros. É digno salientar que as melhores práticas internacionais incluem o uso de inteligência artificial e *machine learning* para monitoramento contínuo de ameaças, bem como a cooperação entre bancos, governos e entidades de segurança cibernética.

No contexto moçambicano, os bancos comerciais e o Banco de Moçambique estão, de acordo com Ndavuko [7], no centro das atenções por sua responsabilidade legal de garantir que medidas eficazes sejam adoptadas para mitigar os impactos dos crimes cibernéticos. A eficácia dessas medidas, no entanto, depende não apenas da adopção de tecnologia avançada, mas também de uma colaboração activa com o Serviço Nacional de Investigação Criminal (SERNIC), responsável pela investigação de tais crimes. Esta colaboração visa garantir que os criminosos sejam identificados e responsabilizados, como reforçado por Oliveira[8], que aponta a necessidade urgente de fortalecer a capacidade investigativa em cibercrimes no país.

---

[6] MUCAVELE, Carlos. 2020, Op cit, pag:17

[7] NDAVUKO, Sérgio. Segurança Cibernética em Moçambique: Desafios e Perspectivas. Maputo, UEM. 2021, Op cit, pag.13

[8] OLIVEIRA, J. A ciber-segurança no sector bancário: Desafios e soluções. Revista de Direito Financeiro.S/ed, S/l, 2022.Pag:6

Portanto, a responsabilidade dos bancos em Moçambique deve ser analisada tanto sob a óptica da prevenção quanto da investigação, considerando os desafios locais e as melhores práticas globais. Este estudo busca explorar essas responsabilidades e sugerir caminhos para o fortalecimento da segurança cibernética no sector bancário moçambicano, alinhando-se às exigências do regime jurídico actual.

Problema da pesquisa

Com o crescimento acelerado da digitalização e o aumento do uso da *internet* no sector bancário, os bancos moçambicanos têm enfrentado uma série de novos desafios relacionados à segurança cibernética. O avanço da tecnologia, embora essencial para a modernização do sistema financeiro, trouxe consigo a expansão dos crimes cibernéticos, que têm-se tornado cada vez mais sofisticados e difíceis de detectar[9].

Em Moçambique, a implementação de serviços bancários digitais, como o *internet banking* e as transferências electrónicas via M-Pesa, E-mola e M-Kesh, aumentou a conveniência para os clientes, mas também abriu espaço para ataques cibernéticos, como fraudes e acessos não autorizados a contas bancárias[10].

Ademais, tem-se visto várias situações em que são recebidas mensagens para envio de determinado valor para contactos desconhecidos. Verificam-se páginas que apresentam teor suspeito e propícia para fraudes. Noutro prisma, há situações de clonagem de cartões bancários, sequestro de contas em redes sociais e depois exige-se resgate, como também, se tem visto situações de ataque de endereços electrónicos, o que lhes permite acesso às contas bancárias através de *internet banking.*

Por via disso, suscita-nos a questão central que este estudo busca responder que é: *Qual é a responsabilidade legal dos bancos na prevenção e investigação de crimes cibernéticos em Moçambique*?

[9] NDAVUKO, Sérgio. Segurança Cibernética em Moçambique: Desafios e Perspectivas. Maputo, UEM. 2021, Op cit, pag:10

[10] MUCAVELE, Carlos. Crimes cibernéticos e o sistema bancário moçambicano. Maputo: Escola Superior de Economia e Gestão. 2020, Pag:15

Hipóteses

- ✓ O regime jurídico existente em Moçambique relacionado aos crimes cibernéticos é insuficiente para assegurar que os bancos desempenhem um papel efectivo na prevenção e investigação desses crimes.
- ✓ A responsabilidade dos bancos comerciais na prevenção e investigação de crimes cibernéticos difere significativamente da responsabilidade do Banco de Moçambique, que actua mais como regulador e supervisor.

Justificativa

A transformação digital e o aumento do uso da internet nas operações bancárias trouxeram não apenas novas oportunidades, mas também desafios significativos para o sector financeiro, especialmente no que diz respeito à segurança cibernética. Moçambique, assim como muitos outros países em desenvolvimento, está enfrentando uma crescente ameaça de crimes cibernéticos, à medida que suas instituições financeiras avançam na adopção de novas tecnologias. Segundo Ndavuko[11], o aumento de fraudes e acessos indevidos a sistemas bancários, têm impactado directamente a confiança do público nos serviços bancários digitais. Esse cenário torna imprescindível uma investigação detalhada sobre a responsabilidade legal dos bancos na prevenção e investigação desses crimes.

Este trabalho é justificado pela necessidade de analisar o regime jurídico e a contribuição dos bancos na investigação do cibercrime, identificando quais medidas os bancos têm adoptado e até que ponto elas são eficazes na protecção dos dados e dos sistemas financeiros.

Do ponto de vista prático, o tema é altamente relevante para as instituições financeiras moçambicanas, na medida em que enfrentam pressões crescentes para garantir a segurança dos sistemas bancários e das informações dos clientes.

Por fim, esta investigação justifica-se pelo seu potencial impacto na confiança pública no sector bancário digital, visto que a crescente incidência de crimes cibernéticos pode minar a adopção de serviços bancários digitais, essenciais para a inclusão financeira e o desenvolvimento económico de Moçambique. Ao fortalecer a ciber-segurança e a colaboração entre bancos e órgãos de investigação, espera-se que o estudo contribua para um ambiente financeiro mais seguro e confiável no país.

[11] NDAVUKO, Sérgio. Op Cit. Pg: 13

Objectivos

Geral

- ✓ Compreender a responsabilidade legal dos bancos na prevenção e investigação de crimes cibernéticos em Moçambique.

Específicos

- ✓ Descrever o regime jurídico do crime cibernético em Moçambique;
- ✓ Verificar o papel dos bancos na prevenção e investigação dos crimes cibernéticos;
- ✓ Analisar a responsabilidade dos bancos em Moçambique.

Metodologia

A presente pesquisa, é de carácter qualitativo e exploratório, adopta uma abordagem teórica e normativa para analisar a responsabilidade legal dos bancos em Moçambique na prevenção e investigação de crimes cibernéticos. Esta metodologia foi escolhida em razão da complexidade do tema e da necessidade de compreender as bases legais, os desafios e as implicações práticas envolvidas no cumprimento das obrigações impostas às instituições financeiras no contexto moçambicano.

A escolha dessa metodologia está alinhada com os objectivos da pesquisa, uma vez que o tema exige uma análise aprofundada das normas legais e de sua aplicação prática no contexto bancário. Além disso, o enfoque teórico permite a realização do estudo dentro das limitações temporais e de recursos disponíveis, sem comprometer a qualidade e a profundidade da investigação.

O estudo fundamenta-se em duas estratégias principais de pesquisa: a revisão bibliográfica e a análise documental.

Revisão Bibliográfica

A revisão bibliográfica consiste na análise crítica de literatura relevante e actual sobre os conceitos de crimes cibernéticos, responsabilidade legal e segurança digital no sector bancário. Examinamos livros, artigos científicos, relatórios de organizações nacionais, internacionais e estudos já publicados que abordem o impacto das actividades cibernéticas no sector financeiro, com ênfase no contexto moçambicano e em experiências internacionais correlatas. Essa etapa

permite identificar os principais conceitos, teorias e abordagens que fundamentam o tema, bem como estabelecer um diálogo com outros autores[12].

Análise documental

A análise documental será voltada à interpretação de normas legais e regulamentações relacionadas à segurança cibernética e à protecção de dados em Moçambique. Em particular, serão examinadas a Lei n.º 3/2017, de 9 de Janeiro, conhecida como Lei das transacções electrónicas, e outras legislações complementares que estabelecem obrigações específicas às instituições bancárias. Essa abordagem possibilitará uma compreensão detalhada do arcabouço jurídico aplicável e das lacunas existentes na legislação[13].

Delimitação da pesquisa

Considerando a limitação temporal e a ausência de colecta de dados empíricos, o estudo restringe-se a fontes secundárias, tais como publicações académicas, relatórios institucionais e documentos legais. Não serão realizadas entrevistas ou estudos de caso, sendo a análise voltada exclusivamente para a interpretação teórica e normativa.

Método de análise dos dados

A análise dos dados será conduzida de forma qualitativa e interpretativa, com base na hermenêutica jurídica e no confronto das normas analisadas com os conceitos teóricos extraídos da literatura revisada. Essa abordagem permitirá avaliar como a legislação moçambicana tem sido estruturada para prevenir e combater crimes cibernéticos e identificar possíveis desafios enfrentados pelos bancos no cumprimento dessas disposições legais.

Estrutura do Trabalho

O presente trabalho encontra-se dividido em duas partes. A primeira parte é referente à introdução do trabalho que engloba as hipóteses, a contextualização, a justificativa, os objectivos, a metodologia e a estrutura do trabalho. A segunda parte do trabalho encontra-se estruturado em quatro capítulos. O primeiro capítulo debruça-se sobre os crimes cibernéticos

[12] GIL, António Carlos. Métodos e Técnicas de Pesquisa Social. 6ª Ed. São Paulo: Editora Atlas. 2008. Pg: 44

[13] BOWEN, Glenn. A. Document analysis as a qualitative research method. *Qualitative Research Journal, Vol.9 2ª Ed*, sem local, 2009. Pg: 27-40.

no sector bancário. Faz-se uma abordagem das tipologias de crimes cibernéticos. No segundo capítulo debate-se sobre a análise jurídica das leis relevantes no contexto da responsabilidade legal dos bancos em crimes cibernéticos. Por último, encontra-se o terceiro capítulo relativo a responsabilidade legal dos bancos na prevenção de crimes cibernéticos. De salientar que este capítulo engloba também a conclusão do trabalho e as recomendações.

CAPÍTULO I: CRIMES CIBERNÉTICOS NO SECTOR BANCÁRIO

1.1. Conceito de crime e Cibercrime

O conceito de crime é fundamental para compreender os actos que devem ser prevenidos e investigados, especialmente no contexto de crimes cibernéticos que envolvem instituições financeiras.

O crime será um facto voluntário, típico, ilícito e culpável declarado punível pela lei penal, este conceito e definido tendo em conta o direito positivo ou constituído, pois é ele que delimita o âmbito do conceito e ainda sugere a miscigenação do aspecto formal e material[14].

Os crimes cibernéticos são definidos como actos ilícitos cometidos em ambientes digitais, têm impactado profundamente o sector bancário em todo o mundo. Esses crimes incluem desde fraudes financeiras, *phishing* e *ransomware*, até o acesso não autorizado a dados confidenciais[15]. No contexto bancário, essas práticas prejudicam tanto os clientes quanto as instituições financeiras, gerando perdas financeiras significativas, danos reputacionais e comprometendo a confiança no sistema bancário.

