INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DE LISBOA

ISCAL

SIGILO BANCÁRIO NAS RELAÇÕES DAS INSTITUIÇÕES BANCÁRIAS COM OS SEUS CLIENTES NA ERA DIGITAL

Tatiana dos Reis Gabriel

Lisboa, março de 2025

INSTITUTO POLITÉCNICO DE LISBOA

INSTITUTO SUPERIOR DE CONTABILIDADE E

ADMINISTRAÇÃO DE LISBOA

SIGILO BANCÁRIO NAS RELAÇÕES DAS INSTITUIÇÕES BANCÁRIAS COM OS SEUS CLIENTES NA ERA DIGITAL

Tatiana dos Reis Gabriel

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Gestão das Instituições Financeiras realizada sob a orientação científica da área de Direito Comum do Professor Doutor Carlos Carranho Proença.

Constituição do júri:

Presidente do Júri: Doutora Ana Maria Sotomayor

Arguente: Doutor António Alfredo Mendes

Orientador: Doutor Carlos Proença

Lisboa, março de 2025

Agradecimentos

A presente dissertação de mestrado representa o culminar de um percurso académico exigente e enriquecedor, que não teria sido possível sem o apoio e contributo de diversas pessoas, às quais deixo o meu mais sincero agradecimento.

Em primeiro lugar, expresso a minha profunda gratidão ao Professor Doutor Carlos Carranho Proença, meu orientador, pelos valiosos contributos, pela constante disponibilidade e pelo incentivo fundamental ao longo de todas as etapas deste trabalho. A sua orientação foi determinante para a concretização desta investigação. Estendo igualmente o meu reconhecimento a todos os professores que, ao longo deste percurso, partilharam os seus conhecimentos e contribuíram significativamente para o meu desenvolvimento académico e pessoal.

À minha família, manifesto o meu mais profundo reconhecimento. Um agradecimento especial ao meu esposo, que esteve sempre ao meu lado, oferecendo apoio incondicional e motivação nos momentos mais desafiantes. Aos meus pais e às minhas irmãs, o meu eterno agradecimento pelo amor, dedicação e encorajamento que sempre me proporcionaram. O vosso suporte foi, e continuará a ser, o pilar que me inspira e sustenta. Agradeço também aos meus padrinhos e à restante família, que, com carinho e confiança, me apoiou nesta caminhada.

Aos amigos, um especial agradecimento pelo estímulo e amizade, que foram fundamentais para enfrentar os desafios deste percurso com resiliência e determinação.

Quero ainda expressar a minha gratidão ao meu local de trabalho pela flexibilidade concedida, permitindo-me, em momentos cruciais, ajustar o meu horário para frequentar as aulas e dedicar-me a esta investigação. Aos meus chefes, pelo apoio compreensivo e constante, e aos meus colegas de trabalho, pela cooperação e estímulo ao longo deste processo, o meu sincero agradecimento.

Por fim, deixo um agradecimento muito especial a todos os inquiridos que participaram neste estudo. A vossa disponibilidade e colaboração foram essenciais para o desenvolvimento desta investigação, permitindo uma reflexão mais aprofundada sobre os temas abordados e conferindo maior relevância ao trabalho aqui apresentado.

A todos, o meu mais profundo e sincero obrigado por fazerem parte deste projeto e por contribuírem para a concretização deste objetivo.

Resumo

O presente trabalho explora o sigilo bancário no âmbito das relações jurídicas e estratégicas estabelecidas entre as instituições bancárias e os seus clientes, com especial enfoque em Portugal e Angola. O estudo pretende abordar a evolução histórica do sigilo bancário, desde a sua origem até à sua consagração jurídica, identificando as principais normas que lhe deram forma ao longo do tempo. Serão ainda analisados os fundamentos teóricos e valores que sustentam o sigilo bancário, bem como a caracterização das regras e procedimentos que regulam o levantamento desse sigilo, sendo estas estabelecidas no Decreto-Lei nº 298/92, de 31 de dezembro, que aprova o Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF), entre outras legislações relevantes. No que respeita ao Direito Angolano, o sigilo bancário encontra-se protegido constitucionalmente, conforme disposto no artigo 32.º da Constituição da República de Angola (CRA), o que lhe confere um peso significativo nas relações entre instituições bancárias e clientes. Este estudo aborda ainda as condições em que pode ocorrer o levantamento do sigilo bancário, comparando as abordagens legais de Portugal e Angola e as particularidades do setor bancário em cada país, especialmente no contexto da era digital. Adicionalmente, serão apresentados casos práticos que ilustram a quebra do sigilo bancário, juntamente com a análise de jurisprudência relevante, permitindo uma comparação das respostas jurídicas aplicadas em Portugal e Angola. O objetivo deste trabalho é oferecer uma compreensão aprofundada sobre o sigilo bancário, sendo especialmente relevante para profissionais do setor bancário, gestores, académicos e para o público em geral que deseje compreender a importância deste tema nas relações financeiras modernas.

Palavras-chave: sigilo bancário, relações jurídicas, fidúcia, confidencialidade, levantamento de sigilo, era digital.

Abstract

This dissertation explores banking secrecy in the legal and strategic relationships established between banking institutions and their clients, with a particular focus on Portugal and Angola. The study addresses the historical evolution of banking secrecy, from its origins to its legal recognition, identifying the key norms that have shaped it over time. It also examines the theoretical foundations and values that underpin banking secrecy, as well as the rules and procedures governing its lifting, as established in Decree-Law No. 298/92 of 31 December, which approves the General Regime of Credit Institutions and Financial Companies (RGICSF), along with other relevant legislation. Regarding Angolan law, banking secrecy is constitutionally protected, as outlined in Article 32 of the Constitution of the Republic of Angola (CRA), granting it significant weight in the relationships between banking institutions and clients. This study further addresses the conditions under which banking secrecy may be lifted, comparing the legal approaches of Portugal and Angola, and the particularities of the banking sector in each country, especially in the context of the digital age. Additionally, practical cases illustrating the breach of banking secrecy will be presented, along with an analysis of relevant jurisprudence, allowing for a comparison of the legal responses applied in Portugal and Angola. The objective of this work is to provide an in-depth understanding of banking secrecy, making it particularly relevant for banking professionals, managers, academics, and the public interested in understanding the importance of this topic in modern financial relations.

Keywords: banking secrecy, legal relationships, fiduciary duty, confidentiality, lifting of secrecy, digital era.

Índice

Índice de Gráficos

Lista de Siglas

ASF - Autoridade de Supervisão de Seguros e Fundos de Pensões

AT – Autoridade Tributária

BCE - Banco Central Europeu

BNA- Banco Nacional de Angola

BFA- Banco de Fomento de Angola

BP - Banco de Portugal

BPN- Banco Português de Negócios

CCPA- *California Costumer Protection Acts*

CMC- Comissão de Mercado de Capitais

CNPD - Comissão Nacional de Proteção de Dados

CPC - Código do Processo Civil

CP – Código Penal

CPP - Código do Processo Penal

CRA- Constituição da República de Angola

CRP - Constituição da República Portuguesa

CRS- *Common Reporting Standard*

DL –Decreto-Lei

IA- Inteligência Artificial

GDPR- *General Data Protection Regulation*

KYC- *Know your customer.*

UIF - Unidade de Informação Financeira

LGT - Lei Geral Tributária

LGPD- Lei Geral da Proteção de Dados

OCDE - Organização para a Cooperação e Desenvolvimento Económico

RCBE - Registo Central de Beneficiário Efetivo

RGIGSF - Regime Geral das Instituições de Crédito e Sociedades Financeiras

RGPD- Regulamento Geral Sobre a Proteção de Dados

SEBC - Sistema Europeu de Bancos Centrais

STJ - Supremo Tribunal de Justiça

TIAC - Transparência e Integridade, Associação Cívica

TJUE - Tribunal de Justiça da União Europeia

UE- União Europeia

1- Introdução

A confidencialidade na atividade bancária é uma obrigação legal que impõe aos bancos e instituições financeiras a responsabilidade de preservar o sigilo sobre todas as informações relacionadas aos seus clientes. Essa obrigação é fundamental não apenas para proteger os dados pessoais e financeiros dos clientes, mas também para garantir a integridade e a segurança do sistema financeiro como um todo. O sigilo bancário fortalece a confiança nas relações entre clientes e instituições, desempenhando um papel crucial na estabilidade e no bom funcionamento do setor financeiro (Bessis, 2015, p. 134).

Historicamente, o conceito de sigilo bancário remonta a práticas que surgiram no século XVIII, quando as instituições financeiras começaram a reconhecer a importância da confidencialidade na construção de relacionamentos sólidos com seus clientes. Segundo Luhmann (1996, p. 58), a confiança é um elemento essencial nas interações sociais, e o sigilo bancário configura-se como um mecanismo de construção dessa confiança no setor financeiro. À medida que o sistema bancário evoluiu, especialmente com a globalização e a liberalização dos mercados, a proteção dos dados dos clientes tornou-se ainda mais crucial.

Com a crescente digitalização dos serviços financeiros, surgem novos desafios e oportunidades para a proteção do sigilo bancário. Como destaca Zohar (2020, p. 215), a era digital impõe a necessidade de um equilíbrio entre inovação tecnológica e a proteção da privacidade dos consumidores. A implementação de tecnologias como a inteligência artificial e *big data* pode facilitar a personalização dos serviços, mas também levanta questões sérias sobre a segurança e a privacidade dos dados. Dessa forma, as instituições financeiras enfrentam a difícil tarefa de garantir a confidencialidade num ambiente cada vez mais complexo e regulado.

