www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 157, 2026 | DOI: 10.69849/qr18m134

Responsabilidade bancária nos crimes cibernéticos

Banking Liability in Cybercrime

Gércio Modesto Lourenço Macie[1]
Elizete Márcia António Macie[2]

RESUMO

O presente artigo tem como tema de abordagem a responsabilidade bancária nos crimes cibernéticos. Pretende-se com o referido tema trazer uma análise no que concerne aos limites e âmbito da responsabilidade bancária, decorrente dos riscos da sua actividade, focando-se necessariamente nos crimes cibernéticos, uma vez que, na actualidade tem se verificado com maior frequência a clonagem de cartões, acesso indevido a *internet banking,* o que consubstancia em crimes informáticos (cibernéticos). Portanto, para chegar-se a conclusões palpáveis tive como objectivo geral, a análise da responsabilidade bancária face aos crimes cibernéticos. E como objectivos específicos, existem três, sendo, identificar os tipos de responsabilidade; analisar os limites da responsabilização bancária; identificar a relação da actividade bancária com as tecnologias. Com estes objectivos alcançados responder-se-á a seguinte pergunta de partida: Qual é a responsabilidade dos bancos quando verifica-se uma fraude nas contas dos clientes decorrente de ilícitos informáticos? Neste contexto, para uma conclusão cabal usou-se como metodologia da pesquisa, quanto a abordagem o presente estudo é de carácter analítico, adoptando uma abordagem marcadamente qualitativa porque baseou-se numa argumentação lógica de ideias. Quanto aos objectivos a pesquisa é de carácter exploratória, pois proporciona maior familiaridade com o problema, tem como finalidade desenvolver, esclarecer e modificar conceitos e ideias. Na vertente dos procedimentos técnicos e fontes de informação a pesquisa é bibliográfica. No que diz respeito ao método de abordagem será indutivo. O resultado do estudo sugere, em última análise, que os bancos respondem pelos ilícitos informáticos que prejudiquem aos seus clientes, mas a responsabilização deve atender ao grau de culpabilidade, tendo atenção aos limites da responsabilização bancária.

Palavras-chave: Responsabilização; Bancos; Tecnologia.

ABSTRACT

This article addresses the topic of banking liability in cybercrime. The purpose of this topic is to provide an analysis concerning the limits and scope of banking liability arising from the risks of banking activity, necessarily focusing on cybercrime, since, at present, card cloning and unauthorized access to internet banking have occurred more frequently, which constitutes computer-related (cyber) crimes. Therefore, in order to reach tangible conclusions, the general objective was to analyze banking liability in the face of cybercrime. As for the specific objectives, there are three: to identify the types of liability; to analyze the limits of banking liability; and to identify the relationship between banking activity and technology. Once these objectives are achieved, the following guiding question will be answered: What is the liability of banks when fraud occurs in customers' accounts as a result of computer-related unlawful acts? In this context, for a comprehensive conclusion, the research methodology used in this study was, in terms of

[1] Mestrando em Direito Empresarial, Universidade Católica de Moçambique (FAGRENM), Tete, Cidade de Tete, Moçambique. E-mail: gerciomodesto@gmail.com
[2] Mestre em Administração e Gestão de Negócios (MBA), Universidade Católica de Moçambique (FAGRENM), Tete, Cidade de Tete, Moçambique. E-mail: elizetantonio@gmail.com

approach, analytical in nature, adopting a markedly qualitative approach because it was based on a logical argumentation of ideas. Regarding its objectives, the research is exploratory in nature, as it provides greater familiarity with the problem and aims to develop, clarify, and modify concepts and ideas. In terms of technical procedures and sources of information, the research is bibliographic. With regard to the method of approach, it is inductive. The result of the study ultimately suggests that banks are liable for computer-related unlawful acts that harm their customers, but such liability must take into account the degree of fault, with due attention to the limits of banking liability.

Keywords: Liability; Banks; Technology.