Em Moçambique, o rápido crescimento das transacções digitais tem aumentado a vulnerabilidade do sector financeiro aos crimes cibernéticos. Matavele, aponta que o uso de tecnologias como *internet banking* e aplicativos móveis, apesar de facilitar o acesso aos serviços bancários, expõe os usuários a ataques, especialmente em um cenário marcado pela baixa consciencialização sobre segurança cibernética. Além disso, a falta de uma infra-estrutura robusta de protecção digital tem dificultado a resposta eficaz a essas ameaças[16].

De acordo com a União Internacional de Telecomunicações (UIT)[17], Moçambique apresenta desafios relacionados à falta de mecanismos técnicos e institucionais adequados para mitigar crimes cibernéticos no sector financeiro. Esse cenário reforça a necessidade de medidas

[14] MACIE, Albano. Manual de direito Penal, Parte Geral, Volume I, Escolar Editora, 2021. Pag: 155.

[15] GONDWE, Gregory.Op Cit. Pg: 57.

[16] MATAVELE, Fernando. Op Cit. Pg: 28.

[17] União Internacional de Telecomunicações (UIT). (2021). *Global Cybersecurity Index 2020*. Geneva: ITU Publications.

preventivas mais eficazes por parte das instituições bancárias, em alinhamento com as obrigações legais.

Além disso, a utilização de técnicas de branqueamento de capitais e financiamento ao terrorismo via meios digitais, muitas vezes ligadas a crimes cibernéticos, representa uma ameaça adicional às instituições bancárias. Nesse sentido, a coordenação entre bancos, reguladores e autoridades investigativas torna-se essencial para mitigar esses riscos.

O crime cibernético no sector bancário é uma actividade criminosa que inclui um computador ou a internet, visando instituições financeiras para roubar dados, interromper serviços ou obter acesso não autorizado. Pode variar de simples *e-mails* de *phishing* a tentativas sofisticadas de *hacking* com métodos complexos. O motivo por trás desses ataques pode ser ganho monetário, agendas políticas, espionagem ou simplesmente causar interrupção.

No mundo digital de hoje, os bancos enfrentam uma ameaça constante de criminosos cibernéticos. Como as pessoas usam tecnologia e plataformas *online* para questões financeiras, é mais fácil para os *hackers* atingirem os bancos e seus clientes. Ataque cibernético não significa apenas perder dinheiro; também prejudica a reputação do banco, faz com que os clientes percam a confiança e quebrem as regras.

Os *hackers* continuam mudando a maneira como atacam os bancos, dificultando que os bancos acompanhem. Uma maneira comum é o *phishing*, onde eles enganam as pessoas para que compartilhem informações confidenciais, como logins. Mas agora, eles também usam métodos avançados como *ransomware* e ameaças internas para explorar as fraquezas e ou vulnerabilidades dos bancos.

Além disso, o *phishing* engana as pessoas com *e-mails*, mensagens ou sites falsos que parecem reais. É difícil de encontrar porque os *hackers* descobrem novas maneiras de passar pela segurança. Em 2019, o Capital One foi atingido, e mais de 100 milhões de informações de clientes foram roubadas. Isso mostra o quão sério e prejudiciais esses ataques podem ser[18].

[18] https://www.63saps.com. Crime Cibernetico no Sector Bancario: Estratégias para Mitigar o Impacto dos Ataques Cibernéticos. 2024. Acesso no dia 6/01/2025

Ransomware é quando *hackers* entram no sistema de um banco, bloqueiam informações e exigem dinheiro como forma de resgate, para desbloqueá-las. Não custa apenas dinheiro; ele baralha o sistema bancário e causa problemas para os clientes[19].

As ameaças internas ocorrem quando pessoas que trabalham para o banco usam informações de forma indevida de propósito, propiciando um ataque interno, e informações privadas de clientes são roubadas e usadas pelos próprios funcionários bancários, onde por exemplo, ordenam transferências bancarias para contas de pessoas conhecidas ou próximos a eles, e mais tarde os contactam para reaver os valores.

No sector bancário, seguir regras e padrões é crucial para um ambiente seguro. Os requisitos regulatórios descrevem o que os bancos devem fazer para se proteger contra ameaças, adoptando a auto-avaliação e gestão do risco e resiliência cibernética[20]. Além disso, a conformidade desempenha um papel vital em garantir que os bancos sigam essas regras e apliquem boas práticas de segurança cibernética. Não cumprir tem consequências sérias, impactando os esforços para prevenir crimes cibernéticos.

Além disso, a não conformidade não só convida a penalidades e multas, mas também enfraquece a defesa geral contra ameaças cibernéticas. Portanto, a adesão aos padrões regulatórios não é apenas uma obrigação legal, mas um factor essencial para mitigar efectivamente os riscos cibernéticos e garantir um cenário bancário resiliente.

1.2. Tipologias de Crimes Cibernéticos

Os crimes cibernéticos podem ser classificados em diversas tipologias e ou modalidades, dependendo de sua natureza e dos objectivos dos agentes maliciosos, por via disso o legislador moçambicano, optou por usar outras designações traduzidas de algumas que vamos a seguir abordar. As principais categorias incluem:

[19] https://www.63saps.com. Crime Cibernético no Sector Bancário: Estratégias para Mitigar o Impacto dos Ataques Cibernéticos. 2024. Acesso no dia 6/01/2025

[20] Cfr. Art. 5,7 e seguintes do Aviso n° 2/GBM/2024 de 15 de Março.

Phishing: O termo foi criado nos primórdios da internet, na segunda metade dos anos 1990, quando *hackers* buscavam atrair usuários para roubar suas contas hospedadas no América Online (AOL)[21].

Trata-se de uma prática em que criminosos enviam comunicações fraudulentas, como *e-mails* ou mensagens, com o objectivo de enganar as vítimas e obter informações sensíveis, como senhas e dados bancários dos usuários por meio de *links*, *e-mails*, aplicativos ou sites construídos especificamente para roubar dados, como senhas, números e cartões, entre outros dados. Muitas vezes, os criminosos se passam por alguém conhecido e confiável ou mesmo alguma empresa que tenha boa reputação a fim de atrair vítimas. Esse tipo de ataque é altamente prevalecente em Moçambique, especialmente com o crescimento do uso de aplicativos de pagamento digital[22]. Esta tipologia, quando traduzido e de acordo com descrição aqui apresentada, corresponde ao uso abusivo de dispositivos estabelecido no art. 339 do CP.

Malware: Refere-se a *softwares* maliciosos projectados para danificar ou interromper sistemas. Temos como exemplos que incluem vírus, *worms* e *ransomware*, que têm sido utilizados para sequestrar dados de bancos e exigir resgates em troca de sua restauração[23]. Corresponde a esta tipologia no nosso ordenamento jurídico, o disposto no art. 338 do CP, pois trata-se de interferência em sistemas.

Ataques DDoS: A sigla vem do inglês "Distributed Denial of Service" que, em português, significa ataques de Negação de Serviço Distribuída (DDoS) têm como objetivo sobrecarregar sistemas, tornando-os indisponíveis para os usuários legítimos. Um outro ataque próximo do DDoS é o DoS, no qual apenas um criminoso, por meio de um único computador, ataca várias máquinas. Dessa forma, "derruba" redes, servidores ou computadores comuns que contenham baixas especificações técnicas.

No DDoS, um computador pode comandar diversos outros (até milhões) e assim coordenar um ataque em massa. O aparelho principal, chamado de mestre, "escraviza" outras máquinas que, obrigatoriamente, acessam o que o mestre pede.

---

[21] https://fia.com.br. Crimes cibernéticos: o que são, tipos e como detectar. 2021. Acesso no dia 7/01/2025

[22] RUDRA, Ahona. Cibersegurança no Sector Bancário: Principais ameaças e melhores formas de as evitar. 2023. https://powerdmarc.com.pt. Acesso no dia 10/01/2025

[23] *Ibidem*

Como os servidores de internet têm uma quantidade limitada de acessos, o alto número de computadores na mesma direcção (no mesmo servidor) pode fazer com que determinado *website* fique completamente travado[24]. Em comparação com o que descreve, corresponde também ao uso abusivo de dispositivos conforme o art.339 do CP.

Bancos em Moçambique relataram incidentes desse tipo que interromperam operações por horas, causando prejuízos significativos[25].

Hacking: este crime é o acesso ilegal, a interceptação ou obtenção dos dados do computador: Refere-se a actos que envolvam o acesso a dados de computador sem autorização ou justificação, incluindo obtenção de dados durante uma transmissão que não se destinam para que ela seja pública, bem como a obtenção de dados de computador (por exemplo, copiá-los) sem autorização. O principal objectivo é de roubar informações, desactivar operações ou desviar fundos. Conforme o estabelecido no art. 337 do CP.

As instituições bancárias moçambicanas, têm sido alvo frequente de *hackers*, como demonstrado nos relatórios anuais do Banco de Moçambique[26].

Roubo de Identidade: são crimes informáticos relacionados à identidade, que refere-se a actos que envolvem a transferência, posse ou uso de um meio de identificar outra pessoa armazenada em dados de computador, sem o direito de fazê-lo, com a intenção de cometer, assistir ou incitar, ou em relação a qualquer actividade ilegal que constitua um crime, conforme dispõe o art. 336 do CP.

Estudos indicam que o roubo de identidade está em ascensão devido à falta de consciencialização sobre segurança digital em Moçambique[27].

Estas tipologias e ou modalidades de ataques cibernéticos constituem fraudes bancárias relativas aos instrumentos de pagamento electrónico e são um mal que abrange toda a sociedade, afectando bens jurídicos diversos, particularmente os financeiros, o que gera insegurança aos clientes, instabilidade para os bancos, sendo, por isso, punidas por lei. Cada

[24] RUDRA, Ahona. Op Cit.

[25] *Ibidem*

[26] Relatório do Banco de Moçambique (2022) pg:15

[27] *Ibidem*, pg:15

uma dessas tipologias representa um desafio específico para as instituições financeiras, exigindo abordagens diversificadas para mitigação e resposta. A compreensão dessas categorias é essencial para o desenvolvimento de estratégias de segurança mais eficazes.

Os crimes cibernéticos tendo emergido como um dos principais desafios no cenário global, especialmente no sector financeiro, devido à crescente dependência da tecnologia para a realização de transacções económicas. Esses crimes abrangem uma gama diversificada de práticas ilícitas, como fraudes electrónicas, roubo de identidade, acesso não autorizado a sistemas e a manipulação de dados sensíveis[28]. A digitalização do sector bancário, embora tenha proporcionado benefícios como agilidade e acessibilidade, ampliou a superfície de exposição das instituições financeiras às ameaças cibernéticas.