Além disso, a legislação relacionada com o sigilo bancário tem-se adaptado às novas realidades. A Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, foi substituída pelo Regulamento (UE) 2016/679, conhecido como Regulamento Geral sobre a Proteção de Dados (RGPD), adotado em 27 de abril de 2016 e que entrou em vigor em 25 de maio de 2018. Este regulamento, promovido pelo Parlamento Europeu e pelo Conselho da União Europeia,

reforça a proteção dos dados pessoais e estabelece novas normas sobre o seu tratamento. Este regulamento estabelece normas rigorosas para a coleta, armazenamento e processamento de dados pessoais, visando garantir a privacidade dos indivíduos e aumentar a responsabilidade das organizações que lidam com esses dados (Kuner, 2017, p.87).

Os princípios fundamentais do RGPD incluem o consentimento explícito dos indivíduos para a coleta de seus dados, a transparência em relação ao uso desses dados, e o direito de acesso e retificação, permitindo que os indivíduos acedem e corrijam informações imprecisas. Além disso, os indivíduos possuem o direito ao esquecimento, que lhes permite solicitar a exclusão de seus dados pessoais em determinadas circunstâncias. O regulamento também impõe a obrigação de que as organizações implementem medidas técnicas e organizacionais adequadas para garantir a segurança dos dados (Regulamento (UE) 2016/679).

A influência do RGPD estende-se além das fronteiras da Europeia (UE), tendo impactos significativos em legislações de diversos países, como Angola, que têm evoluído suas normas para se alinhar a essas novas exigências de proteção de dados (Kuner, 2017, p.87).

Neste contexto, o presente trabalho visa abordar aspetos cronológicos das principais alterações ao nível conceptual do sigilo bancário, enfatizando suas conquistas e desafios na era digital.

A estrutura deste trabalho está organizada em quatro capítulos principais. O primeiro capítulo, introdução, problemática, evolução histórica e fundamentos do sigilo bancário, fará uma introdução ao tema, destacando a relevância do sigilo bancário no contexto jurídico e financeiro, bem como analisar a sua evolução histórica e os seus fundamentos essenciais. No segundo capítulo, Angola e Portugal: evolução e comparação, serão abordadas as particularidades do sigilo bancário em Angola e Portugal, com ênfase na evolução legislativa em ambos os países, destacando as semelhanças no tratamento jurídico dessa questão. O terceiro capítulo, sobre o sigilo bancário na era digital: Angola e Portugal, irá analisar casos práticos relevantes, focando a aplicação do sigilo bancário na era digital, assim como a legislação pertinente em Angola e Portugal, e refletindo sobre os desafios e riscos trazidos pela digitalização dos serviços bancários. Por fim, o quarto capítulo, apresentação de resultados e considerações finais, apresentará os resultados

obtidos ao longo do estudo, oferecendo uma análise crítica e reflexiva sobre as conclusões alcançadas, e propondo sugestões para futuras investigações, além de destacar as implicações práticas no setor bancário. Através desta divisão temática, espera-se fornecer uma compreensão mais aprofundada do sigilo bancário e da sua importância nas relações entre as instituições financeiras e os seus clientes, num mundo cada vez mais digitalizado.

1.1. Problemática

A digitalização dos serviços bancários trouxe uma série de desafios e oportunidades para a proteção do sigilo bancário. Com o aumento das transações *online* e o uso de tecnologias como a inteligência artificial e *big data*, questiona-se:

Como as instituições bancárias asseguram a privacidade e a proteção dos dados dos clientes na era digital, e em que medida as legislações atuais acompanham os desafios e riscos impostos por essa transformação digital?

1.2. Hipóteses

Considera-se as seguintes hipóteses:

H1: As instituições bancárias têm implementado medidas adequadas para proteger o sigilo bancário dos seus clientes na era digital, mas ainda existem lacunas significativas nas legislações portuguesas e angolanas que regulam essas práticas.

H2: A conscientização dos consumidores sobre a importância do sigilo bancário e suas implicações nas relações com as instituições bancárias é insuficiente, resultando numa maior vulnerabilidade a riscos de segurança.

H3: O uso de tecnologias emergentes, como inteligência artificial e *big data*, tem contribuído para a melhoria das práticas de segurança, mas também tem criado desafios para a proteção do sigilo bancário.

1.3. Objetivo Geral

O objetivo geral é analisar as práticas de sigilo bancário nas relações entre as instituições bancárias e seus clientes na era digital, identificando os desafios, riscos e medidas de proteção de dados em um contexto tecnológico em constante evolução.

1.4. Objetivos Específicos

a) Identificar e descrever as principais medidas de proteção de dados implementadas pelas instituições bancárias para garantir o sigilo bancário.
b) Examinar a perceção dos trabalhadores das instituições bancárias sobre a eficácia das práticas atuais de proteção de dados e sigilo bancário.
c) Avaliar o nível de conscientização e compreensão dos clientes em relação aos seus direitos de privacidade e proteção de dados no contexto das transações bancárias digitais.
d) Investigar os principais desafios enfrentados pelas instituições bancárias na proteção do sigilo bancário, especialmente em relação ao uso de tecnologias emergentes como IA e *big data*[1].

1.5. Justificação

A proteção do sigilo bancário é fundamental para a confiança nas relações financeiras. No contexto atual, em que as tecnologias digitais estão em constante evolução, a preocupação com a privacidade das informações é mais pertinente do que nunca. A análise das práticas das instituições financeiras, aliada à compreensão das legislações em vigor, pode contribuir para a formulação de políticas que assegurem a proteção dos dados dos clientes, promovendo a transparência e a responsabilidade das instituições.

No entanto, as medidas tecnológicas, por mais sofisticadas que sejam, não eliminam as lacunas existentes nas legislações que regulamentam o sigilo bancário. Segundo Gomber et al. (2017, p.220), as regulamentações bancárias muitas vezes são lentas para acompanhar o rápido desenvolvimento tecnológico, o que resulta em brechas na proteção dos dados dos consumidores, especialmente em relação ao compartilhamento de dados com terceiros e à prevenção de ataques cibernéticos. Isso é particularmente evidente em países onde a legislação de proteção de dados ainda está em processo de amadurecimento, como em algumas economias emergentes.

[1] *Big data* consiste na recolha e guarda de grande volume e variedade de dados, que são processados a grande velocidade com recurso a ferramentas tecnológicas e métodos analíticos avançados e cuja utilização permite prever comportamentos e padrões de consumo (*Data Mining*) (Banco de Portugal). Big data - o que é | Portal do Cliente Bancario

Essas lacunas legais são agravadas por um cenário global em que as normas de sigilo bancário variam significativamente entre as jurisdições, criando complexidades para os bancos que operam internacionalmente. Tal diversidade legislativa pode resultar em situações onde a privacidade do cliente é comprometida devido à fragmentação regulatória (Mersch, 2018, p.159).

Embora as instituições financeiras estejam cada vez mais preocupadas com a segurança dos dados dos clientes, a conscientização dos consumidores sobre o sigilo bancário ainda é limitada. Estudos mostram que muitos clientes não estão plenamente cientes de como os seus dados são coletados, armazenados e compartilhados pelas instituições financeiras. De acordo com Milne (2016, p. 121), os consumidores frequentemente aceitam termos e condições sem entender plenamente as suas implicações, especialmente em relação ao compartilhamento de dados com terceiros. Além disso, essa discussão é crucial para educar os consumidores sobre os seus direitos e para fomentar um ambiente de confiança nas interações financeiras digitais.

1.6. Metodologia

Neste tópico são detalhados os procedimentos metodológicos adotados para o desenvolvimento do presente projeto. Segundo Lakatos e Marconi (2017, p. 83), a utilização de métodos científicos vai além da ciência formal, sendo aplicável também na resolução de problemas do quotidiano. Os autores destacam que "não há ciência sem o emprego dos métodos científicos", enfatizando a importância de seguir uma metodologia rigorosa para garantir a validade e a fiabilidade dos resultados.

Em relação aos métodos de pesquisa, o presente estudo adotará dois enfoques principais: o método dedutivo e o método hipotético-dedutivo. O método dedutivo, conforme exposto por Gil (2019, p. 43), envolve partir de princípios gerais para compreender situações particulares, sendo ideal para pesquisas que buscam validar teorias pré-estabelecidas. Já o método hipotético-dedutivo, como descreve Popper (2002, p. 89), parte de uma problemática de pesquisa, formulando hipóteses que podem ser testadas ao longo do processo investigativo.

Quanto à forma de abordagem do problema, a pesquisa será qualitativa e quantitativa. A abordagem qualitativa, segundo Pereira (2001, p. 57), reconhece que há uma interação dinâmica entre o sujeito e o mundo real, criando um vínculo indissociável entre o mundo

objetivo e a subjetividade do investigador, o que não pode ser plenamente traduzido em números. Complementarmente, a pesquisa quantitativa permitirá a coleta e análise de dados numéricos que ajudem a validar as observações qualitativas.

Em termos de objetivos, o estudo será descritivo, conforme o conceito de Gil (2002, p. 117), que define a pesquisa descritiva como aquela que busca descrever características de uma população ou fenómeno, ou ainda estabelecer relações entre variáveis. Este tipo de pesquisa é essencial para proporcionar uma visão clara e detalhada do objeto de estudo, sem manipular as variáveis, mas sim observando-as em seu estado natural.

Por fim, quanto aos procedimentos metodológicos, será realizada uma pesquisa bibliográfica, que, de acordo com Lakatos e Marconi (2017, p. 93), envolve a análise de materiais já publicados, como livros, artigos científicos, dissertações e fontes *online*. Esta técnica é fundamental para garantir que o estudo seja fundamentado num corpo sólido de conhecimento já existente, permitindo ao investigador um contacto direto com o material previamente produzido sobre o tema.