Introdução

A actividade bancária prestada por meio de cartões de crédito ou débito, assim como através da *internet* são várias vezes alvos de ilícitos cibernéticos que muitas vezes consistem na entrada de um estranho, neste caso de terceiro indivíduo não autorizado no sistema (informático) do banco para de forma ilícita, realizar as movimentações necessárias na conta bancária dos utentes.

Portanto, neste artigo vamos abordar a responsabilidade bancária nos crimes cibernéticos. Para o efeito, o artigo vai cingir-se nos seguintes tópicos: a actividade bancária e os seus riscos; análise da responsabilidade pelo risco em geral. Dentro de cada tópico existem os subtemas.

Para a elaboração do presente artigo, o foco baseou-se na seguinte pergunta: Qual é a responsabilidade dos bancos quando verifica-se uma fraude nas contas dos clientes decorrente de ilícitos informáticos?

Portanto, como objectivo geral temos, a análise da responsabilidade bancária face aos crimes cibernéticos. E como objectivos específicos, existem três, sendo, identificar os tipos de responsabilidade; analisar os limites da responsabilização bancária; identificar a relação da actividade bancária com as tecnologias.

No que diz respeito à metodologia da pesquisa, quanto a abordagem o presente estudo é de carácter analítico, adoptando uma abordagem marcadamente qualitativa porque baseou-se numa argumentação lógica de ideias. Quanto aos objectivos a pesquisa é de carácter exploratória, pois proporciona maior familiaridade com o problema, tem como finalidade desenvolver, esclarecer e modificar conceitos e ideias. Na vertente dos procedimentos técnicos e fontes de informação a pesquisa é bibliográfica. No que diz respeito ao método de abordagem será indutivo.

1. Actividade bancária e os seus riscos

Segundo António Ferreira, "a função de gestão do risco desenvolve-se no sistema financeiro fundamentalmente através de duas áreas específicas: por um lado, a dos instrumentos financeiros derivados e, por outro lado, a da actividade seguradora, cujo objecto se traduz na negociação dos denominados riscos puros.[3]

Portanto, consagra o artigo 7 das Directrizes de Gestão de Risco (Aprovadas pelo Aviso n° 2/GBM/2024 de 15 de Março), a gestão do risco cibernético contempla, no nosso ordenamento jurídico, 9 domínios, sendo: governação, identificação, protecção, detecção, resposta e

[3] FERREIRA, António Pedro. ***Direito Bancário***. 2ª ed. Lisboa: Quid Juris Sociedade Editora, 2009, p.230

recuperação, consciência situacional, teste, terceirização e, aprendizagem.

Neste ínterim, para António Ferreira, tradicionalmente, podem ser identificadas as seguintes vertentes de risco: risco de crédito; risco da taxa de juro e da liquidez; e o risco das operações fora de balanço.[4]

Ao abrigo do artigo 1.2 das directrizes de gestão de risco (Aprovadas pelo aviso nº 4/GBM/2013, de 18 de Setembro), veremos que, os riscos associados à actividade bancária em Moçambique, comporta 9 categorias, 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 Diretrizes de Gestão do Risco Cibernético e o Quadro de Supervisão do Risco Cibernético.

Nos termos do nº 1 do artigo 9 das Directrizes de Gestão de Risco (Aprovadas pelo Aviso n° 2/GBM/2024 de 15 de Março), constata-se que a gestão de risco cibernético deve ser estabelecida como parte integrante do programa de gestão do risco organizacional, na qual as instituições avaliam o risco cibernético inerente às pessoas, processos, tecnologia, actividades, produtos e serviços identificados.

Segundo Albano Silva e Guilaze, alegam que 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.[5]

Estabelece artigo 90 da Lei n° 20/2020 de 31 de Dezembro, que é da competência dos órgãos 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.