Em Moçambique, a expansão do uso de tecnologias digitais no sistema bancário não foi acompanhada, de maneira proporcional, pela implementação de medidas robustas de segurança cibernética. A falta de infra-estrutura tecnológica avançada e a carência de políticas de ciber-segurança eficazes tornam o sector bancário moçambicano vulnerável a ataques cibernéticos, com impactos negativos tanto para os bancos quanto para os seus clientes[29].

1.3 A Segurança Cibernética

À medida que o mundo avança rumo ao acesso universal à Internet, pode ser que os conceitos de cibercrime tenham que operar em vários níveis: específicos e detalhados no caso da definição de alguns actos individuais de cibercrime, mas suficientemente amplos para assegurar que poderes de investigação e mecanismos de cooperação internacional possam ser aplicados, com salvaguardas efectivas, devido a constante migração do crime no mundo físico para suas variantes *on-line*.

A segurança cibernética está preocupada em tornar o ciberespaço seguro contra ameaças, ou seja, ameaças cibernéticas. A noção de "ameaça cibernética" é bastante vaga e implica o uso malicioso da tecnologia da informação e comunicação (TIC) como um alvo ou como uma ferramenta por uma ampla gama de actores malévolos. A segurança cibernética é muitas vezes

[28] GONDWE, Gregory. Op Cit. Pg: 57

[29] MATAVELE, Fernando. Op Cit. Pg: 31.

confundida com a segurança nacional, enquanto a segurança nacional, pode muitas vezes estar implicada em alguns casos de segurança cibernética. A segurança cibernética como um termo refere-se apenas à segurança de redes e sistemas – computadores, electrónicos e dispositivos auxiliares. Questões típicas de segurança cibernética incluem: confidencialidade da informação; e integridade de sistemas e capacidade de sobrevivência de redes (CIS). O principal objectivo da segurança cibernética inclui: protecção do sistema de redes contra acesso não autorizado e alteração de dados a partir de dentro; e defesa contra intrusão de fora[30].

Conforme comumente usado, o termo "segurança cibernética" refere-se a três coisas:

- Um conjunto de actividades e outras medidas, técnicas e não técnicas, destinadas a proteger computadores, redes de computadores, dispositivos de *hardware* e software relacionados e as informações que contêm e comunicam, incluindo software e dados, bem como outros elementos do ciberespaço, de todas as ameaças, incluindo ameaças à segurança nacional;
- O grau de protecção resultante da aplicação dessas actividades e medidas;
- O campo associado de actuação profissional, incluindo pesquisa e análise, visando à implementação e a essas actividades e melhorando sua qualidade.

A segurança cibernética é, portanto, mais do que apenas segurança da informação ou segurança de dados, mas está intimamente relacionada a esses dois campos, porque a segurança da informação está no cerne da questão. Segurança da informação refere-se a todos os aspectos da protecção de informações. Na maioria das vezes, esses aspectos são classificados em três categorias: confidencialidade, integridade e disponibilidade de informações. "Confidencialidade" refere-se à protecção de informações de divulgação para partes não autenticadas, enquanto "integridade" refere-se à protecção de informações contra alterações não autorizadas. "Disponibilidade" significa que as informações devem estar disponíveis para as partes autorizadas quando solicitadas. Às vezes, "prestação de contas", o requisito de que as acções de uma entidade sejam exclusivamente rastreáveis a essa entidade é adicionado à lista.

[30] TAVARES, Thiago Daniel Ribeiro; at all. Crimes informaticos e Ciberneticos: Ciência Jurídica. Vol 28. Ed 133. 2024. Pg: 9-12.

O domínio das tipologias de rede tem implicações para a forma das políticas de protecção e, subsequentemente, para determinar os esforços, metas, estratégias e instrumentos de protecção apropriados para solução de problemas:

- Ciber-segurança como uma questão de Tecnologia da Informação: A segurança cibernética pode ser abordada como uma questão de segurança de TI ou garantia da informação, com um forte foco na segurança da Internet. As políticas visam, assim, combater as ameaças à infra-estrutura de informações por meios técnicos, como *firewalls*, software antivírus ou software de detecção de intromissões. As principais ameaças percebidas variam de acidentes, falhas de sistema, programação incorrecta e falhas humanas em ataques de *hackers*.
- Ciber-segurança como uma questão económica: A segurança cibernética é relevante para a continuidade do negócio e, especialmente, para o e-business, que requer acesso permanente a infra-estruturas de TIC e processos de negócios permanentemente disponíveis para garantir um desempenho comercial satisfatório. Os principais actores são representantes do sector privado que incluem os bancos. As principais ameaças são vírus e *worms*, falhas humanas, mas também ataques de *hackers* de todos os tipos e actos de *cibercrime*.
- Ciber-segurança como uma questão de aplicação da lei: A segurança cibernética é vista como relevante para o cibercrime. O cibercrime é um termo muito amplo, com vários significados, e a definição pode incluir desde crimes habilitados por tecnologia até crimes cometidos contra computadores individuais. Os principais actores são órgãos de investigação criminal. As principais ameaças são actos de criminalidade informática, mas também terrorismo cibernético.

A segurança cibernética é uma questão de segurança nacional: a sociedade como um todo e seus valores centrais estão ameaçados, devido à sua dependência das TIC. A acção contra a ameaça é voltada para vários níveis (técnico, legislativo, organizacional ou internacional). Os principais actores são especialistas em segurança. As principais ameaças são terroristas, mas também ameaças de guerra de informação de outros estados.

1.4 A prevenção do crime cibernético.

A Prevenção ao crime refere-se a estratégias e medidas que visam reduzir o risco da ocorrência de crimes e seus potenciais efeitos nocivos sobre as pessoas e a sociedade, através de intervenções que influenciam as múltiplas causas do crime. As Directrizes das Nações Unidas para a Prevenção do Crime destacam que a liderança do governo tem um papel importante na prevenção do crime, em combinação com a cooperação e alianças entre ministérios e entre autoridades, organizações comunitárias, organizações não-governamentais, sector empresarial e indivíduos. As boas práticas de prevenção do crime começam com princípios básicos (como liderança, cooperação e estado de direito), sugerem formas de organização (como planos de prevenção ao crime) e derivam na implementação de métodos (como o desenvolvimento de uma sólida base de conhecimento) e abordagens (incluindo a redução de oportunidades para o crime e o endurecimento das penas)[31].

O crime cibernético apresenta desafios particulares em termos de prevenção. Isso inclui a crescente omnipresença e acessibilidade dos dispositivos *online*, que resultam em um grande número de vítimas em potencial; a disposição comparativa das pessoas para assumir o comportamento 'arriscado' *online*; a possibilidade de anonimato e uso de técnicas de ocultação pelos perpetradores; a natureza transnacional de muitos actos de cibercrime; e o ritmo acelerado da inovação criminal. Cada um desses desafios tem implicações para a organização, métodos e abordagens adoptadas para a prevenção do cibercrime[32].

As estruturas organizacionais, por exemplo, devem reflectir a necessidade de cooperação internacional e regional na prevenção do cibercrime. Os métodos devem assegurar uma imagem constantemente actualizada das ameaças cibernéticas, e as abordagens terão que envolver uma série de actores – particularmente as organizações do sector bancário que possuem e operam a infra-estrutura e os serviços de Internet.

[31] TAVARES, Thiago Daniel Ribeiro; at all. Op Cit. Pg: 14

[32] *Ibdem*

CAPÍTULO II: ANÁLISE JURÍDICA DAS LEIS RELEVANTES NO CONTEXTO DA RESPONSABILIDADE LEGAL DOS BANCOS EM CRIMES CIBERNÉTICOS

A actuação dos bancos na prevenção e investigação de crimes cibernéticos em Moçambique está fundamentada em diversos instrumentos legais, embora estas legislações sejam essenciais, apresentam lacunas que podem comprometer sua eficácia no enfrentamento dos desafios impostos pelos crimes cibernéticos.

2.1. A Lei das Transacções Electrónicas (Lei n.º 3/2017 de 9 de Janeiro)

A Lei n.º 3/2017, de 9 de Janeiro, constitui um instrumento jurídico de Moçambique voltado para a prevenção e repressão de crimes cibernéticos. A legislação estabelece directrizes específicas para proteger sistemas informáticos e regular o uso responsável das tecnologias digitais. Além disso, a lei define responsabilidades tanto para usuários quanto para instituições que operam em ambientes digitais, incluindo bancos conforme artigo 13 e seguintes.

A legislação desempenha um papel crucial no enfrentamento dessas ameaças, ao impor responsabilidades legais às instituições financeiras para a adopção de medidas preventivas e a colaboração na investigação de crimes cibernéticos. No contexto moçambicano, a Lei n.º 3/2017, de 9 de Janeiro, conhecida como Lei das transacções electrónicas, esta lei prevê, entre outras disposições, a obrigatoriedade de protecção dos sistemas informáticos e a responsabilização das entidades que operam em ambientes digitais, incluindo os bancos conforme os artigos 63 a 70[33].

No entanto, estudiosos apontam que, embora a legislação forneça directrizes importantes, sua implementação enfrenta desafios significativos. De acordo com Januário e Chongo[34], destacam que a ausência de um sistema nacional de ciber-segurança devidamente estruturado e a limitada capacitação técnica das instituições bancárias são entraves para a eficácia das medidas legais. Além disso, as práticas criminosas em ambiente cibernético evoluem rapidamente, exigindo das instituições financeiras uma constante actualização de suas estratégias de defesa.

[33] Cfm. Lei 3/2017 de 9 de Janeiro.

[34] JANUÁRIO, T, & CHONGO, D. Op. Cit. Pg: 48.

Por via disso, a eficácia desta lei enfrenta desafios práticos. Januário e Chongo destacam que, embora a legislação imponha obrigações de protecção e reporte às instituições financeiras, muitos bancos enfrentam dificuldades em cumprir esses requisitos devido à ausência de capacidades técnicas, recursos financeiros limitados e uma supervisão estatal insuficiente[35].

Outro aspecto relevante é que a lei nos artigos 66 a 70, prevê infracções de natureza contravencional e as respectivas penalidades, mas no que diz respeito as infracções criminais nos remetem ao Código Penal, isto é para crimes informáticos, mas não detalha suficientemente as directrizes operacionais para a implementação de medidas de segurança por parte das instituições financeiras. Essa lacuna contribui para interpretações divergentes e para a falta de uniformidade nas práticas preventivas adoptadas pelos bancos no país.

Além da Lei das transacções electrónicas, a Lei n.º 14/2023, de 28 de Agosto, sobre o Branqueamento de Capitais e Financiamento ao Terrorismo, também desempenha um papel fundamental na regulação do sector financeiro. O n°1 b) do artigo 6, desta lei define como crime de branqueamento, a ocultação ou dissimulação da origem de bens provenientes de actividades ilícitas, incluindo aquelas praticadas no ambiente cibernético. Já o artigo 11 obriga as instituições financeiras a adoptarem medidas de *due diligence*, como identificação de clientes e monitoramento de transacções suspeitas.