Capítulo 1. Enquadramento histórico do sigilo bancário

O sigilo bancário em Portugal é um conceito legal fundamental que protege as informações financeiras e pessoais dos clientes das instituições financeiras (Afonso, 2014, p. 45). Esse princípio está intrinsecamente ligado ao direito à privacidade, que assegura que as informações partilhadas com o banco não sejam divulgadas a terceiros sem o consentimento explícito do cliente.

O direito à privacidade é um direito fundamental reconhecido na Constituição da República Portuguesa (CRP), especificamente no artigo 26.º, que garante a proteção da vida privada e familiar, da correspondência e de outros meios de comunicação. Este direito é considerado essencial para a dignidade da pessoa humana e para o exercício da liberdade individual (Cruz, 2018, p. 123). Segundo Figueiredo (2019, p. 78), a privacidade é um pilar da confiança nas relações financeiras, uma vez que os clientes devem sentir-se seguros ao partilhar informações sensíveis com as instituições financeiras. Portanto, o Decreto-Lei n.º 337/90, de 30 de outubro de 1990, estabeleceu regras para a proteção do sigilo bancário, incluindo a proibição da divulgação de informações geradas no exercício das funções do banco.

Em 1822 surgiu a primeira referência normativa estatutária ao segredo bancário em Portugal, constando do artigo 73.º do Regulamento do Banco de Lisboa. Este regulamento estabelecia que as operações do banco e os depósitos dos clientes particulares eram objeto de segredo. Um colaborador que revelasse qualquer informação sobre clientes poderia ser repreendido se a sua ação não resultasse em dano ou despedido se resultasse.

O artigo 83.º do Regulamento Administrativo do Banco de Portugal, resultante da fusão do Banco de Lisboa com a Companhia de Confiança Nacional, aprovado por decreto do Governo em 28 de janeiro de 1847 e publicado no Diário do Governo, estabelecia um regime idêntico para tais empregados, substituindo "expulso" por "despedido" (Sousa, cit. *in* Azevedo, 2012, p. 212).

A legislação fiscal geral também determina as circunstâncias em que os dados bancários podem ser divulgados, por exemplo, para efeitos fiscais. O sigilo bancário pode ser levantado em determinadas circunstâncias, como na existência de provas de fraude fiscal ou quando são solicitadas informações pelas autoridades para fins legítimos (Figueiredo, 2019). O autor ainda menciona que, em caso de levantamento do sigilo bancário sem

fundamento legal, o cliente pode apresentar reclamação ao Banco de Portugal e à Comissão Nacional de Proteção de Dados.

Alguns autores, como Sousa (2012, p. 212), interpretam a natureza jurídica do sigilo bancário como um aspeto do sigilo profissional, pelo qual os bancos bem como os seus trabalhadores são obrigados a não divulgar informações pessoais e financeiras sobre os seus clientes.

A obrigação de manter o sigilo bancário reflete o respeito à privacidade dos clientes e constitui um princípio central da ética profissional no setor financeiro. Além disso, o sigilo bancário é amplamente reconhecido como um direito fundamental, protegido tanto pela CRP, quanto pela Lei Orgânica do Banco de Portugal (*Vide infra*, cit. *in* Afonso, 2014, p. 8).

Na CRP, a proteção do sigilo bancário pode ser derivada do artigo 26.º, que trata dos direitos de personalidade, assegurando o direito à privacidade, incluindo a "reserva da intimidade da vida privada" e a "proteção legal contra qualquer forma de abuso". O sigilo bancário é, portanto, uma extensão natural do princípio constitucional de proteção da privacidade dos cidadãos.

Complementando essa proteção, a Lei Orgânica do Banco de Portugal (Lei n.º 5/98, de 31 de janeiro) regulamenta o sigilo bancário de forma mais detalhada. O artigo 80.º da referida lei estabelece o dever de sigilo, impondo às instituições financeiras a responsabilidade de manter confidenciais todas as informações relativas aos seus clientes e às suas operações bancárias, salvo quando a lei dispuser em contrário. Esta disposição visa garantir que o sigilo bancário seja respeitado, exceto em circunstâncias legalmente previstas, como em casos de investigação judicial ou supervisão bancária.

De acordo com o Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF), aprovado pelo Decreto-Lei n.º 298/92, de 31 de dezembro, com as suas alterações subsequentes, o sigilo bancário aplica-se não apenas às instituições financeiras, mas também àqueles que exerçam ou tenham exercido funções no Banco de Portugal, bem como a qualquer pessoa ou entidade que lhe preste ou tenha prestado serviços, quer de forma ocasional, quer de forma permanente (artigo 80.º, n.º 1). Além disso, as autoridades, organismos e pessoas que participem na troca de informações com o Banco de Portugal estão igualmente vinculados ao dever de sigilo, conforme estabelecido no

artigo 81.º, n.º 5, que regula os deveres de cooperação entre entidades nacionais e estrangeiras. Essas disposições garantem a confidencialidade e a proteção de informações sensíveis no âmbito da atividade bancária, reforçando a confiança nas relações entre o Banco de Portugal e outras instituições.

O mesmo consagra ainda uma enumeração exemplificativa, da qual constam elementos considerados relevantes que estão sujeitos a segredo, sendo estes "os nomes dos clientes, as contas de depósito e seus movimentos e outras operações bancárias".

Resumindo, em Portugal, o sigilo bancário é um conceito jurídico que visa proteger a informação financeira e pessoal dos clientes das instituições financeiras, garantindo a confidencialidade e segurança dos dados. Embora possa ser levantado em determinadas circunstâncias, o sigilo bancário é essencial para a credibilidade das instituições financeiras e para a proteção dos direitos dos clientes.

1.1. O sigilo bancário no âmbito do RGICSF em Portugal

O sigilo bancário depende diretamente da dimensão e do conteúdo pelo qual é reconhecido o direito à intimidade da vida privada. No n.º 2 do artigo 26.º da CRP verifica-se que a legislação defende o direito à reserva de vida privada e garante que a lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas ou contrárias à dignidade humana, de informações relativas às pessoas e famílias (Canotilho, 2007, p.458), ou seja, o Estado não pode violar como ainda tem de assegurar que mais ninguém desrespeita este direito.

O artigo 79.º do RGICSF, estabelecido pelo Decreto-Lei n.º 298/92, de 31 de dezembro, prevê várias exceções ao dever de sigilo bancário. Em termos gerais, o sigilo bancário protege a confidencialidade das informações entre a instituição financeira e o cliente, contudo, existem situações específicas em que essa proteção pode ser levantada.

Uma dessas exceções ocorre quando o cliente transmite autorização expressa à instituição bancária para que a informação referente à sua conta ou transações possa ser revelada. Esta autorização deve ser clara e inequívoca, garantindo que a instituição tenha consentimento para partilhar os dados.

Adicionalmente, o Banco de Portugal pode ter acesso a essas informações no âmbito das suas funções de supervisão e regulação do sistema financeiro. Da mesma forma, a Comissão do Mercado de Valores Mobiliários (CMVM) está autorizada a aceder a

informações protegidas pelo sigilo bancário no exercício das suas atribuições de supervisão e regulação dos mercados de valores mobiliários.

Além disso, instituições como o Fundo de Garantia de Depósitos[2], o Sistema de Indemnização aos Investidores[3] e o Fundo de Resolução[4] podem aceder a essas informações no cumprimento das suas funções de proteção dos investidores e de intervenção em crises financeiras.

Outra exceção ao dever de sigilo bancário ocorre quando as autoridades judiciárias, no âmbito de processos penais, solicitam o levantamento do sigilo bancário para efeitos de investigação ou julgamento, sobretudo em casos de suspeita de atividades ilícitas, como fraude ou branqueamento de capitais.

A Administração Tributária também pode pedir o levantamento do sigilo bancário no exercício das suas funções de fiscalização fiscal, principalmente para prevenir e combater a evasão fiscal e outros crimes tributários.

Por fim, o dever de segredo pode ser limitado por outras disposições legais que prevejam expressamente o levantamento do sigilo bancário em determinadas circunstâncias. Exemplos disso incluem a legislação relacionada com o combate ao branqueamento de capitais e ao financiamento do terrorismo, que pode prever exceções ao dever de sigilo. Estas exceções visam equilibrar a proteção da privacidade dos clientes com a necessidade de supervisão e regulação por parte das autoridades competentes e o cumprimento das obrigações legais, nomeadamente no âmbito de processos judiciais e da luta contra crimes financeiros.

O segredo profissional, no qual está inserido o sigilo bancário, é regulado pelo RGICSF (do artigo 78.º ao artigo 84.º), sendo que este já foi alvo de inúmeras alterações. O RGICSF prevê o dever de segredo no n.º 1 do artigo 78.º.

---

[2] O Fundo de Garantia de Depósitos é um mecanismo criado para proteger os depositantes bancários em caso de insolvência da instituição financeira onde possuem contas. Em Portugal, foi estabelecido pelo Decreto-Lei n.º 298/92, de 31 de dezembro. Fundo Garantia Depósitos: Quando é acionado e como é feito o reembolso

[3] O Sistema de Indemnização aos Investidores visa proteger os clientes de instituições financeiras que fornecem serviços de investimento, caso estas não cumpram as suas obrigações financeiras. Regulamentado pela Lei n.º 67/98, este sistema é aplicável em situações de insolvência das entidades, cobrindo perdas relacionadas com valores mobiliários ou dinheiro detido por estas instituições para a prestação de serviços de investimento. CMVM - Portal Institucional

[4] O Fundo de Resolução foi criado para apoiar a estabilização do sistema financeiro, atuando na recapitalização ou reestruturação de instituições financeiras em dificuldade. É financiado pelas próprias instituições de crédito e pode ser mobilizado em situações como medidas de resolução bancária.