As instituições financeiras devem monitorizar as actividades dos sistemas informáticos, de modo a detectar ataques ou iniciativas de ataques nos seus sistemas e serviços, ao abrigo do nº 1 do artigo 31 das Directrizes de Gestão de Risco (Aprovadas pelo Aviso n° 2/GBM/2024 de 15 de Março). De igual modo, as instituições financeiras são obrigadas a estabelecer uma área operacional responsável pela fiscalização dos riscos nas suas actividades, responsável por assegurar a existência de processos eficazes para identificar riscos presentes e futuros, desenvolver sistemas informáticos altamente capazes na avaliação de riscos, estabelecer políticas, procedimentos, práticas e outros mecanismos de gestão.

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

Conforme Albano Silva e Guilaze, na disponibilização e comercialização de produtos e serviços

---

[4] FERREIRA, António Pedro. ***Direito Bancário***. 2ª ed. Lisboa: Quid Juris Sociedade Editora, 2009, p.230

[5] https://www.asg.co.mz/responsabilidade-dos-bancos-no-ambito-das-fraaudes-eletronicas/. Acesso em 04 de Julho de 2024

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.

2. Tecnologia de Informação e os riscos associados

A transformação digital exige das empresas a integração da tecnologia aos processos diários dos negócios, e tudo isso demanda uma infraestrutura confiável. Nesse cenário, é fundamental garantir a confiabilidade de todos os activos de tecnologia de informação, reduzindo a margem de erros e os riscos, não apenas os de segurança, mas todos aqueles que possam afectar o desempenho dos negócios, reduzindo a capacidade competitiva das empresas.[6]

O Banco de Moçambique, procurou salvaguardar os riscos associados às Tecnologias de Informação, aprovando deste modo vários instrumentos orientadores para as demais instituições financeiras, um dos instrumentos é as Directrizes de Gestão de Risco (Aviso nº 04/GBM/2013 de 18 de Setembro), onde classifica que os serviços bancários baseados meramente na internet, são de serviços de informação e transacionais.

Nos termos do ponto 2.2.6 do Aviso nº 04/GBM/2013 de 18 de Setembro, veremos que os serviços transacionais, serviços de *Internet Banking*, permitem ao cliente executar transações financeiras online e, constituem a categoria de risco mais elevado, porque requerem controlo e segurança mais fortes.

A Internet é uma rede global intrinsecamente insegura, pois existem ameaças à segurança decorrentes de ataques de negação de serviços, nos termos do ponto 2.3 do Aviso nº 04/GBM/2013 de 18 de Setembro. Neste sentido, o banco tem a obrigação de garantir o controlo e segurança dos seus sistemas informáticos, garantindo aos seus clientes maior confidencialidade de dados.

2.1. Risco Cibernético

São considerados riscos cibernéticos os eventos que venham a causar perda financeira, interrupção (rede inoperante), extração ou dano a informações contidas nos sistemas, ou dano à reputação de uma organização em um futuro próximo em um determinado período de tempo.[7]

Segundo Guilaze, o ciber-risco coloca desafios aos tradicionais Programas de Gestão de Risco Operacional devido a natureza persistente da presença dum 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.

Neste contexto, sabendo-se da natureza dinâmica das ameaças cibernéticas, urge a necessidade de adoptar-se mecanismos para mitigar essas eventuais ameaças, por isso que

[6] https://gaea.com.br/riscos-de-ti/. Acesso em 05 de Julho de 2024.
[7] https://www.claranet.com/br/blog/riscos-ciberneticos-principais-fatores. Acesso em 05 de Julho de 2024

Banco de Moçambique, na qualidade de regulador e supervisor da actividade bancária em Moçambique, veio orientar que todas instituições financeiras devem ter políticas de segurança física e informática que seja abrangente e que façam face às potenciais vulnerabilidades e ameaças.