Esta Lei impõe às instituições financeiras o dever de identificar, monitorar e relatar transacções suspeitas, bem como de implementar medidas preventivas para evitar o uso de seus sistemas por criminosos, conforme dispõe o art. 15, que exige que os bancos adoptem procedimentos rigorosos de identificação de clientes, como um elemento crucial na prevenção de fraudes cibernéticas e lavagem de dinheiro.

O artigo 12 e seguintes são relevantes para o tema em análise, pois exigem que as instituições bancárias implementem mecanismos de controlo interno para detectar e prevenir transações relacionadas ao financiamento do terrorismo. Ainda que o artigo 38 aborda a questão das transações electrónicas e ao mesmo tempo reforça a necessidade de integrar medidas de cibersegurança aos procedimentos de prevenção de crimes financeiros.

O artigo 44 estabelece a obrigação de reportar actividades suspeitas ao Gabinete de Informação Financeira de Moçambique (GIFiM), sendo esta uma das vias e ou formas de os bancos

[35] Januário, T e Chongo, D. Op Cit. Pg: 48.

prestarem colaboração com outras instituições, contribuindo para a detecção e investigação de crimes cibernéticos.

Gondwe[36] destaca que "o GIFiM desempenha um papel central na coordenação de esforços entre instituições financeiras e autoridades no combate ao branqueamento de capitais". Enquanto, Matavele observa que "a exigência de procedimentos de identificação de clientes é uma medida essencial para prevenir fraudes digitais" [37].

Por outro lado, a eficácia das medidas legais em Moçambique também depende da capacidade de colaboração entre os bancos e as autoridades públicas responsáveis pela investigação e repressão de crimes cibernéticos. A falta de integração entre os diferentes actores do sistema jurídico e financeiro é frequentemente apontada como um obstáculo para a mitigação dessas ameaças[38].

2.2. Lei de Supervisão Bancária (Lei n.º 20/2020, de 31 de Dezembro)

A Lei de Supervisão Bancária estabelece o regime jurídico para supervisão prudencial das instituições financeiras, atribuindo ao Banco de Moçambique poderes amplos para monitorar, regular e sancionar práticas inadequadas no sector bancário. Essa lei impõe aos bancos a obrigação de adoptar práticas de gestão de riscos, incluindo os riscos operacionais relacionados a ataques cibernéticos.

2.2.1. Pontos Positivos

- Os artigos 90 e 106 exigem que os bancos adoptem sistemas robustos de gestão de riscos, incluindo mecanismos que abordem os riscos tecnológicos e cibernéticos.
- O Banco de Moçambique, no exercício de suas funções de regulador, pode impor sanções às instituições que não implementem medidas de segurança cibernética adequadas (artigo 58). A inclusão de requisitos de gestão de risco tecnológico é um

[36] GONDWE, Gregory. Cybersecurity and Financial Institutions in Africa. 2020; Op Cit. Pg: 78.

[37] MATAVELE, Fernando. Criminalidade cibernética em Moçambique. 2009. Op Cit. Pg: 53.

[38] *Ibidem*. Pg: 37.

avanço necessário no combate aos crimes cibernéticos, dada a crescente dependência de transacções digitais no sector bancário[39].

2.2.2. Lacunas Jurídicas

Apesar de suas disposições, a Lei não detalha requisitos específicos sobre ciber-segurança e protecção de dados. A ausência de padrões mínimos para sistemas de segurança cibernética deixa espaço para interpretações divergentes, comprometendo a uniformidade das práticas entre as instituições financeiras. Destaca-se que "a falta de regulamentação específica sobre segurança cibernética o que, enfraquece a capacidade das instituições financeiras de responder de forma eficiente às ameaças digitais" [40].

[39] JANUÁRIO, T e CHONGO, D. Segurança cibernética no setor financeiro: Desafios e oportunidades em Moçambique. Op Cit. Pg: 58.

[40] MATAVELE, Fernando. Op Cit. Pg: 51.

CAPÍTULO III: RESPONSABILIDADE LEGAL DOS BANCOS NA PREVENÇÃO DE CRIMES CIBERNÉTICOS

3.1. Definição da Responsabilidade Legal

A responsabilidade legal refere-se à obrigação de indivíduos ou entidades de responder pelos actos que realizam, de acordo com as leis vigentes. No contexto dos bancos, isso significa a obrigação legal das instituições financeiras de adoptar medidas preventivas e correctivas em relação aos crimes cibernéticos, garantindo a segurança dos dados dos clientes, a integridade das transacções e a conformidade com as normas estabelecidas pelas autoridades competentes.

A responsabilidade legal dos bancos em relação aos crimes cibernéticos é multifacetada. Ela inclui a obrigação de prevenir ataques, proteger os dados financeiros e pessoais de seus clientes, além de cooperar com as autoridades para investigar e punir os responsáveis por tais crimes. Em termos jurídicos, os bancos devem adoptar uma postura proactiva para mitigar riscos relacionados à ciber-segurança, conforme determinado pelas legislações nacionais e internacionais aplicáveis.

3.1.1. A responsabilidade dos Bancos

Os bancos, enquanto guardiões de informações financeiras e pessoais de seus clientes, possuem responsabilidades legais específicas no que diz respeito à prevenção de crimes cibernéticos. Essas responsabilidades estão intimamente ligadas ao princípio da diligência, que exige a adopção de medidas adequadas para proteger os dados e prevenir fraudes[41].

No contexto moçambicano, a legislação obriga as instituições financeiras a implementarem sistemas de segurança digital que minimizem os riscos de ataques cibernéticos. No entanto, estudos indicam que a maioria dos bancos no país ainda está longe de alcançar padrões internacionais de ciber-segurança. Conforme Matavele ressalta que, a ausência de investimentos substanciais em tecnologia de ponta e a falta de programas de consciencialização para funcionários e clientes são entraves significativos[42].

Verifica-se ainda que, há uma crescente demanda por auditorias regulares de segurança cibernética, tanto para identificar vulnerabilidades quanto para garantir conformidade com as

[41] GONDWE, Gregory. Cybersecurity and Financial Institutions in Africa. Op Cit. Pg: 39.

[42] MATAVELE, Fernando. Criminalidade cibernética em Moçambique. Op Cit. Pg: 35.

normas legais. Contudo, a falta de recursos financeiros e técnicos limita a capacidade de muitas instituições bancárias de implementar essas práticas de forma eficaz.

Além disso, a legislação sobre branqueamento de capitais e financiamento ao terrorismo exige que os bancos sejam proactivos na identificação de transacções suspeitas e na cooperação com autoridades investigativas. O art. 44 da Lei n.º 14/2013, estabelece a comunicação obrigatória de transacções que levantem suspeitas de irregularidades. Essa exigência coloca os bancos em uma posição central no combate a crimes cibernéticos associados a actividades financeiras ilícitas.

3.1.2 O Risco associado a actividade bancária

Quando ocorre uma fraude bancária electrónica, surge de imediato a questão de determinar o responsável pelos prejuízos incorridos pelos clientes. Neste contexto, é importante abordar a responsabilidade dos bancos por risco, nos casos de ocorrência de fraudes electrónicas.

No que respeita ao risco associado a actividade bancária, à luz do artigo 1.2.1 das Directrizes de Gestão de Risco (Aprovadas pelo Aviso n° 4/GBM/2013 de 18 de Setembro), a actividade bancária comporta, no nosso país, 9 categorias de riscos associados, sendo os mais relevantes, designadamente, o Risco de Crédito, Risco de Liquidez, Risco de Taxa de Juro, Risco de Taxa de Câmbio, Risco Operacional, Risco Estratégico, Risco de Reputação, Risco de *Compliance,* e Risco de Tecnologias de Informação. Para complementar o quadro vigente com a componente de Risco Cibernético, o Banco de Moçambique desenvolveu as Directrizes de Gestão do Risco Cibernético e o Quadro de Supervisão do Risco Cibernético[43].

No contexto de riscos, os bancos são obrigados, no exercício das suas actividades, a desenvolver Programas de Gestão de Risco (PGR) detalhados, ajustados à dimensão e complexidade das suas actividades, compostos fundamentalmente por 4 processos chaves designadamente: Identificação, Mensuração, Controlo e Acompanhamento de risco.

Compete ao órgão da administração aprovar e rever as estratégias e políticas relativas a assunção, gestão, controle e redução de riscos que o banco possa sujeitar-se, alocar recursos de gestão de riscos, e participar activamente na utilização de notações de risco externo e de modelos internos relacionados a esses riscos, conforme resulta do artigo 90 da Lei n° 20/2020 de 31 de Dezembro. Ou seja, os bancos possuem sistemas de acompanhamento e gestão de

[43] COSSA, Nocita. Responsabilidade dos Bancos no Âmbito das Fraudes Electronicas. 2022. https://www.asg.co.mz.

risco que proporcionam aos administradores e à gestão de topo, um entendimento claro das exposições ao risco.

Outrossim, as instituições financeiras estão obrigadas a estabelecer uma área funcional responsável pela fiscalização da gestão dos riscos intrínsecos nas suas operações, responsável por assegurar a existência de processos eficazes para identificar riscos presentes e futuros, desenvolver sistemas de medição e avaliação de riscos, estabelecer políticas, procedimentos, práticas e outros mecanismos de gestão, acompanhar as posições tomadas, tendo como base os limites de tolerância aprovados, reportar os resultados de monitorização de riscos ao órgão de administração e gestão de topo.

Através da Integração da Gestão de Riscos, os bancos captam inter-relações existentes entre diferentes tipos de riscos e são capazes de testar a capacidade de resposta de contingência para assegurar que eventos razoavelmente prováveis de ocorrer e de produzir impactos adversos à instituição possam ser abarcados.

Portanto, na disponibilização e comercialização de produtos e serviços bancários, execução de operações de pagamento como transferência de fundos, consulta de saldo, extracto da conta bancária, execução de débitos, entre outras operações necessárias para gestão da conta bancária do cliente, os bancos desenvolvem Programas de Gestão de Risco (PGR), que conferem aos próprios bancos, a capacidade de identificar e mensurar os riscos existentes e os que podem surgir, bem como determinar o seu impacto na instituição e controlar o nível de riscos a que estão expostos, comunicar os limites de risco, políticas, normas e procedimentos que definem responsabilidade e linhas de autoridade[44].

3.1.3 Risco de Tecnologia de Informação (TI)

O Risco Associado às Tecnologias de Informação está ligado ao tipo de serviço disponibilizado pelos bancos. E os serviços baseados na internet podem ser classificados em serviços de informação, de troca interactiva de informação e transaccionais (art. 2.2.3 das Directrizes de Gestão de Risco, Aviso nº 04/GBM/13 de 24 de Maio).