Assim, o sigilo bancário, apresenta duas facetas importantes, a primeira cinge-se na carência de acautelar a vantagem do indivíduo, ou seja, o cliente e a segunda, na carência de acautelar um conjunto de vantagens inerentes à sociedade. (Tavares, 2021, p.3).

1.2. Fundamentos do sigilo bancário e relação das instituições e os clientes

O sigilo bancário não existe apenas tendo em vista a tutela da posição do cliente. Visa proteger a própria instituição bancária, em termos reequacionais ou reputacionais, estando por isso em causa o crédito e bom nome da pessoa coletiva (art.º 484 do CC; art.º 160 do CC; art.º 12, n.º 2, da CRP). Se a instituição bancária não oferecer a confiança necessária, dará lugar ao descrédito, que será impeditivo de uma situação de atração de clientela nova e de manutenção da carteira de clientes. A ausência de uma relação de confiança, nos termos referidos, colocaria em causa o funcionamento de todo o sistema bancário, com as sucessivas repercussões na economia.

A relação que o cliente estabelece com o Banco baseia-se em interesses recíprocos que vão além da simples proteção das informações do cliente. Essa relação revela que o segredo bancário também está associado a um interesse público, uma vez que a preservação da confidencialidade é crucial para o funcionamento do sistema financeiro. A justificação económica, ao promover a estabilidade e confiança no sistema bancário, é um fundamento tão legítimo quanto a tutela da privacidade do cliente. A confiança depositada nas instituições bancárias gera incentivos à poupança e ao investimento, estabelecendo uma dimensão que transcende a relação entre as partes e contribui para o desenvolvimento económico do país.

Nesse contexto, o artigo 101.º da CRP reconhece a importância da preservação e desenvolvimento da propriedade privada, destacando a função social da economia e sua contribuição para o crescimento do país. Assim, o sigilo bancário desempenha um papel crucial na manutenção da confiança do público nas instituições financeiras, sendo essencial não apenas para os interesses individuais, mas também para a estabilidade económica e o bem-estar social.

Os fundamentos do sigilo bancário partem de um princípio de confiança, que beneficia ambas as partes numa relação bancária, mas com repercussões para o sistema bancário em geral, ao criar um ambiente de segurança e confiança no público. Isso demonstra que o sigilo bancário vai além da confidencialidade, abrangendo outras dimensões que refletem o impacto dos dados bancários na vida pessoal e económica dos clientes.

Marques (2016, p. 6) reforça essa ideia ao destacar que o segredo bancário não se limita à proteção do cliente, mas tem também uma finalidade pública e económica.

A relação contratual estabelecida com o Banco deve, portanto, pautar-se por uma garantia de confidencialidade, assegurando a privacidade do cliente. Essa relação impõe lealdade mútua entre as partes, exigindo que nenhuma informação obtida seja revelada ou usada indevidamente, exceto nos casos previstos por lei. A obrigação de discrição, conforme disposto no RGICSF, é uma regra de conduta essencial para as instituições bancárias. O seu artigo 78.º, por exemplo, estipula que o dever de sigilo cobre todas as informações obtidas durante a prestação de serviços, sendo permitido o seu levantamento apenas em situações claramente previstas na legislação, como investigações criminais ou ordens judiciais. Marques (2016, p.7) destaca que essa obrigação de discrição protege a posição do cliente face a terceiros em todas as operações realizadas.

Com o tempo, o sigilo bancário deixa de ser apenas uma exigência de confiança contratual bilateral e passa a ser uma necessidade pública essencial para o funcionamento eficiente das instituições financeiras. Cordeiro (2014) defende que a confiança pública nas instituições financeiras é um pilar fundamental para a sustentabilidade do sistema bancário.

1.3. Direito à reserva da intimidade da vida privada e o segredo bancário

O sigilo bancário está relacionado com a privacidade financeira das pessoas e empresas, sendo assim é tratado sob a perspetiva do direito à reserva da intimidade da vida privada. Tendo como foco tutelar interesses públicos e privados dos clientes da instituição bancária. O direito à reserva da intimidade da vida privada é um princípio fundamental em Portugal e está protegido pela CRP, no seu artigo 26.º (Cordeiro, 2001, p.456)

Assim, ninguém irá tranquilo a um hospital se pensar que pode ser violentado, em público, na sua sensibilidade ou no seu pudor. Ou, por exemplo, ninguém confiará no seu advogado se tiver a ideia que este poderá revelar, fora do que exija a defesa dos interesses, quanto lhe confiar (Cordeiro, 2014, p.353).

Face ao exposto, torna-se clara a relevância do direito à reserva sobre a intimidade da vida privada. O direito à reserva sobre a vida privada insere-se no âmbito de um direito geral de personalidade, consagrado pelo art.º 70.º do Código Civil (CC), e, de forma mais específica, encontra-se regulado pelo art.º 80.º do CC. Este artigo estipula que “todos

devem guardar reserva quanto à intimidade da vida privada de outrem", protegendo as várias esferas da vida pessoal. De acordo com a teoria das esferas, o artigo oferece proteção a três níveis: a esfera privada, a secreta e a íntima. A esfera privada relaciona-se com o conjunto de informações sobre a vida de uma pessoa que são partilhadas apenas com um círculo restrito de indivíduos. A esfera secreta abrange questões de natureza confidencial, as quais são conhecidas por poucos ou mantidas ocultas de forma intencional. Já a esfera íntima diz respeito aos aspetos mais profundos da vida pessoal, que são exclusivamente do conhecimento do próprio indivíduo, envolvendo sentimentos, pensamentos e emoções.

O artigo 80.º do CC, no seu nº 2, estabelece que a extensão da reserva sobre a intimidade é delimitada por dois elementos: um objetivo e outro subjetivo. O elemento objetivo refere-se a situações em que, por razões de justiça ou interesse público, pode haver uma intromissão na privacidade. Já o elemento subjetivo depende das expetativas que a pessoa tem em relação à proteção da sua privacidade, o que exige uma ponderação caso a caso (Oliveira, 2024, p. 45).

A violação do dever de sigilo bancário pode conduzir à responsabilidade civil, conforme previsto no artigo 483.º, n.º 1 do CC, que estabelece a obrigação de indemnizar por atos ilícitos que causem danos a outrem. Para que exista responsabilidade civil, é necessário provar a existência de um ato ilícito, culpa, dano e nexo de causalidade entre o ato e o prejuízo. No contexto da violação de sigilo, se uma instituição financeira ou um dos seus colaboradores divulgar indevidamente informações confidenciais de um cliente, essa divulgação pode constituir um ato ilícito que gera o dever de indemnizar o lesado pelos danos sofridos.

Além disso, pode haver responsabilidade pelo risco, conforme os artigos 500.º e 501.º do CC, aplicável às responsabilidades do comitente, do Estado e outras pessoas coletivas públicas. Estes artigos dispõem que, em atividades que, pela sua própria natureza, envolvem um risco elevado para terceiros, por exemplo, o uso de tecnologia avançada ou sistemas digitais que podem expor informações sensíveis, o responsável por essa atividade pode ser obrigado a reparar os danos causados, independentemente de culpa. Ou seja, a responsabilidade baseia-se no risco inerente à atividade, e o lesado não precisa de provar que houve negligência ou dolo para ter direito à indemnização.

No caso de ocorrer uma intromissão indevida na privacidade de uma pessoa, o artigo 70.º, n.º 2, do CC permite que o lesado solicite medidas para fazer cessar essa violação. Este artigo protege o direito à personalidade, incluindo o direito à privacidade, e prevê que a pessoa cujos direitos sejam violados pode pedir providências adequadas para prevenir ou parar essa intromissão. Entre as medidas que podem ser solicitadas estão as medidas cautelares, que têm como objetivo evitar a continuidade ou o agravamento da violação do direito, suspendendo temporariamente a conduta lesiva enquanto o processo principal não é julgado. Além disso, podem ser aplicadas sanções pecuniárias compulsórias, uma forma de coação financeira para garantir que o infrator cesse a sua conduta lesiva, sob pena de pagamento de uma quantia estabelecida pelo tribunal.

Estas disposições visam garantir a proteção eficaz dos direitos de personalidade, nomeadamente no que respeita à privacidade e confidencialidade, bem como a responsabilização daqueles que violam esses direitos, seja por via de atos ilícitos ou pelo risco inerente a certas atividades.

No âmbito penal, a proteção da privacidade tem sido significativamente reforçada com a criminalização de condutas que atentam contra este direito fundamental. O CP de Portugal, nos seus artigos 190.º, 192.º e 193.º, exemplifica essa evolução ao tratar dos crimes relacionados com a violação da correspondência e da vida privada. Essas disposições visam assegurar a inviolabilidade da intimidade das pessoas, garantindo que a sua correspondência, comunicações e informações pessoais sejam protegidas contra atos ilícitos.