3. Análise da responsabilidade pelo risco em geral

No cômputo geral, olhando pelos limites da responsabilidade civil, segundo Ermenegildo Guilaze, veremos que:

> 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 responsabilidade pelo risco o facto, o nexo de imputação objetiva ou risco, o dano e o nexo de causalidade.[8]
>
> 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 controle.[9]

Portanto, neste entendimento, nota-se que, na responsabilidade civil pelo risco, o fornecedor do serviço será sempre chamado a responsabilizar-se pelo eventual dano decorrente das suas actividades, independentemente de culpa, basta que exista nexo de causalidade entre o serviço fornecido e o aludido risco.

3.1. Responsabilidade pelo risco da actividade bancária nos ilícitos eletrónicos

Estabelece do nº 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, portanto, o produtor, neste caso o fornecedor de serviços é responsável, independentemente da culpa, pelos danos causados por defeitos de produtos que coloque no mercado.

Portanto, nos termos do estipulado no nº 2 artigo 7 do Aviso n° 2/GBM/2014 de 31 de Dezembro, que aprova o Regulamento sobre Procedimentos de disponibilização de produtos e serviços de pagamento electrónico, estabelece que 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. Neste contexto, é mais que cristalino que os bancos sendo uma instituição que comercializa bens e serviços de utilidade pública, seja automaticamente responsável pelos tais produtos ora colocados à disposição do público.

---

[8] GUILAZE, Ermenegildo. ***Análise económica dos limites da responsabilidade civil***. Maputo: Escolar Editora, 2020, P. 18

[9] Idem, p. 19

Nos termos do nº 8 do artigo 14 da Lei n° 22/2009 de 28 de Setembro – Lei de Defesa do Consumidor, estabelece que os serviços são considerados defeituosos quando não oferecem a segurança que o consumidor 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.

Ora, numa conjugação do artigo 14 da Lei de defesa do consumidor e o nº 2 do artigo 9 Decreto n° 27/2016 de 18 de Julho, aprova o Regulamento da Lei de Defesa do Consumidor, estabelece que 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.

Em suma, no que diz respeito a relação sinalagmática estabelecida entre os bancos e os seus clientes, quanto ao consumo e fornecimento de bens e serviços, portanto, reconhecendo-se a fragilidade do consumidor e com vista a garantir a segurança da relação de consumo e direitos supervenientes, a regra é de que os bancos são responsáveis pelos produtos que comercializam e respondem, independentemente da culpa, pelos danos causados aos consumidores, neste caso, os clientes.

No âmbito das actividades bancárias, a maior vulnerabilidade dos serviços prestados por estes entes, recaem essencialmente nos serviços de caracter eletrónico, como as transações com cartões quer de crédito ou débito, ou então recorrendo a internet, são actividades que elevam mais riscos, assim sendo, para a disponibilização destes serviços requer-se maior segurança e controlo, aplicações ou sistemas de segurança mais eficientes e eficazes.

Neste contexto, as tecnologias de criptografia como um meio de segurança tecnológica, desempenham um papel fundamental na garantia da confidencialidade, cujo objectivo é garantir a confidencialidade dos dados das contas dos clientes e dos detalhes das transações, assim como melhorar a confiança nas transações electrónicas, combatendo deste modo as fraudes através da internet ou *clonagem* de cartões, pelo que, no âmbito da redução e controlo dos riscos, é da competência dos bancos provar que foram implementadas todas medidas de segurança na confidencialidade dos dados e integridade dos sistemas.

Estabelece o artigo 61 da Lei n.º 20/2020 de 31 de Dezembro (Lei das instituições de crédito e sociedades financeiras) que as instituições de crédito e sociedades financeiras devem assegurar aos clientes, em todas as actividades que exerçam, elevados níveis de competência técnica, dotando a sua organização empresarial com os meios materiais e humanos necessários para proporcionar condições apropriadas de qualidade e eficiência. Outrossim, os utentes devem estar informados de forma clara e precisa sobre os seus direitos, obrigações e responsabilidades assim como as responsabilidades que recaem para o banco em matéria de transações electrónicas, não basta que seja um contrato tendencialmente de adesão, vezes há, que verifica-se problemas que possam surgir de erros de processamento, e falhas de segurança, pelo que, no âmbito do dever de proteção ao cliente, incumbe aos bancos desenvolver mecanismos técnicos e meios humanos para salvaguardar e proporcionar as condições apropriadas de qualidade.