Os serviços transaccionais, de *Internet Banking*, permitem ao cliente executar transacções *online* como transferências de fundos, pagamentos de contas, entre outras transacções financeiras e constituem a categoria de risco mais elevado, porque requerem controlo e segurança mais fortes, conforme resulta do artigo 2.2.6. das directrizes.

[44] COSSA, Nocita. Responsabilidade dos Bancos no Âmbito das Fraudes Electronicas. 2022. https://www.asg.co.mz.

Portanto, na disponibilização de produtos e serviços electrónicos, requer-se controlo e segurança mais elevados, sistemas operativos robustos contra ameaças, vulnerabilidades e exposições presentes na configuração do sistema e em serviços como redes internas e externas, *hardware, softwares*, aplicações, *interfaces* de sistemas, operações humanas com a motivação e capacidade para efectuar ataques, entre outras, pois uma vez realizadas (as transacções) são normalmente irrevogáveis.

Ou seja, o banco tem a obrigação de garantir o controlo e segurança mais elevados na confidencialidade de dados, integridade de sistemas, disponibilidade de sistemas, autenticidade do cliente, transacção e protecção ao cliente[45].

O risco cibernético coloca desafios aos tradicionais Programas de Gestão de Risco Operacional devido a natureza persistente da presença de um adversário activo e algumas vezes sofisticado em termos de ciberataques. Ao contrário de outras fontes, os ataques maliciosos são normalmente difíceis de identificar ou erradicar completamente e a dimensão dos danos difíceis de determinar.

Ao abrigo do artigo 3.1 do Quadro de Supervisão do Risco Cibernético, constituem riscos intrínsecos à actividade bancária, os provedores de serviços de internet (ISP), as ligações com entidades externas, o volume de dispositivos de rede, a extensão dos serviços na nuvem, utilização de dispositivos pessoais, alteração do pessoal de segurança, canais bancários dependendo da natureza específica de produtos ou serviços oferecidos.

Pelo que, reconhecendo a natureza dinâmica das ciber-ameaças, e necessidade de adoptar métodos evolutivos para mitigar essas ameaças, o Banco de Moçambique orienta que as Instituições de Crédito e Sociedades Financeiras (ICSF) devem ter políticas de segurança física e de informação abrangentes que façam face às potenciais vulnerabilidades e ameaças e, na prática, no contexto da gestão do risco cibernético, os bancos devem implementar controlos de tecnologias de informação robustos e consistentemente demonstrar ambientes de controlo efectivos.

A responsabilidade pelo risco é a situação na qual uma pessoa fica adstrita a uma obrigação de ressarcir outra, por um determinado dano, independentemente de, ilicitamente e com culpa, o ter originado. A responsabilidade pelo risco também é designada por responsabilidade objectiva, imputação objectiva ou imputação sem culpa. E são pressupostos da

[45] COSSA, Nocita. Responsabilidade dos Bancos no Âmbito das Fraudes Electronicas. 2022. https://www.asg.co.mz

responsabilidade pelo risco o facto, o nexo de imputação objectiva ou risco, o dano e o nexo de causalidade[46].

A esfera de risco pode ser estabelecida por diversas concepções que por vezes cumulam entre si, designadamente: a concepção de risco criado, segundo a qual, cada pessoa que cria uma situação de perigo deve responder pelos riscos que resultem dessa situação; a concepção de risco proveito segundo a qual, a pessoa deve responder pelos danos resultantes das actividades de que tira proveito; e a concepção de risco autoridade, segundo a qual, a pessoa deve responder pelos danos resultantes das actividades que tem sob controlo.

Nos termos da responsabilidade civil pelo risco, existindo o dano, o fornecedor do serviço deve ser responsabilizado a repará-lo, independentemente de culpa. Basta que se verifique o nexo de imputação objectiva ou o risco. Ou seja, no lugar da "culpa", toma-se em atenção o factor "risco criado", "risco-proveito" ou "risco da actividade empresarial" que se funda no princípio de que é reparável o dano causado a terceiro em consequência do exercício da actividade empresarial lucrativa realizada em benefício do responsável.

3.2. Responsabilidade Civil dos Bancos na Prevenção e investigação do Cibercrime

3.2.1 Conceito de Responsabilidade Civil

Quando a lei impõe ao autor de certos factos ou ao beneficiário de certa actividade a obrigação de reparar os danos causados a outrem, por esses factos ou por essa actividade, depara-se-nos a figura da responsabilidade civil. A responsabilidade civil actua, portanto através do surgimento da obrigação de indemnização, esta visa colocar a vítima na situação em que estaria sem a ocorrência do facto danoso[47].

De acordo com Mota Pinto, a responsabilidade civil consiste, por conseguinte na necessidade imposta pela lei a quem causa prejuízos a outrem de colocar o ofendido na situação em que estaria sem a lesão (arts. 483 e 562 do CC). Esta reconstituição da situação em que o lesado estaria sem a infracção deve em princípio ter lugar mediante uma reconstituição natural (restauração natural, restituição ou execução especifica)[48].

---

[46] PINTO, Carlos Alberto da Mota, Teoria Geral do Direito Civil. 4ª Ed, Coimbra Editora. 2012. Pg: 128.

[47] Idem

[48] Idem

A indemnização em dinheiro cobre os danos patrimoniais sofridos pelo lesado, isto é, os prejuízos susceptíveis de avaliação em dinheiro. Além da existência do dano e de uma ligação causal entre o facto gerador de responsabilidade e o prejuízo, devem verificar-se outros pressupostos para o surgimento da responsabilidade civil, sendo necessário em princípio, que o facto seja ilícito, isto é, violador de direitos subjectivos ou interesses alheios tutelados por uma disposição legal e culposo, ou seja, passível de uma censura ético-jurídica ao sujeito actuante.

A culpa traduzida numa reprovação ou censura da conduta desrespeitadora dos interesses tutelados pelo direito, pode resultar da existência de uma intenção de causar dano violando uma proibição (dolo) ou da omissão dos deveres de cuidado, diligência ou perícia exigíveis para evitar o dano (negligência ou mera culpa). Embora a responsabilidade civil deva conduzir à reconstituição da situação que existiria se não se tivesse produzido o evento que obriga à reparação (art. 562 do CC), a nossa lei admite uma limitação equitativa de indemnização quando a responsabilidade se funde em mera culpa (art. 494 do CC).

A responsabilidade civil dos bancos em relação aos crimes cibernéticos decorre da necessidade de garantir a protecção dos bens e informações de seus clientes, prevenindo possíveis danos causados por ataques cibernéticos. Essa responsabilidade está ancorada nos princípios gerais de diligência e segurança, com base em legislações específicas, como a Lei Transacções Electrónicas (Lei n.º 3/2017) e a Lei de Branqueamento de Capitais (Lei n.º 14/2013). A negligência na adopção de medidas preventivas pode gerar a responsabilização das instituições financeiras pelos danos materiais e imateriais sofridos por seus clientes. Destaca-se ainda que "os bancos em Moçambique enfrentam desafios críticos no cumprimento de obrigações legais de segurança cibernética devido à escassez de infra-estrutura e recursos técnicos" [49].

Dada esta situação e tratando-se de instituições de natureza financeira, os seus clientes aderem os seus serviços por via de um contracto de prestação de serviços bancários, o que acarreta riscos de maior proporção por causa do uso das TICs, para a transferência de valores monetários.

Ao abrigo do artigo 7 n° 2 do Aviso n° 2/GBM/2014 de 31 de Dezembro, que aprova o Regulamento sobre Procedimentos de Disponibilização de Produtos e Serviços de Pagamento

[49] MATAVELE, Fernando. Criminalidade cibernética em Moçambique. Op Cit. Pg: 32.

Electrónico, a responsabilidade pela disponibilização de um produto ou serviço de pagamento electrónico recai sobre a Instituição de Crédito ou Sociedade Financeira ou prestador de serviços de pagamento nos termos da legislação aplicável. Ou seja, os bancos são responsáveis pelos produtos e serviços que comercializam ao público.

A par disso, os n^{os} 4 e 5, do artigo 14 da Lei n° 22/2009 de 28 de Setembro – Lei de Defesa do Consumidor, estabelece que o consumidor tem direito à indemnização pelos danos patrimoniais e não patrimoniais resultantes do fornecimento de bens ou prestações de serviços defeituosos[50].

Os serviços são considerados defeituosos quando não oferecem a segurança que o consumidor dele pode esperar tomando em consideração as circunstâncias relevantes, nomeadamente o modo do seu funcionamento, o resultado e os riscos que razoavelmente dele se esperam e a época em que foi fornecido (n° 8 do artigo 14 da Lei n° 22/2009 de 28 de Setembro).

E, o fornecedor de serviços responde, independentemente da existência de culpa, pela reparação de danos causados ao consumidor, por defeitos relativos à prestação de serviços, bem como por informações insuficientes sobre a sua fruição e risco – artigo 9 n° 2 do Decreto n° 27/2016 de 18 de Julho, que aprova o Regulamento da Lei de Defesa do Consumidor.

Ou seja, no âmbito das relações de consumo que os bancos estabelecem com os clientes, reconhecendo a vulnerabilidade do consumidor e com vista a garantir a segurança da relação de consumo e direitos daí advenientes, nos termos do Regulamento sobre Procedimentos de Disponibilização de Produtos de Pagamento Electrónico, bem como o Regulamento da Lei de Defesa do Consumidor, a regra é de que os bancos são responsáveis pelos produtos que comercializam e respondem, independentemente da culpa, pelos danos causados aos consumidores[51].

Note-se que, os serviços transaccionais, serviços electrónicos e, ou serviços de *Internet Banking* constituem, na actividade bancária, a categoria de risco mais elevado, razão pela qual a sua disponibilização requer controlo e segurança mais elevados, sistemas operativos robustos contra ameaças, vulnerabilidades e exposições presentes na configuração do sistema e serviços como redes internas e externas, *hardware*, *softwares*, aplicações, interfaces de sistemas, operações humanas com a motivação e capacidade para efectuar ataques, entre outras.

[50] Cfm. lei n° 22/2009 de 28 de Setembro.

[51] COSSA, Nocita. Op Cit.

Ao abrigo do artigo 2.9.5 das Directrizes de Gestão de Risco, aprovadas pelo Aviso n° 4/GBM/2013 de 18 de Setembro, na eventualidade de ocorrência de falhas de segurança de acesso e realização de transacções fraudulentas a partir de contas *online* de clientes, os bancos devem explicar em seus *websites* que processos serão evocados para resolver o problema e disputa, assim como as condições e circunstâncias nas quais as perdas ou estragos resultantes serão imputados à instituição ou ao cliente.