O artigo 190.º do CP aborda o crime de violação de correspondência ou de telecomunicações, tutelando a confidencialidade das comunicações privadas. Este artigo considera crime qualquer ato que, sem autorização, tenha por objetivo tomar conhecimento de correspondência alheia, seja por via de cartas, mensagens telefónicas ou comunicações eletrónicas. A violação ocorre quando alguém, sem o consentimento do destinatário, abre, oculta, desvia ou destrói correspondência fechada ou, ainda, intercepta comunicações entre outras pessoas. Além disso, é igualmente considerado crime a utilização indevida de informações contidas nessas correspondências. A proteção da privacidade é essencial nesse contexto, dado que a correspondência e as telecomunicações são elementos centrais nas relações pessoais e profissionais dos indivíduos. A pena aplicável para esta infração pode ir até 1 ano de prisão ou uma multa até 240 dias.

Contudo, em casos em que o crime seja praticado por profissionais que ocupam cargos específicos, como trabalhadores de serviços postais ou telecomunicações, ou em situações de abuso de funções, a gravidade da punição pode aumentar.

O artigo 192.º do CP, por sua vez, trata do crime de devassa da vida privada. Este artigo protege a intimidade das pessoas, proibindo a divulgação ou utilização de informações privadas sem o consentimento da pessoa envolvida, quando isso possa prejudicar a sua honra ou reputação. Este tipo de infração pode ocorrer, por exemplo, quando se divulga publicamente dados pessoais, imagens ou detalhes da vida íntima de alguém, sem autorização, o que pode resultar em danos à sua imagem pública. A violação da privacidade prevista neste artigo é punível com pena de prisão até 1 ano ou multa até 240 dias, mas o grau de penalização aumenta se o crime for cometido por meio de comunicação social, dada a maior exposição e o potencial de danos mais amplos que este meio acarreta.

Finalmente, o artigo 193.º do CP, foca-se em gravações e fotografias ilícitas, criminalizando a captação e a utilização de imagens, vídeos ou gravações de áudio de uma pessoa sem o seu consentimento, em circunstâncias que violem a sua privacidade. A proteção oferecida por este artigo incide particularmente sobre atos que ocorram em locais privados ou de acesso restrito, ou em situações onde sejam captados aspetos da vida íntima de alguém. O facto de uma pessoa ser gravada ou fotografada em situações privadas sem o seu conhecimento ou autorização constitui uma ofensa grave à sua esfera pessoal. A pena prevista para esta conduta é de prisão até 1 ano ou multa até 240 dias, podendo ser agravada até 2 anos de prisão caso as imagens ou gravações sejam divulgadas sem autorização.

Dessa forma, aqueles três artigos exemplificam a preocupação do legislador com a proteção da privacidade no contexto penal, garantindo que atos que interferem com a intimidade e a vida privada das pessoas sejam devidamente punidos.

Ao criminalizar tais condutas, o CP reafirma a importância da privacidade como um direito fundamental, assegurando a tutela da dignidade humana e da liberdade individual, valores essenciais numa sociedade democrática.

A privacidade, neste sentido, torna-se um pilar que sustenta não apenas a vida pessoal, mas também a convivência social, ao criar barreiras jurídicas contra a intrusão indevida na esfera íntima do cidadão.

Assim, os artigos 190.º, 192.º e 193.º do CP demonstram um compromisso claro em proteger a correspondência e a vida privada, reforçando o princípio da inviolabilidade da intimidade e garantindo que as infrações contra este direito sejam efetivamente sancionadas, de forma a preservar a dignidade e os direitos fundamentais dos indivíduos.

No plano constitucional, o sigilo bancário encontra fundamento no direito à intimidade da vida privada e familiar, que está consagrado no artigo 26.º, n.º 1 da CRP. Esta disposição garante que "a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação". Além disso, o art.º 25.º, nº 1, da CRP, ao referir a inviolabilidade da integridade moral das pessoas, também protege a intimidade, já que a sua violação afetaria diretamente a dignidade do indivíduo perante terceiros.

A questão central é que o direito à reserva da intimidade da vida privada e familiar abrange a proteção dos dados bancários dos clientes. O Tribunal Constitucional, no Acórdão n.º 278/95, de 31 de maio (proc. 510/91), reconheceu que os dados relativos às operações bancárias de um cliente revelam aspetos importantes sobre o seu património, que estão inseridos no direito à privacidade. Assim, o sigilo bancário surge como um meio de proteção dessa intimidade. Influenciados pela teoria das esferas, autores como (Habermas,1992, p. 237) e (Brandeis, 1890, p. 195) fazem a distinção entre as diferentes dimensões da privacidade para justificar o sigilo bancário. Para eles, a esfera íntima abrange elementos que devem ser protegidos do escrutínio público, e os dados bancários inserem-se nesta esfera.

Outros, como Marques (2016, p. 89), adotam uma visão mais restrita, argumentando que o sigilo bancário não está diretamente ligado ao direito à intimidade, mas sim à proteção patrimonial, uma vez que a vida económica e profissional não se confundiria com a esfera íntima do indivíduo.

Parte significativa da doutrina defende que o sigilo bancário encontra seu fundamento no direito à intimidade da vida privada. A este respeito, Canotilho e Moreira sublinham que "o direito à intimidade é um direito fundamental que abrange a proteção de informações pessoais, incluindo dados financeiros (CRP, 2007, p. 465). De igual modo, (Miranda e Medeiros), em comentário ao artigo 26.º da CRP, indicam que o sigilo bancário se relaciona diretamente com a esfera privada, sendo esta "um domínio impenetrável sem o consentimento do titular, exceto nos casos expressamente previstos pela lei" (CRP, 2010, p. 310).

Verifica-se que o sigilo bancário é, em grande medida, uma manifestação do direito à intimidade, conforme defendido pela maioria da doutrina e reconhecido em diversos acórdãos judiciais. Costa (2010, p.57) argumenta que o sigilo bancário, como manifestação do direito à intimidade, encontra amparo na proteção constitucional conferida à vida privada, destacando a sua relevância no campo dos direitos fundamentais.

Autores influenciados pela teoria das esferas, como (Jellinek,1905, p. 45), encontram divisões internas no conceito de direito à intimidade, estabelecendo distinções entre a esfera privada, secreta e íntima, sendo que a proteção conferida ao sigilo bancário estaria mais diretamente ligada à esfera secreta, relacionada à vida profissional e económica. (Carvalho, 2004, p. 112) também explora essa divisão, afirmando que o direito à intimidade abrange aspetos diferentes da vida do indivíduo, em que a esfera privada representa um conjunto de interesses mais pessoais e íntimos, enquanto a esfera secreta protege informações que, embora privadas, estão ligadas à vida económica.

Por outro lado, uma minoria doutrinária, representada por autores como Santos (2003, p. 164) não admite que o segredo bancário derive diretamente do direito à intimidade. Segundo essa visão, o segredo bancário teria uma natureza predominantemente patrimonial, uma vez que a intimidade está intrinsecamente ligada à subjetividade do indivíduo, não se estendendo de forma automática à sua vida profissional e económica

Portanto, o segredo bancário goza de proteção em duas frentes: primeiramente, através da tutela da privacidade, como argumentado por Costa, nos termos já expostos. Além disso, o sigilo bancário também visa garantir o desenvolvimento económico-social,

conforme previsto constitucionalmente no artigo 101.º da CRP, que trata das responsabilidades do Estado na promoção do bem-estar social e económico da nação.

1.4. Limites do sigilo bancário na relação jurídico-fiscal: Análise das fronteiras entre a proteção da privacidade financeira e as obrigações de transparência perante as autoridades fiscais

O sigilo bancário tem como objetivo proteger a posição dos clientes nas suas relações com as instituições financeiras, garantindo, por extensão, a privacidade de suas vidas financeiras. No entanto, os interesses privados muitas vezes entram em conflito com o interesse público, especialmente quando há necessidade de levantamento do sigilo para fins de investigação criminal ou fiscalização tributária. Segundo Schwartz (2019, p. 75), esse equilíbrio envolve decisões complexas, em que, frequentemente, prevalece o interesse público em questões de segurança e combate a ilícitos financeiros.

A quebra do sigilo bancário pode ser justificada em situações que buscam combater fraudes fiscais e concorrência desleal, evitando assim a perda de receitas nacionais. Conforme Pais (2016, p. 102), o levantamento do sigilo tem como objetivo permitir uma melhor avaliação da situação fiscal dos contribuintes, assegurando um sistema tributário mais justo e equitativo.

Embora os contribuintes sejam obrigados a fornecer informações regulares e divulgar seus rendimentos, isso não exclui a possibilidade de intervenção da Autoridade Tributária e dos Tribunais Tributários quando houver suspeitas de irregularidades. Segundo Marques (2016, p. 58), a relação entre um cliente e uma instituição financeira pode ser explorada para ocultar práticas fraudulentas ou para evasão fiscal, o que torna necessário um sistema de informações capaz de lidar com tais riscos, preservando a confidencialidade, mas permitindo que a fiscalização atue de maneira eficaz.

O sigilo bancário, ainda que seja uma garantia fundamental na relação entre cliente e instituição financeira, encontra limitações quando confrontado com o interesse público. Mendes (2017, p. 89) defende que, para combater crimes como branqueamento de capitais, financiamento ao terrorismo, corrupção e evasão fiscal, é necessário que as instituições financeiras equilibrem a proteção da privacidade dos seus clientes com a obrigação de cumprir as regulações legais e colaborar em investigações oficiais.

A proteção dos dados financeiros é, assim, entendida como parte do direito à reserva da intimidade da vida privada, abrangendo também os dados de natureza patrimonial. Segundo Andrade (2019, p. 144), o sigilo bancário pode ser considerado um direito constitucional fundamental, protegido pelas disposições relativas aos direitos, liberdades e garantias, conforme previsto no artigo 26.º da CRP.