Segundo Albano Silva e Guilaze, entendem que, 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 ciber-ataques, 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.

No que diz respeito à ocorrência de ilícitos bancários, verificando-se preenchidos os pressupostos da responsabilidade civil pelo risco, nos termos do estabelecido no artigo 499º do Código Civil, designadamente, o dano e o nexo de causalidade, os bancos responsabilizam-se, independentemente da culpa, pela reparação dos danos causados ao consumidor (cliente), por defeitos relativos à prestação de serviços, bem como por informações insuficientes sobre a fruição e risco, nos termos conjugados do artigo 9 da Lei de Defesa do Consumidor e nº 1 do artigo 796 do Código Civil.

3.2. Limites da responsabilidade bancária no âmbito dos ilícitos cibernéticos

Segundo António Ferreira, o exercício da actividade bancária pode fazer incorrer o ente colectivo ou a pessoa singular, verificados os pressupostos legais respectivos, diversos tipos de responsabilidade, que podem ser civil ou criminal.[10] Estabelece o artigo 33° do Código de Conduta Bancária que, nenhuma responsabilidade poderá ser atribuída aos bancos pelos prejuízos que vierem a resultar da acção fraudulenta meramente dos clientes.

Portanto, o fornecedor de serviços pode estar isento de qualquer responsabilidade desde que prove que: 1) tendo prestado o serviço, o defeito era inexistente; 2) que a culpa é exclusiva do consumidor ou de terceiro, nos termos do nº 3 do artigo 9 do Regulamento da Lei de Defesa do Consumidor.

A culpa pode ser analisada sob duas vertentes, sendo o dolo e a mera culpa, previsto no nº 1 do artigo 483 do CC (Código Civil). Com isto, sabe-se que, em regra, a culpa consiste num juízo de censura ao agente por este ter praticado um acto à margem da permissão legal.

De acordo com Guilaze,

> 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.[11]

Neste cenário, havendo negligência dos clientes (consumidor), obviamente que os bancos ficam isentos de qualquer responsabilidade e não respondem pelos prejuízos resultantes de

---

[10] FERREIRA, António Pedro. ***Direito Bancário***. 2ª ed. Lisboa: Quid Juris Sociedade Editora, 2009, p.593

[11] GUILAZE, Ermenegildo. ***Análise económica dos limites da responsabilidade civil***. Maputo: Escolar Editora, 2020, P. 18

fraudes bancárias ligadas a aspectos tecnológicos, desde que, nos termos do artigo 344 do CC provem, que a fraude resulta da negligência do cliente.

Para que se verifique a exclusão de responsabilidade dos bancos pelas fraudes, resulta da prova, que nos termos do artigo 341 CC, tem por função a demonstração da realidade dos factos, para chegar-se a conclusão que a conduta do cliente ou seus actos constituem o único factor gerador do prejuízo, neste contexto, caberá ao banco demonstrar que as suas ferramentas tecnológicas utilizadas para proteger os clientes das fraudes bancárias não são defeituosas.

Nos termos do nº 1 do artigo 8 do Aviso n° 2/GBM/2014 de 31 de Dezembro, conjugado com o artigo 344 CC, veremos que, ao banco recai o ónus de prova, pelo que, deve este, alegar e provar que, na disponibilização dos produtos e serviços por meio dos quais a fraude bancária eletrónica ocorreu, foi divulgado as condições gerais de utilização do 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.

Conforme o estabelecido no artigo 9 do Aviso n° 2/GBM/2014 de 31 de Dezembro, compete ao banco o dever outrossim de 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.