Ademais, as tecnologias de criptografia desempenham um papel importante na garantia da confidencialidade, autenticidade e integridade, cujo objectivo é proteger a confidencialidade dos dados das contas dos clientes e dos detalhes das transacções, assim como melhorar a confiança na *internet banking* combatendo ataques e várias formas de fraudes através da internet, pelo que, no âmbito da mitigação e controlo de riscos, incumbe aos bancos provar que foram implementadas todas medidas de segurança na confidencialidade de dados e integridade de sistemas.

Mais ainda, os clientes devem estar informados de forma clara e precisa sobre os seus direitos, obrigações e responsabilidades e os do banco em matéria de transacções *online*, particularmente problemas que possam surgir de erros de processamento, e falhas de segurança, informações escritas, pelo que, no âmbito do dever de protecção ao cliente, incumbe aos bancos desenvolver técnicas e meios humanos para proporcionar condições apropriadas de qualidade e eficiência.

A maioria dos produtos e serviços fornecidos pelos bancos oferecem um nível de risco elevado, incluindo aqueles disponibilizados às outras instituições, por isso, os bancos têm o dever de implementar medidas para captura e análise de comportamentos anómalos de pessoas com acesso aos seus sistemas, pois, os próprios bancos podem se tornar canais de propagação de ciberataques, através de funcionários de má-fé ou descuidados que abrem canais para potenciais exposições. Nesse contexto, incumbe igualmente aos bancos a capacidade para assistir na condução ou execução de investigações forenses de incidentes cibernéticos e desenhar controlos protectivos e detecção para facilitar o processo investigativo, estabelecer políticas de registo nos sistemas de registo que incluem os tipos de registos de sistema a serem mantidos e os respectivos períodos de retenção, tomar os passos apropriados para que as investigações possam ser efectuadas após ocorrência do evento através da preservação dos registos dos sistemas e evidências necessárias.

Pelo que, na ocorrência de fraude bancária, verificando-se preenchidos os pressupostos da responsabilidade civil pelo risco, ao abrigo do artigo 499º do Código Civil (CC), designadamente, o facto, o nexo de imputação objectiva, o dano e o nexo de causalidade, os bancos respondem, independentemente da culpa, pela reparação de danos causados ao consumidor, por defeitos relativos à prestação de serviços, bem como por informações insuficientes sobre a sua fruição e risco.

3.2.2. Limites à responsabilidade dos bancos.

Ao abrigo do artigo 33° do Código de Conduta Bancária, nenhuma responsabilidade poderá ser atribuída aos bancos pelos prejuízos que vierem a resultar da acção fraudulenta dos clientes.

Ao abrigo do artigo 9 n° 3 da Lei de Defesa do Consumidor, o fornecedor de serviço está isento de responsabilidade quando, entre outros, prove: a) que tendo prestado o serviço, o defeito era inexistente; b) que a culpa é exclusiva do consumidor ou de terceiro[52].

Ora, a culpa consiste num juízo de censura ao agente por ter adoptado uma determinada conduta, quando de acordo com o comando legal estaria obrigado a adoptar conduta diferente. Conforme o previsto no artigo 483 n° 1 do CC, a culpa comporta duas modalidades, o dolo e a mera culpa ou a negligência.

A negligência traduz-se na omissão da diligência exigida, ou seja, consideram-se negligentes os clientes que tendo sido exortados pelo banco sobre medidas de segurança e protecção de dados, não tomam medidas apropriadas de segurança, deixam de proteger seus dispositivos, sistemas computacionais, PIN, *tokens* de segurança, detalhes pessoais, dados confidenciais entre outros procedimentos de segurança. Nesse contexto, os bancos ficam isentos de responsabilidade e não respondem pelos prejuízos resultantes de fraudes bancárias, desde que provem, entre outros factos, que a fraude resulta da acção negligente do cliente, artigo 344º do CC.

Outrossim, nos casos em que o cliente intencionalmente viola o compromisso celebrado com o banco, contrapondo-se às regras contratuais e de boa-fé, que pressupõe zelo, lealdade, bom senso, equidade e justiça, enquanto valores supremos a serem observados por todos, o banco pode ficar isento de responsabilidade, não respondendo pelos prejuízos decorrentes da fraude

[52] Cfm. Lei 22/2009 de 28 de Setembro. Lei do consumidor.

bancária, desde que prove, entre outros factos, que a fraude resulta de culpa exclusiva do cliente.

Portanto, a verificação da exclusão de responsabilidade dos bancos pelas fraudes bancárias, resulta da prova e demostração de que a conduta do cliente ou seus actos constituem o único factor gerador do dano, mediante prova de que as ferramentas tecnológicas empregadas pelo banco em seus sistemas para proteger os clientes das fraudes bancárias não são defeituosos.

Portanto, ao banco recai o ónus de prova nos termo do art. 344º do CC, ou seja, incumbe, alegar e provar que, na disponibilização dos produtos e serviços por meio dos quais a fraude bancária electrónica ocorreu, divulgou as condições gerais de utilização do produto ou serviço de pagamento electrónico ao público, em tempo útil e previamente à sua subscrição em todas agências, em lugar bem visível e de acesso directo em dispositivo de consulta fácil e directa ao abrigo do artigo 8 n° 1 do Aviso n° 2/GBM/2014 de 31 de Dezembro.

Incumbe ainda ao banco demonstrar que, após a contratação de um produto ou serviço de pagamento electrónico, forneceu ao respectivo utilizador as condições gerais de utilização do produto ou serviço de pagamento electrónico ao abrigo do artigo 9 do Aviso n° 2/GBM/2014 de 31 de Dezembro.

Neste contexto, os bancos estão isentos de responsabilidade pelos prejuízos incorridos pelo cliente quando demostrem, dentre outros factos, que, na ocorrência da fraude, o cliente agiu com dolo ou negligência, não cumprindo com as suas obrigações decorrentes do contracto celebrado para o fornecimento do produto ou serviço de pagamento electrónico ou das condições gerais de utilização do produto ou serviço de pagamento electrónico, isentando-se o banco, de responsabilidade pelos prejuízos incorridos pelo cliente em decorrência da fraude bancária[53].

Outrossim, invocando-se a culpa de terceiro, importa referir que nem todo facto de terceiro é causa de exclusão de responsabilidade, somente aquele que por si só insere o nexo causal da fraude bancária. Portanto, a culpa de terceiro equipara-se ao caso fortuito, por ser uma causa estranha à conduta do agente, imprevisível e inevitável[54].

[53] COSSA, Nocita. Responsabilidade dos Bancos no Âmbito das Fraudes Electronicas. 2022. https://www.asg.co.mz

[54] *Ibidem*

No entanto, o fortuito interno, facto imprevisível e, por isso, inevitável ocorrido no momento da fabricação do produto ou da realização do serviço, não exclui a responsabilidade dos bancos porque faz parte da sua actividade e está ligado aos riscos do empreendimento, submetendo-se à noção geral de defeito de concepção do produto ou serviço. Portanto, o banco é sempre responsável pelas suas consequências, ainda que decorrente de facto imprevisível e inevitável. O mesmo já não ocorre com o fortuito externo, facto absolutamente estranho ao produto ou serviço e que não pressupõe defeito do produto ou do serviço.

Os bancos têm o dever de adoptar mecanismos robustos para prevenir ataques cibernéticos e proteger os dados de seus clientes. Essas obrigações preventivas incluem medidas tecnológicas, monitoramento contínuo e a capacitação de funcionários, investigadores criminais e consciencialização de clientes.

3.3. Responsabilidade Criminal dos Bancos como Pessoas Colectivas.

3.3.1. Conceito de pessoa colectiva

As pessoas colectivas são organizações constituídas por uma colectividade de pessoas ou por uma massa de bens, dirigidos à realização de interesses comuns ou colectivos, às quais a ordem jurídica atribui a personalidade jurídica. Trata-se de organizações integradas essencialmente por pessoas ou essencialmente por bens, que constituem centros autónomos de relações jurídicas – autónomos mesmo em relação aos seus membros ou às pessoas que actuam como seus órgãos[55].

Uma pessoa colectiva é uma entidade legalmente reconhecida como uma empresa ou associação, que possui direitos e obrigações separadas das pessoas que a compõem. Ela pode realizar actos e contractos, adquirir e vender bens, e é responsável por suas próprias dívidas e obrigações. Além disso possui um património próprio e sua existência não depende da vida de seus membros.

3.3.2. Fundamentos da Responsabilidade Criminal das pessoas colectivas

Em harmonia com o sentido da distinção entre direito civil e direito criminal, enquanto a responsabilidade civil se dirige à restauração, especifica ou por equivalente, dos interesses

[55] PINTO, Carlos Alberto da Mota, Op Cit. Pg: 269.

individuais lesados, a responsabilidade criminal visa satisfazer interesses da comunidade, ofendida pelo facto ilícito criminal.

A responsabilidade criminal manifesta-se na aplicação de uma pena ao autor do facto criminoso. A pena, diversamente da responsabilidade civil, não visa restabelecer os interesses privados da pessoa ofendida. Traduz-se na produção de um mal a sofrer pelo agente criminoso, com a finalidade de retribuir o mal causado à sociedade com a infracção, de intimidar as outras pessoas, mostrando-lhes como a sociedade reage ao crime (prevenção geral) e impedir o próprio infractor de cometer novas infracções, segregando-o do convívio social ou aproveitando a reclusão para uma actividade regeneradora (prevenção especial)[56].

Os fundamentos da responsabilidade criminal das pessoas colectivas estão relacionados à ideia de que a empresa é uma entidade autónoma e independente aos seus membros, capaz de praticar actos ilícitos em seu próprio nome. Dessa forma, a responsabilidade criminal de pessoas colectivas é justificada pela necessidade de protecção de valores sociais e da ordem jurídica, além de ser uma forma de prevenir a impunidade de condutas criminosas cometidas em nome da organização[57].

Além disso, o autor destaca que a responsabilidade criminal de pessoas colectivas é baseada no princípio da responsabilidade objectiva, que estabelece que a pessoa colectiva pode ser responsabilizada mesmo que não haja comprovação da culpa ou dolo por parte dos seus dirigentes ou representantes. Isso se justifica pelo facto de que a empresa é uma entidade autónoma, capaz de praticar actos ilícitos em seu próprio nome e que deve arcar com as consequências dessas condutas.

Salienta ainda que, a responsabilidade criminal das pessoas colectivas busca equilibrar a responsabilidade individual dos dirigentes e representantes com a responsabilidade colectiva de empresa como um tudo, isso significa que os indivíduos que cometerem as condutas ilícitas também podem ser responsabilizadas criminalmente, mas a empresa como um todo também pode ser punida.

---

[56] PINTO, Carlos Alberto da Mota. Op Cit. Pg: 130-131.