Além da proteção penal direta oferecida pelos artigos 190.º, 192.º e 193.º do CP, o direito à privacidade e ao sigilo encontra proteção indireta através da CRP, mais especificamente no artigo 17.º da CRP. Este artigo estabelece o regime aplicável aos direitos, liberdades e garantias, conferindo uma base constitucional sólida para a defesa dos direitos fundamentais dos cidadãos, incluindo o direito à privacidade e à inviolabilidade das comunicações. Nesse sentido, este artigo fortalece a proteção dos direitos fundamentais, assegurando que a privacidade e o sigilo das comunicações estejam amparados por um regime jurídico especial, que obriga as autoridades a respeitarem e protegerem esses direitos de maneira rigorosa.

A privacidade é considerada um direito essencial para a dignidade humana e o desenvolvimento da personalidade, e o artigo 17.º reforça esse entendimento ao conferir aos direitos fundamentais uma posição de destaque no ordenamento jurídico português.

O sigilo das comunicações, por exemplo, além de ser tutelado pelas disposições específicas do CP, encontra um suporte implícito na Constituição através deste artigo, que obriga o legislador a salvaguardar os direitos à inviolabilidade da correspondência e das comunicações. Assim, qualquer ingerência indevida sobre esses direitos enfrenta uma barreira jurídica significativa, visto que os direitos à privacidade e ao sigilo são protegidos não apenas por normas penais, mas também pela hierarquia constitucional.

Esta interligação entre a legislação penal e a Constituição reflete o compromisso do Estado português em garantir que os direitos à privacidade e à inviolabilidade das comunicações sejam tratados como princípios fundamentais, sobre os quais repousa a própria estrutura da convivência democrática.

No entanto, a importância das obrigações fiscais não pode ser desconsiderada. A relação entre as autoridades fiscais e os contribuintes deve ser pautada pela segurança jurídica e pela confiança legítima, o que facilita o cumprimento voluntário das obrigações fiscais.

Conforme discute Nogueira (2020, p. 231), o cumprimento voluntário é um dos pilares da justiça fiscal, contribuindo para um sistema tributário mais eficiente e equilibrado.

1.5. O sigilo bancário no âmbito das relações jurídicas fiscais

O sigilo bancário tem sido fonte de grandes controvérsias, pois visa proteger a posição do cliente na relação bancária, garantindo a privacidade de sua vida financeira. Entretanto, ao interesse privado contrapõe-se o interesse público, que, em certas circunstâncias, pode exigir a quebra do sigilo bancário para garantir a fiscalização tributária e prevenir crimes financeiros. A ponderação entre esses interesses é fundamental para determinar qual deles prevalece. De acordo com o artigo 63º-A da Lei Geral Tributária, a ponderação desses valores é crucial para garantir o equilíbrio entre os direitos dos contribuintes e as necessidades de fiscalização do Estado.

O predomínio do interesse público pode implicar a aceitação do sigilo bancário como um instituto de direito público, em defesa dos interesses da coletividade. Por outro lado, a recusa de certos limites ao sigilo, como a abertura das informações bancárias às autoridades fiscais, poderia consagrar o sigilo bancário como um valor superior na proteção da privacidade dos cidadãos. Como apontam Andrade (2019, p. 78) e Gouveia (2018, p. 120), a relação entre sigilo bancário e direito tributário envolve um intrincado balanço entre os direitos individuais e os deveres de supervisão fiscal.

No quadro das relações jurídicas tributárias, que se estabelecem entre a Autoridade Tributária e os contribuintes, é comum que estes também mantenham relações jurídicas financeiras com instituições bancárias, uma vez que são titulares de contas nesses estabelecimentos. De acordo com Cordeiro (2017, p. 45), as instituições financeiras têm o dever legal de preservar a confidencialidade das informações de seus clientes. Isso significa que os bancos estão proibidos de divulgar dados sobre contas bancárias, transações ou outras informações financeiras sem uma autorização legal adequada, exceto quando exista um fundamento jurídico que justifique tal divulgação. O sigilo bancário, portanto, atua como um mecanismo de proteção da privacidade dos clientes, garantindo que suas informações financeiras não sejam acedidas por terceiros sem o seu consentimento explícito.

Contudo, esse direito à privacidade pode representar um obstáculo ao acesso das autoridades fiscais a informações relevantes para investigações tributárias e execuções

fiscais. Nesse sentido, o acesso das autoridades a dados bancários exige o cumprimento de procedimentos legais rigorosos, que balanceiam a necessidade de fiscalização com a proteção dos direitos dos contribuintes (Simas, 2019, p. 98).

As instituições financeiras são reguladas por normas rigorosas que reforçam o sigilo bancário e impõem responsabilidades adicionais no tratamento de informações pessoais, conforme o estabelecido pelo Regulamento Geral sobre a Proteção de Dados (RGPD). Segundo Gouveia (2021, p. 34), as disposições do RGPD são fundamentais para assegurar a integridade e segurança dos dados dos clientes. No entanto, em certas circunstâncias, admite-se a quebra do sigilo bancário quando tal medida é justificada pelo interesse público. O RGPD apresenta normas que, em casos excecionais, permitem essa flexibilização. O artigo 5º define os princípios fundamentais para o tratamento de dados pessoais, como legalidade, lealdade, transparência, integridade e confidencialidade, os quais devem ser observados pelas instituições financeiras. Já o artigo 6º estabelece as bases legais para o processamento de dados, permitindo-o, por exemplo, quando necessário para o cumprimento de uma obrigação legal ou o exercício de funções de interesse público. Além disso, o artigo 23º permite a limitação de certos direitos dos titulares dos dados, incluindo o sigilo bancário, quando essa restrição for necessária para proteger a segurança pública, a defesa nacional ou outros interesses públicos essenciais. Assim, essas disposições refletem o equilíbrio entre a proteção da privacidade dos clientes e a necessidade de, em determinadas situações, permitir o acesso ou divulgação de dados em prol do interesse público.

A quebra do sigilo bancário geralmente exige autorização judicial ou uma ordem formal emitida por autoridade competente, como previsto no artigo 135º do Código de Processo Penal (CPP). Novais (2019, p. 56) discute que as autoridades fiscais só podem aceder a essas informações se houver um fundamento jurídico sólido, de modo a não violar os direitos dos clientes.

A confiança dos clientes é vital para as instituições financeiras, que podem ser relutantes em compartilhar informações sem justificativa legal clara. Segundo Garoupa (2020, p. 101), a perceção de que o sigilo bancário está sendo enfraquecido pode minar a confiança no sistema bancário, prejudicando tanto as instituições quanto os seus clientes. Em resumo, o sigilo bancário representa um desafio no contexto das relações fiscais, uma vez que protege a privacidade e a confidencialidade das informações financeiras dos clientes,

enquanto cria obstáculos para a fiscalização e a prevenção de crimes financeiros. Como sublinham Gouveia (2018, p. 122) e Cordeiro (2020, p. 74), o equilíbrio entre a proteção dos direitos individuais e as exigências da administração fiscal é essencial para garantir a integridade do sistema financeiro e a justiça tributária.

Para levantar o sigilo bancário, geralmente é necessária autorização, como uma ordem judicial ou um pedido formal de uma autoridade competente. Como discute Marcelo Rebelo de Sousa, Presidente da República, em um discurso, sem uma base jurídica adequada, as autoridades fiscais enfrentam dificuldades para ceder dados financeiros. (Site da Presidência da República Portuguesa,2019).

Capítulo 2. A evolução do sigilo bancário em Angola e Portugal na era digital

Um dos países que necessita de um estudo aprofundado e uma melhor atenção é Angola, um país em fase de desenvolvimento e que carece de diversas ferramentas para o combate a quebra do sigilo bancário e às questões fiscais em desenvoltura.

Angola, como um país em desenvolvimento, enfrenta desafios significativos na gestão e proteção do sigilo bancário e das questões fiscais. O sigilo bancário em Angola, conforme estabelecido pela Lei de Bases das Instituições Financeiras, Lei n.º 13/05, de 30 de setembro de 2005, garantiu a confidencialidade das informações sobre transações financeiras, valores mobiliários e operações realizadas por instituições financeiras. Este princípio visa proteger tanto os interesses dos consumidores quanto os das instituições financeiras, assegurando uma abordagem ética e segura no tratamento de dados financeiros. No entanto, o sigilo bancário não é absoluto; ele pode ser suspenso em casos específicos relacionados ao combate à corrupção, ao branqueamento de capitais, à evasão fiscal e ao financiamento ao terrorismo. Essa possibilidade de suspensão foi reafirmada pela legislação atual, que inclui a Lei n.º 14/21, de 19 de maio de 2021, que substituiu a Lei n.º 13/05 e introduziu atualizações importantes no enquadramento legal do sistema financeiro angolano.

O Banco Nacional de Angola (BNA) desempenha um papel crucial na regulamentação do sistema financeiro, estabelecendo diretrizes e procedimentos que visam prevenir crimes financeiros e garantir a integridade do setor. Entre as principais obrigações impostas pelo BNA, destaca-se o cumprimento das normas de "Conheça o Seu Cliente" (KYC) *Know your customer*. Essas normas exigem que as instituições financeiras realizem a identificação e verificação da identidade de seus clientes, incluindo titulares de contas e beneficiários finais. Para isso, é necessário que sejam coletados documentos de identidade válidos, e, em casos onde o cliente apresenta maior risco, como pessoas politicamente expostas (PEPs), é exigida uma diligência devida ampliada. Esta diligência envolve uma verificação mais rigorosa das fontes de renda e um monitoramento contínuo das transações para identificar quaisquer padrões suspeitos.