Em suma, os bancos ficam isentos de responsabilidade pelos prejuízos incorridos pelo cliente quando demostrem que, na ocorrência da fraude, o cliente agiu com dolo ou negligência, portanto não cumprindo com os seus deveres decorrentes do contrato ora celebrado para o fornecimento do serviço de pagamento electrónico ou das condições gerais de utilização do produto ou serviço de pagamento eletrónico.

Conclusão

No âmbito das actividades bancárias comportam-se riscos, sendo os mais relevantes no presente estudo, o risco cibernético e o risco das tecnologias de informação pois, é no contexto destes riscos que muitas das vezes as fraudes bancárias ocorrem, mediante a invasão na rede informática dos bancos para a realização de movimentos indevidos nas contas bancárias dos clientes.

Devido à dinâmica dos cibercrimes, o Banco de Moçambique veio orientar que os bancos devem adoptar políticas de segurança que façam face às potenciais vulnerabilidades e ameaças cibernéticas, implementem controlos de tecnologias de informação robustos.

No que diz respeito à relação contratual, os bancos são responsáveis pelos produtos ou serviços que disponibilizam aos seus clientes nos termos do nº 2 do artigo 7 do Aviso n° 2/GBM/2014 de 31 de Dezembro, os quais têm direito à indemnização pelos danos resultantes do fornecimento de bens ou prestações de serviços defeituosos.

Com base no artigo 499 CC, notaremos que ao banco recai a responsabilidade pelo risco, ou respondendo deste modo, independentemente de culpa, pela reparação dos prejuízos que recaíram aos clientes por defeitos relativos à prestação de serviços bem como por informações insuficientes sobre a sua fruição e risco.

Portanto, nenhuma responsabilidade poderá recair aos bancos pelos danos supervenientes de

fraudes bancárias decorrentes de ataques cibernéticos, resultantes da acção negligente ou dolosa do cliente (consumidor). Assim sendo, nos termos da interpretação do nº 3 do artigo 9 do Regulamento da Lei de defesa do consumidor, percebe-se que o banco fica isento de responsabilidade quando prova que, tendo prestado o serviço, o defeito era inexistente, que a culpa pela ocorrência da fraude é exclusiva do cliente.

Referências Bibliográficas

FERREIRA, António Pedro. ***Direito Bancário***. 2ª ed. Lisboa: Quid Juris Sociedade Editora, 2009.

GONZÁLEZ, José Alberto, ***Responsabilidade Civil***, 2ª Edição, *Quid Juris* Sociedade Editora.

GUILAZE, Ermenegildo. ***Análise económica dos limites da responsabilidade civil***. Maputo: Escolar Editora, 2020.

https://www.asg.co.mz/responsabilidade-dos-bancos-no-ambito-das-fraaudes-eletronicas/. Acesso em 04 de Julho de 2024

https://gaea.com.br/riscos-de-ti/. Acesso em 05 de Julho de 2024.

https://www.claranet.com/br/blog/riscos-ciberneticos-principais-fatores. Acesso em 05 de Julho de 2024

Legislação moçambicana

Banco de Moçambique, Aviso nº 4/GBM/20213 de 18 de Setembro.

Banco de Moçambique, Aviso nº 2/GBM/2014 de 31 de Dezembro.

Banco de Moçambique, Aviso nº 2/GBM/2018 de 16 de Abril, aprova o Código de Conduta. Bancária.

Banco de Moçambique, Aviso 4/GBM/ 2024 de 15 de Março.

Decreto nº 27/2016 de 18 de Julho, aprova o Regulamento da Lei do Consumidor.

Lei nº 22/2009 de 28 de Setembro, aprova a Lei do Consumidor

Lei n.º 20/2020 de 31 de Dezembro, aprova a Lei das instituições de crédito e sociedades financeiras.

REPÚBLICA DE MOÇAMBIQUE, Código Civil, actualizado pelo decreto-lei n˚3/2006 de 23 de Agosto, Maputo: plural-Editores