[57] MENDES, Paulo de Souza. A Responsabilidade Penal de Pessoas Colectivas. Coimbra. Ed: Almedina. 2013. Pg: 52.

Os fundamentos da responsabilidade criminal das pessoas colectivas estão relacionados à ideia de que as empresas e outras entidades jurídicas podem ser responsabilizadas criminalmente por condutas ilícitas cometidas por seus representantes ou funcionários em nome da organização.

Alguns dos principais fundamentos da responsabilidade criminal das pessoas colectivas, incluem:

- **Protecção dos direitos e interesses da sociedade**: a responsabilidade criminal das pessoas colectivas é importante para garantir a protecção dos direitos e interessas da sociedade como um todo. A possibilidade de punir as empresas criminalmente por condutas ilícitas cometidas em seu nome pode desestimular a prática de crimes e promover a ética e a legalidade nos negócios.
- **Prevenção de condutas ilícitas**: a responsabilidade criminal das pessoas colectivas pode incentivar a adopção de práticas mais éticas e transparentes, evitando a impunidade de condutas criminosas cometidas em nome da organização.
- **Responsabilidade objectiva**: a qual estabelece que a pessoa colectiva pode ser responsabilizada mesmo que não haja comprovação da culpa ou dolo por parte dos seus dirigentes ou representantes.

3.3.3. Critérios Para Estabelecer a Responsabilidade Criminal das pessoas colectivas.

Os critérios para estabelecer a responsabilidade criminal das pessoas colectivas são importantes para determinar se a empresa pode ser responsabilizada criminalmente por crimes cometidos em seu nome ou benefício. Esses critérios geralmente incluem a conexão entre a conduta delitiva e a actividade empresarial, a presença de dolo ou culpa, a falta de controlo interno e a obtenção de benefícios económicos[58].

De acordo com Silva Sanchez, existem 4 critérios para estabelecer a responsabilidade criminal das pessoas colectivas que são:

- **A conexão entre a conduta delitiva e a actividade empresarial**: a conduta delitiva deve estar relacionada com a actividade empresarial, ou seja, ter sido cometida em nome ou benefício da empresa ou em conexão com a sua actividade.

[58] SILVA SANCHEZ, Jesus Maria da. A Responsabilidade Penal das Pessoas Colectivas: Revista de direito Penal e Criminologia. S/l, Vol:2; 2ª Ed. 2011. Pg: 173-199.

- **Imputação objectiva**: deve haver uma relação causal entre a conduta delitiva e o resultado produzido. Isso significa que a pessoa colectiva só pode ser responsabilizada se o resultado do crime for directamente causado pela conduta delitiva.
- **Falta de dever de vigilância**: a empresa deve ter falhado em estabelecer o sistema de controlo interno adequado para prevenir a prática do crime, isso significa que a pessoa colectiva deve ter falhado em estabelecer medidas adequadas para prevenir a prática do crime.
- **Benefício económico**: a empresa deve ter obtido algum benefício económico directo ou indirecto com a conduta delitiva. Isso significa que a pessoa colectiva só pode ser responsabilizada se ela obteve algum benefício financeiro com o crime.

Para que uma pessoa colectiva seja responsabilizada criminalmente, é necessário que haja conexão entre a conduta delitiva e a actividade empresarial, ou dolo ou culpa por parte dos representantes legais ou mandatários da empresa, a falha na implementação de um sistema de controlo interno adequado e obtenção de um benefício económico directo ou indirecto, com a conduta delitiva. Além disso, deve haver uma relação causal entre a conduta e o resultado produzido adequado para prevenir a prática de crimes.

3.3.4. Sanções Penais Aplicáveis às Pessoas Colectivas.

No nosso solo pátrio, as sanções penais aplicáveis às pessoas colectivas decorrem do Código Penal vigente, aprovado pela lei 24/2019 de 24 de Dezembro. De acordo com o CP, as pessoas colectivas podem ser condenadas em seguintes sanções penais:

- **Multa:** as pessoas colectivas podem ser condenadas a pagar uma multa, cujo valor é fixado pelo Tribunal com base na gravidade do crime e na capacidade da pessoa colectiva.
- **Dissolução em casos graves:** as pessoas colectivas podem ser dissolvidas pelo Tribunal. A dissolução pode ser decretada quando a pessoa colectiva foi criada com o propósito de cometer crimes ou quando a sua actividade é a prática de actividades criminosas.
- **Proibição de actividades:** a pessoa colectiva pode ser proibida de exercer determinadas actividades por um período de tempo determinado, pelo Tribunal.

- **Publicação da sentença:** o Tribunal pode ordenar a publicação da sentença condenatória em um jornal de grande circulação ou em outros meios de comunicação social.

A aplicação dessas sanções é importante para responsabilizar as pessoas colectivas pelos crimes cometidos por seus representantes legais, administradores, directores, gerentes, prepostos ou empregados. Além disso, a possibilidade de aplicação de sanções penais a pessoas colectivas pode ter um efeito dissuasório sobre a prática de crimes empresariais.

3.3.5. Eficácia da Responsabilidade Criminal das Pessoas Colectivas na Prevenção de crimes

Em Moçambique, assim como outros países, a responsabilidade criminal de pessoas colectivas, é um tema que tem ganho destaque nos últimos anos. Isso deve-se em grande parte, à crescente preocupação com a prática de crimes empresariais como corrupção, branqueamento de capitais, financiamento ao terrorismo e fraudes.

De acordo com Guedes, a responsabilização criminal de pessoas colectivas pode ter um efeito dissuasório sobre a prática de crimes empresariais, uma vez que as empresas passam a ter um incentivo para adoptar medidas preventivas e de Compliance. Além disso, a responsabilização criminal das pessoas colectivas, permite que sejam impostas sanções mais efectivas e proporcionais à gravidade do crime cometido[59].

No entanto, este autor também destaca que a eficácia da responsabilidade criminal das pessoas colectivas depende da capacidade das autoridades de investigação e do sistema judicial de identificar e punir os responsáveis pelos crimes cometidos. Ressalta ainda que é importante garantir que as sanções impostas às pessoas colectivas sejam aplicadas de forma justa e equitativa, levando em consideração as circunstâncias eficazes de cada caso.

3.3.6. Análise comparativa das Leis 35/2014 e 24/2019 de 24 de Dezembro

A responsabilidade criminal das pessoas colectivas foi um dos princípios inovadores introduzidos pelo Código Penal aprovado através da Lei n.º 35/2014 de 31 de Dezembro. Embora a responsabilização das pessoas colectivas já estivesse consagrada em diversas normas, a introdução no Código Penal representou um passo significativo no desenvolvimento

[59] GUEDES, Armando Marques. Responsabilidade Penal das Pessoas colectivas: Uma visão Comparada. In revista do Direito e Politica; n° 7. S/l, 2016. Pg: 29-44.

normativo desta matéria. Por outro lado, tal mostrava-se necessário face à realidade actual, em que as pessoas colectivas são veículos para a realização de actividades criminosas como o branqueamento de capitais, corrupção, falsidade informática entre outros.

Isto também se enquadra no que é uma tendência global, tendo em conta que outros países, como Portugal, também têm um regime de responsabilização criminal das pessoas colectivas. Embora a previsão da responsabilização criminal das pessoas colectivas tenha representado um grande avanço, a Lei n.º 35/2014 de 31 de Dezembro tinha ficado aquém na regulamentação do instituto em análise, apresentando muitas lacunas que poderiam dificultar a sua aplicabilidade. A título de exemplo, o legislador não enunciou quais as pessoas colectivas que podem ser sujeitas da infracção criminal, sendo que existem pessoas colectivas de naturezas diversas.

O Código Penal aprovado através da Lei n.º 35/2014 de 31 de Dezembro "Código Penal Antigo" foi revogado pela Lei n.º 24/2019 de 24 de Dezembro "Novo Código Penal". O Novo Código Penal também consagra o regime, no entanto, com algumas diferenças significativas. O artigo 30 n.º 1 do Código Penal Antigo prevê que as pessoas colectivas e meras associações de facto são responsáveis pelas infracções previstas no Código, quando praticadas pelos titulares dos seus órgãos ou representantes em seu nome e interesse, estando excluída a responsabilidade nos casos em que o agente tiver actuado contra ordens ou instruções expressas de quem de direito.

O Novo Código Penal, no seu artigo 30 n.º 1, prevê igualmente a responsabilização das pessoas colectivas, mas, diferentemente do Código Penal Antigo, o artigo exclui do seu âmbito de aplicação o Estado, as pessoas colectivas no exercício de prerrogativas de poder público e de organizações de direito internacional público. Ao abrigo do n.º 2, estão abrangidas no conceito de pessoas colectivas no exercício de prerrogativas de poder público as entidades públicas empresariais, as entidades concessionárias de serviços públicos, independentemente da sua titularidade, os institutos públicos e outras assim definidas por Lei.

Ainda no âmbito da aplicação, o Novo Código Penal prevê que as pessoas colectivas são responsáveis criminalmente pelos actos praticados por quem actue sob autoridade das pessoas que ocupam uma posição de direcção. Outra alteração que se destaca é a responsabilização das pessoas colectivas em caso de fusão e cisão.

Ao abrigo do artigo 31 prevê-se que, em caso de cisão e fusão, passam a responder pelo crime: (i) a pessoa colectiva ou entidade equiparada em que a fusão se tiver efectivado; e (ii) as pessoas colectivas ou entidades equiparadas que resultaram da cisão.

Por outro lado, o Código prevê a extensão da responsabilidade aos titulares de órgão de direcção, que são subsidiariamente responsáveis pelo pagamento das multas e indemnizações em que a pessoa colectiva for condenada, relativamente aos crimes: (i) praticados no período de exercício do seu cargo, sem a sua oposição expressa; (ii) praticados anteriormente, quando a decisão definitiva de as aplicar tiver sido notificada durante o período de exercício do seu cargo e lhes seja imputável a falta de pagamento.

Da análise comparativa, podemos aferir que o Novo Código Penal vem preencher as lacunas do Código Penal Antigo, enumerando de forma clara as entidades que não podem ser objecto de responsabilização, e regulando aspectos importantes, tais como a responsabilização solidária em casos de condenação em multas e indemnizações, assim como a responsabilização em caso de vicissitudes nas pessoas colectivas em causa.

No entanto, à semelhança do Código Penal Antigo, o Novo Código Penal não determina quais os crimes que poderão ser imputados às pessoas colectivas, sendo de excluir, à partida, os crimes cuja tipificação pressupõe a sua verificação exclusiva por pessoas singulares. Contudo, é possível enumerar diversos crimes em que seja possível responsabilizar criminalmente as pessoas colectivas tais como: falência culposa, insolvência, poluição, auxílio à imigração ilegal, falsificação de documentos, corrupção entre outros.