Além das obrigações de identificação, as instituições financeiras são obrigadas a comunicar operações suspeitas ao Gabinete de Informação Financeira (GIF) de Angola. Este relatório, conhecido como Relatório de Operações Suspeitas (ROS), deve ser apresentado sempre que houver indícios de branqueamento de capitais, financiamento ao

terrorismo ou outras atividades ilícitas. A legislação prevê também que transações em dinheiro que ultrapassem certos limites estabelecidos pela regulamentação devem ser reportadas, visando aumentar a transparência e a responsabilização no sistema financeiro.

Essas obrigações estão normatizadas em regulamentos, como o Aviso n.º 22/12, de 25 de maio de 2012, que especifica os procedimentos para a identificação de clientes e a comunicação de operações suspeitas. Além disso, as diretrizes do BNA estão alinhadas com as recomendações internacionais do Grupo de Ação Financeira Internacional (GAFI), que orienta os países a adotarem práticas rigorosas para prevenir o branqueamento de capitais e o financiamento ao terrorismo. As recomendações do GAFI incluem a realização de uma avaliação de risco adequada, a implementação de medidas preventivas, a garantia de transparência em relação aos beneficiários finais e a aplicação efetiva de sanções financeiras contra atividades ilícitas.

Portanto, o sistema financeiro angolano está em constante evolução, buscando adequar-se às exigências internacionais e fortalecer suas medidas de controle e supervisão. Essa evolução visa não apenas proteger o sigilo bancário, mas também garantir a eficácia e a segurança do sistema financeiro, promovendo um ambiente mais transparente e íntegro para as instituições e consumidores.

2.1. Impacto das normas internacionais sobre sigilo bancário em Angola

Angola enfrenta desafios únicos na transição para a era digital, particularmente no que diz respeito ao sigilo bancário. A falta de uma infraestrutura tecnológica robusta e a limitada penetração da internet no país são obstáculos ao desenvolvimento de serviços bancários digitais. Além disso, a ausência de uma legislação específica que regule a proteção de dados pessoais, como o RGPD na UE, expõe os bancos angolanos a maiores riscos de violações de privacidade e ciberataques (Fernandes, 2021, p.60).

Nos últimos anos, o sigilo bancário tem sofrido pressões significativas, particularmente devido às normas internacionais que visam combater a evasão fiscal e o branqueamento de capitais. Com o aparecimento do *Common Reporting Standard* (CRS) da Organização da Cooperação e Desenvolvimento Económico (OCDE), introduzido em 2014, como objetivo principal facilitar a troca automática de informações financeiras entre as jurisdições participantes. Portugal, como Estado membro da UE e da OCDE,

implementou o CRS em 2016, o que levou a uma maior flexibilidade na quebra de sigilo bancário quando solicitado por autoridades fiscais estrangeiras.

Em contraste, Angola, embora tenha feito esforços para harmonizar as suas práticas financeiras com as normas internacionais, ainda não aderiu ao CRS. Isso pode ser visto como uma limitação no combate à evasão fiscal e o branqueamento de capitais no país. Entretanto, a Lei n.º 16/10, de 15 de julho, do BNA que regula o branqueamento de capitais, exige maior transparência por parte das instituições financeiras, o que pode ser visto como um movimento em direção à convergência com as normas internacionais.

Segundo Gomes (2022, pp. 102 e108), a implementação dessas normas internacionais em Portugal tem causado um aumento na cooperação entre jurisdições, enquanto em Angola, a falta de adesão ao CRS ainda constitui um obstáculo para uma integração total no sistema financeiro internacional.

Embora a Lei n.º 12/2015, de 17 de junho, do BFA tenha estabelecido algumas bases para a proteção do sigilo bancário, a sua aplicação no contexto digital é limitada. Fernandes (2021, pp. 60 e 67) sugere que Angola precisa adotar medidas legislativas mais rígidas para acompanhar a crescente digitalização do setor bancário, a fim de garantir a segurança das informações dos clientes.

2.2. Garantias penal e processual penal dos direitos do sigilo bancário em Angola

Em termos jurídicos o dever de segredo bancário começa por se apoiar na CRA, como expressão do direito fundamental à intimidade da vida privada, isto é, da privacidade pessoal e patrimonial de cada indivíduo, consagrado no artigo 32.º da CRA. É igualmente expressão do direito à integridade moral das pessoas previsto no artigo 31.º da CRA.

Não obstante, a lei prevê disposições que permitem a quebra do segredo bancário em determinadas circunstâncias relacionadas com a prevenção do crime financeiro na CRA (artigo 32.º).

O sigilo bancário não é, portanto, absoluto, sendo derrogável por interesses ou razões de cariz público ou privado, concretamente justificáveis, quer em sede do Direito Público, designadamente do Direito Penal, do Direito Fiscal, quer em sede do Direito Privado, designadamente, do Direito Civil e Direito Comercial (Afonso, 2022, p.40).

Da mesma forma, como ocorre em Portugal, as violações ao sigilo bancário em Angola são puníveis de acordo com o Código Penal, o Código Civil, o Código Geral do Trabalho e a legislação bancária pertinente. (Lei n.º 16/10 De 15 de Julho)

Contudo, o sigilo bancário não é absoluto e pode ser levantado em situações excecionais (Holanda, 2006, p. 54). Conforme previsto na lei, essa quebra pode ocorrer por decisão judicial, a pedido do cliente, ou por decisão do Governador do Banco Nacional de Angola, conforme o artigo 96, n.º 2, da (Lei n.º 16/10, de 15 de julho).

Portanto, o levantamento do sigilo em determinadas circunstâncias, especialmente no âmbito de investigações relacionadas ao combate ao branqueamento de capitais e ao financiamento do terrorismo. O n.º 3 do artigo 96 da Lei n.º 16/10, de 15 de julho, estabelece que as autoridades competentes têm o direito de aceder a informações bancárias sempre que seja necessário para a investigação desses crimes. Esta disposição jurídica visa facilitar a atuação das autoridades judiciais e administrativas no rastreamento de atividades ilícitas e garantir a transparência das operações financeiras, mesmo que isso implique a suspensão temporária do sigilo bancário.

Além disso, o combate ao branqueamento de capitais e financiamento do terrorismo consagrado na Lei n.º 34/11, de 12 de dezembro, consolidou este quadro normativo ao reforçar as obrigações de reporte de transações suspeitas e ao criar mecanismos de monitorização para instituições financeiras, tornando possível o acesso a dados sigilosos em casos de investigações de crimes económicos. Rodrigues (2015, p.89) salienta que esta legislação representou uma importante evolução no tratamento do sigilo bancário em Angola, ao criar uma base legal para a troca de informações com autoridades internacionais. Cardoso (2017, p.147) acrescenta que este levantamento do sigilo é uma medida crucial para assegurar o combate eficaz ao crime organizado, fortalecendo a cooperação internacional.

A Lei n.º 34/11, de 12 de dezembro, de Combate ao Branqueamento de Capitais e Financiamento do Terrorismo, faz parte de um conjunto de medidas destinadas a enfrentar o crime económico, adaptando-se aos padrões internacionais recomendados pelo Grupo de Ação Financeira Internacional (GAFI). Através desta legislação, o conceito de sigilo bancário foi reformulado, permitindo uma maior flexibilidade para a obtenção de informações financeiras em investigações criminais. Como destaca Silva (2013, p.112),

esta mudança foi essencial para que Angola adotasse práticas mais eficazes no combate ao branqueamento de capitais e financiamento ao terrorismo, alinhando-se com as exigências da globalização e da cooperação internacional, especialmente no intercâmbio de informações entre países, o que é fundamental para rastrear e interromper redes criminosas que operam em nível global.

No entanto, sanções rigorosas são aplicáveis nos casos de violação do sigilo bancário por parte de trabalhadores de instituições bancárias, constituindo uma infração grave que pode até resultar em despedimento, conforme previsto no artigo 96.º, nº 3, da Lei n.º 16/10 de 15 de julho. A proteção jurídica e criminal do sigilo bancário em Angola é constitucionalmente e legalmente amparada, sujeitando o infrator a sanções rigorosas, com exceções específicas previstas na legislação aplicável.

Adicionalmente, a Lei das Instituições Financeiras (Lei n.º 12/2015, de 17 de junho) estabelece um quadro jurídico abrangente para as instituições financeiras, contendo disposições específicas sobre o sigilo bancário. Nos seus artigos 20.º e 88.º, a lei afirma que as instituições financeiras devem manter a confidencialidade de todas as informações recebidas no exercício das suas funções, exceto nos casos expressamente previstos na legislação.

2.3. Problemas do sigilo bancário nas relações jurídicas com os clientes

A análise do sigilo bancário envolve uma tensão entre a necessidade de proteger a privacidade financeira dos indivíduos e o interesse público em garantir transparência, especialmente em investigações criminais ou na regulação do sistema financeiro. A seguir, são discutidos alguns dos principais problemas relacionados a esse tema, com base em autores relevantes e na legislação aplicável.

A quebra de sigilo bancário ocorre quando há a divulgação não autorizada de informações financeiras de clientes por instituições bancárias, seja por negligência ou violação intencional, configurando uma violação da privacidade financeira protegida por leis e pelo RGPD na UE. De acordo com Pinheiro (2019, p. 67), a quebra de sigilo sem autorização judicial ou fora das exceções legais constitui uma violação dos direitos à privacidade e intimidade, que são protegidos por diversas legislações internacionais. Cunha (2020, p. 45) destaca que, embora o sigilo bancário seja um direito fundamental do cliente, ele não é absoluto. Exceções como investigações criminais ou ações fiscais

podem justificar a sua quebra, desde que amparadas por decisão judicial, para evitar abusos.