A responsabilidade criminal dos bancos enquanto pessoas colectivas surge também da necessidade de prevenir e combater crimes cibernéticos que possam comprometer a integridade do sistema financeiro e a confiança dos clientes. A responsabilização de pessoas colectivas, incluindo instituições financeiras, por actos ilícitos praticados em seu benefício. Esta responsabilidade está directamente vinculada à actuação negligente ou intencional dos bancos em situações que envolvem crimes cibernéticos. Januário e Chongo[60] observam que "a responsabilização de pessoas colectivas no sector bancário é fundamental para mitigar a ocorrência de crimes cibernéticos e reforçar a confiança no sistema financeiro".

[60] JANUÁRIO, T e CHONGO, D. Segurança cibernética no setor financeiro: Desafios e oportunidades em Moçambique. Op Cit. Pg: 45

A Lei n.º 24/2019 de 24 de Dezembro estabelece os critérios para a responsabilização criminal de pessoas colectivas, ao abrigo dos artigos 30 e 31. Esses pressupostos incluem a prática do crime no âmbito das actividades da pessoa colectiva, a existência de um benefício directo ou indirecto e a actuação de representantes legais ou pessoas em posição de autoridade dentro da instituição.

3.4. Desafios na Investigação de Crimes Cibernéticos no Sector Bancário

3.4.1. A Prevenção dos ataques cibernéticos

Prevenção refere-se às medidas adoptadas para impedir a ocorrência de crimes. No sector bancário, prevenir crimes cibernéticos é essencial para proteger os activos financeiros e a reputação institucional. A prevenção como "acções destinadas a reduzir a oportunidade de crimes", enfatiza a importância de políticas preventivas para dissuadir potenciais infractores.

3.4.2. A Investigação do Cibercrime

A investigação é crucial para identificar os responsáveis por crimes cibernéticos e reunir evidências suficientes para sua responsabilização jurídica. Fornece uma base sólida para analisar a responsabilidade dos bancos em Moçambique na prevenção e investigação de crimes cibernéticos, equilibrando aspectos legais, técnicos e práticos.

A Investigação criminal compreende o conjunto de diligências que nos termos da lei, se destinam a averiguar a existência de um crime, determinar os seus agentes, sua responsabilidade, descobrir e recolher provas no âmbito do processo penal[61].

A investigação de crimes cibernéticos em Moçambique enfrenta obstáculos estruturais e operacionais que comprometem a responsabilização dos envolvidos. Januário e Chongo[62] apontam que a ausência de um sistema nacional integrado de ciber-segurança e a falta de profissionais qualificados na área dificultam a identificação e a punição dos responsáveis por ataques cibernéticos contra bancos.

Além disso, crimes cibernéticos frequentemente envolvem redes transnacionais, o que exige cooperação internacional para a colecta de evidências e a execução de acções judiciais. No

[61] Cfm. Art. 2 da Lei 2/2017 de 9 de Janeiro (Lei do SERNIC)

[62] JANUÁRIO, T e CHONGO, D. Op Cit. Pg: 37

entanto, a legislação moçambicana ainda carece de mecanismos claros para facilitar essa cooperação, o que dificulta o enfrentamento eficaz de ataques de natureza complexa[63].

Outro desafio é a limitação de recursos tecnológicos nas instituições estatais responsáveis pela investigação. Muitos órgãos públicos, como a Procuradoria-Geral da República e a Polícia da República de Moçambique, enfrentam dificuldades para acompanhar a sofisticação das tecnologias utilizadas pelos criminosos. Isso cria um cenário de impunidade que fragiliza ainda mais a protecção dos sistemas bancários contra ataques cibernéticos.

A colaboração internacional também é prejudicada pela ausência de tratados específicos que facilitem a troca de informações entre países. Além disso, muitos órgãos investigativos em Moçambique carecem de recursos tecnológicos e treinamento especializado para acompanhar a complexidade dos crimes cibernéticos modernos.

No entanto, a legislação sobre branqueamento de capitais e financiamento ao terrorismo fornece um arcabouço para fortalecer as investigações. O artigo 68 da Lei n.º 14/2023 estabelece a cooperação internacional como um princípio central para combater crimes financeiros, incluindo aqueles relacionados a ataques cibernéticos. Esse artigo permite que Moçambique colabore com instituições estrangeiras para rastrear fluxos financeiros ilícitos e identificar redes criminosas.

[63] MATAVELE, Fernando. Op Cit. Pg: 37.

CONCLUSÃO

Chegados aqui, o trabalho suscitou-nos as seguintes conclusões: Para proteger o sector bancário de ameaças cibernéticas, estratégias críticas foram destacadas, como implementar medidas robustas de segurança cibernética, priorizar a confiança do cliente e promover a colaboração. A importância contínua da segurança cibernética não pode ser exagerada, pois sustenta a integridade do sector.

À medida que as ameaças evoluem, os bancos devem permanecer vigilantes e proactivos, adaptando consistentemente suas defesas. Nesta era digital, o comprometimento com essas estratégias é fundamental para manter um cenário financeiro seguro. Vamos defender colectivamente a segurança cibernética, garantindo a resiliência de nossas instituições financeiras contra a ocorrência de ameaças cibernéticas em constante mudança.

No que respeita a responsabilidade civil dos bancos, no contexto dos crimes cibernéticos exige a implementação de medidas preventivas eficazes, a proteção dos direitos dos consumidores e a adopção de práticas proactivas de segurança.

Uma vez preenchidos os pressupostos da responsabilidade civil pelo risco, designadamente, o facto, o nexo de imputação objectiva, o dano e o nexo de causalidade, os bancos respondem, independentemente da culpa, pela reparação de danos causados ao consumidor, por defeitos relativos à prestação de serviços, bem como por informações insuficientes sobre a sua fruição e risco.

Em Moçambique, as obrigações legais impostas pelas Leis das Transações Electrónicas e de Branqueamento de Capitais oferecem um arcabouço jurídico sólido, mas sua aplicação efetiva depende do fortalecimento das capacidades técnicas e operacionais das instituições financeiras.

A responsabilidade criminal dos bancos, como pessoas colectivas em Moçambique é um mecanismo essencial para garantir a segurança do sistema financeiro e prevenir crimes cibernéticos. O arcabouço jurídico, especialmente o Código Penal, reforça a necessidade de os bancos adoptarem medidas preventivas robustas e de cumprirem rigorosamente suas obrigações legais.

Embora as legislações analisadas representem um marco importante na regulação do sector bancário em Moçambique, apresentam lacunas que limitam sua eficácia diante das demandas impostas pelos crimes cibernéticos. É essencial que o legislador moçambicano actualize essas

normas para incluir disposições mais detalhadas sobre segurança cibernética, protecção ao consumidor e uso de tecnologias inovadoras. Isso permitirá uma resposta mais eficaz às ameaças digitais e fortalecerá a confiança no sistema financeiro.

RECOMENDAÇÕES

Para que as instituições bancarias sejam seguras e se protejam conta ataques cibernéticos, recomendamos o seguinte:

- O reforço da legislação sobre matéria de ciber-segurança, com regulamentações específicas para o sector bancário;
- Criação de um órgão especializado em ciber-segurança financeira;
- Fortalecer as parcerias público privadas para o desenvolvimento de soluções tecnológicas;
- Criação de programas de sensibilização pública sobre prevenção de cibercrimes.
- Capacitação técnica nos bancos e nas autoridades judiciais, em matéria de informática forense, para poder lidar com as inovações da inteligência artificial.
- Ractificação da Convenção de Budapeste, sobre segurança cibernética.

REFERÊNCIA BIBLIOGRÁFICA

- CASTELLS, Manuel. A Sociedade em Rede. São Paulo: Paz e Terra. 2009.
- GIL, António Carlos. Métodos e técnicas de pesquisa social (6ª ed.). São Paulo: Atlas, 2008.
- GONDWE, Gregory. Cybersecurity and Financial Institutions in Africa. Cape Town: African Research Press. 2020.
- GUEDES, Armando Marques. Responsabilidade Penal da Pessoas Colectivas: Uma visão comparada in revista do Direito e Politica, n° 7. 2016.
- JANUÁRIO, T., & CHONGO, D. Segurança cibernética no setor financeiro: Desafios e oportunidades em Moçambique. Maputo: Editora Jurídica Moçambicana. 2021.
- MACIE, Albano. Manual de Direito Penal: Parte Geral. Vol I, Editora Escolar. Maputo, 2021.
- MATAVELE, Fernando. Criminalidade cibernética em Moçambique: Uma análise sob a perspectiva do direito penal. Revista de Estudos Jurídicos, 2019.
- MENDES, Paulo de Souza. A Responsabilidade Penal de Pessoas Colectivas. Coimbra. Ed: Almedina. 2013.
- MUCAVELE, Carlos. Crimes Cibernéticos e o Sistema Bancário Moçambicano: Escola Superior de Economia e Gestão. 2020.
- NDAVUKO, Sérgio. Segurança Cibernética em Moçambique: Desafios e Perspectivas. Maputo. UEM, 2021.
- PINTO, Carlos Alberto da Mota, Teoria Geral do Direito Civil. 4ª Ed, Coimbra Editora. 2012.
- RUDRA, Ahona. Cibersegurança no Sector Bancário: principais ameaças e melhores formas de as evitar. 2023.
- SILVA SANCHEZ, Jesus Maria da. A Responsabilidade Penal das Pessoas Colectivas: Revista de direito Penal e Criminologia. Vol:2; 2ª Ed. 2011.
- TAVARES, Thiago Daniel Ribeiro, at all. Crimes Informáticos e Cibernéticos: Ciências Jurídicas Vol. 28. Ed:133/ABR. 2024.

Legislação Nacional

- Lei 3/2017 de 9 de Janeiro.
- Lei 14/2023 de 28 de Agosto.

- Lei 24/2019 de 24 de Dezembro, (Código Penal).
- Lei 2/2017 de 9 de Janeiro.
- Lei 22/2009 de 28 de Setembro.
- Lei 20/2020 de 31 de Dezembro.
- Decreto-lei n° 47 344, de 25 de Novembro de 1966 (Código Civil)
- Decreto n° 27/2016 de 18 de Julho.
- Aviso n° 4/GBM/2013 de 18 de Setembro.
- Aviso n° 2/GBM/2024 de 15 de Março.
- Código de Conduta Bancaria.

Sites

- http://powerdmarc.com.pt
- http://repositorium.sdum.uminho.pt
- http://www.nucleodoconhecimento.com.br

Outros

- União Internacional de Telecomunicações (UIT). 2021. *Global Cybersecurity Index 2020*. Geneva: ITU Publications.
- Relatório do Banco de Moçambique. 2022.
- COSSA, Nocita. Responsabilidade dos Bancos no Âmbito das Fraudes Electronicas. 2022. https://www.asg.co.mz