O aumento das violações de segurança cibernética coloca em risco os dados bancários de clientes, expondo-os ao roubo de identidade e fraude financeira. Segundo Gonçalves e Pinho (2020, p. 123), os bancos têm sido alvos recorrentes de ataques cibernéticos, impulsionados pela crescente digitalização dos serviços financeiros. A violação de dados, especialmente quando envolve informações bancárias, é considerada uma das mais graves ameaças à privacidade financeira e pode resultar em ações judiciais contra as instituições, caso falhas nas medidas de proteção sejam comprovadas.

A utilização não autorizada de informações financeiras por trabalhadores bancários ou terceiros é uma das violações mais graves de confiança. Almeida (2018, p. 89) observa que fraudes internas, onde trabalhadores têm acesso privilegiado a dados de clientes, representam um risco constante nas operações bancárias. Isso é exacerbado quando o consentimento para o uso de dados é mal obtido ou não compreendido adequadamente pelos clientes.

O consentimento dos clientes para o uso de seus dados deve ser livre e informado, de acordo com o artigo 7.º do RGPD. Este artigo estabelece que o consentimento deve ser dado de forma livre, sem pressões ou constrangimentos; específico, referindo-se a finalidades claras; informado, com o cliente plenamente ciente de como os seus dados serão utilizados; e inequívoco, demonstrado por uma ação afirmativa clara por parte do titular dos dados. Além disso, o n.º 2 do artigo 7.º exige que o responsável pelo tratamento dos dados tenha a capacidade de provar que o consentimento foi dado de maneira adequada, enquanto o n.º 3 assegura ao titular o direito de retirar o consentimento a qualquer momento.

No entanto, situações em que o consentimento é obtido sem que o cliente compreenda totalmente suas implicações levantam dúvidas sobre a validade legal desse consentimento. Lima (2021, p. 56) argumenta que a falta de clareza nas políticas de privacidade e nas práticas de obtenção de consentimento pode abrir brechas para abusos, potencialmente levando a disputas judiciais. A ausência de transparência nas explicações fornecidas ao titular dos dados pode comprometer a legalidade do consentimento,

especialmente quando este não foi verdadeiramente livre ou informado, conforme exige o RGPD.

Disputas entre clientes e bancos sobre a divulgação ou armazenamento de dados financeiros são frequentes, especialmente em investigações criminais. Segundo Araújo (2018, p. 134), essas disputas refletem o conflito entre o direito à privacidade e o dever de cooperação com as autoridades judiciais. A ausência de normas claras pode resultar em interpretações divergentes, gerando litígios prolongados.

A legislação sobre sigilo bancário em Angola e Portugal, como observado por Sousa (2017, p. 49), é complexa e, muitas vezes, ambígua. A sobreposição de normas nacionais e internacionais, aliada à constante evolução dos regulamentos sobre proteção de dados, cria desafios para a conformidade por parte das instituições financeiras. Ferreira (2019, p. 78) aponta que a implementação eficaz de mecanismos de proteção é cara e, frequentemente, insuficiente para acompanhar a sofisticação dos crimes cibernéticos.

A confiança dos clientes nas instituições financeiras é abalada quando ocorrem quebras de sigilo. Rodrigues (2019, p. 102) argumenta que essa confiança é a base das relações bancárias e que falhas na proteção de dados podem ter consequências graves, incluindo a perda de clientes e ações judiciais.

Por fim, Martins (2018, p. 92) salienta que os bancos possuem responsabilidade fiduciária e legal sobre as informações de seus clientes. No entanto, esse dever de sigilo entra frequentemente em conflito com a obrigação de cooperação em investigações criminais e fiscais, criando um dilema que muitas vezes resulta em disputas jurídicas sobre até que ponto as instituições podem proteger os dados dos clientes sem violar a lei.

2.4. Desafios do sigilo bancário na transformação da era digital em Angola e Portugal

O sigilo bancário em Portugal é regido por um conjunto de normas que evoluíram ao longo do tempo para acompanhar a crescente complexidade do sistema financeiro e a necessidade de proteção dos dados pessoais. Inicialmente, o sigilo bancário era regulado pela Lei nº 10/91, de 29 de abril, alterada pela Lei nº 28/94, de 29 de agosto. Posteriormente, este regime foi substituído pelo Decreto-Lei nº 67/98, de 26 de outubro, que transpôs para o direito interno a Diretiva 95/46/CE do Parlamento Europeu de 23 de

novembro de 1995 e do Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Os elementos protegidos pelo sigilo bancário estão armazenados em arquivos automatizados e bases de dados pessoais, supervisionados pela Comissão Nacional de Proteção de Dados (CNPD). Conforme Cordeiro (1999, p. 27) salienta, a criação e atualização desses dados sem a devida autorização dos clientes é regulada pela CNPD, que atua sob a tutela da Assembleia da República. A legislação portuguesa, no que se refere à proteção de dados pessoais e à privacidade no setor das comunicações eletrónicas, foi harmonizada com as imposições europeias, tendo sido alvo de várias reformas para acompanhar a evolução tecnológica e as exigências internacionais.

A Lei n.º 41/2004, de 18 de agosto, transpôs para o direito interno a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002. Esta diretiva, conhecida como a Diretiva da Privacidade e Comunicações Eletrónicas, estabeleceu um conjunto de normas para o tratamento de dados pessoais e a proteção da privacidade nas comunicações eletrónicas que regulou o uso de *cookies*, o *marketing* direto e a segurança dos dados transmitidos nas redes de telecomunicações, garantindo que o tratamento de dados pessoais no contexto das comunicações eletrónicas fosse efetuado de forma segura e com o consentimento informado dos utilizadores.

Posteriormente, esta legislação foi alterada pelo Decreto-Lei n.º 46/2012, de 29 de agosto, que adaptou o ordenamento jurídico nacional à Diretiva 2009/136/CE, do Parlamento Europeu e do Conselho, de 25 de novembro de 2009. Esta última diretiva introduziu importantes alterações na Diretiva 2002/58/CE, especialmente no que diz respeito ao reforço da proteção da privacidade dos utilizadores. Entre as mudanças mais significativas está a exigência de maior transparência no uso de tecnologias de rastreamento, como *cookies*, estabelecendo que os utilizadores devem ser devidamente informados e ter a possibilidade de recusar a sua utilização. A diretiva também abordou a necessidade de notificação de violações de dados pessoais às autoridades competentes e aos próprios titulares dos dados, promovendo uma maior segurança e responsabilidade no tratamento da informação pessoal.

Essas adaptações legais, baseadas nas diretivas da UE, são fundamentais para assegurar que o tratamento de dados pessoais, incluindo aqueles abrangidos pelo sigilo bancário,

seja feito de acordo com normas internacionais de proteção de dados e privacidade. Sob a supervisão da CNPD, a aplicação dessas normas garante que os direitos dos titulares dos dados sejam respeitados, em particular no que concerne ao consentimento informado e à proteção da privacidade nas comunicações eletrónicas.

De acordo com Cordeiro (1999, p. 27), o sigilo bancário desempenha um papel crucial na confiança do sistema financeiro, sendo essencial para a proteção dos direitos dos clientes e para a estabilidade das operações bancárias. Gouveia (2008, p. 134) destaca que a legislação deve ser harmonizada para garantir que o direito à privacidade, um pilar fundamental da regulação moderna, seja devidamente protegido.

A era digital, iniciada na segunda metade do século XX, refere-se ao período em que as tecnologias digitais começaram a transformar a sociedade de maneira global e permanente. O conceito de era digital foi popularizado pela crescente utilização de computadores, a internet e dispositivos móveis que tornaram a informação amplamente acessível e o fluxo de dados quase instantâneo. Negroponte (1995, p. 12), na sua obra *Being Digital*, argumenta que a digitalização revolucionou não apenas a comunicação e o armazenamento de dados, mas também a forma como as transações financeiras e os relacionamentos empresariais são conduzidos. Com a digitalização, o sigilo bancário enfrenta novos desafios, já que a proteção das informações bancárias passa a depender de cibersegurança e de regulamentações adequadas para impedir vazamentos ou acessos não autorizados.

Com o crescimento exponencial das transações financeiras *online* e a migração de dados para sistemas digitais, a cibersegurança tornou-se uma preocupação central. Segundo Schneider (2018, p. 122), especialista em segurança digital, a complexidade crescente dos ataques cibernéticos exige que as instituições financeiras adotem medidas robustas de proteção de dados para evitar a violação de informações confidenciais dos clientes. O RGPD reforça esta necessidade, impondo às instituições financeiras europeias a adoção de uma postura proativa para garantir a conformidade com normas de privacidade rigorosas, como destaca Solove (2024, p. 63).

O surgimento das criptomoedas e da tecnologia *blockchain* está revolucionando o conceito de sigilo bancário. O *blockchain* é uma tecnologia de registo distribuído que permite armazenar informações de forma segura e descentralizada, sem a necessidade de

uma autoridade central. Cada transação é registada em um bloco de dados que, uma vez validado, é adicionado a uma cadeia de blocos anteriores, formando o que se chama de *blockchain*. De acordo com Tapscott (2016, p. 45), a transparência inerente ao *blockchain* contrasta com o anonimato prometido por algumas criptomoedas, como o *Bitcoin*, o que levanta questões sobre como equilibrar o sigilo das transações com a necessidade de rastreabilidade e segurança. Apesar do *blockchain* proporcionar transparência nas transações, pode também comprometer o sigilo bancário, dependendo da forma como os dados são estruturados e acedidos na rede.

O uso de *big data* no setor bancário, para inferir padrões de comportamento dos clientes, oferece vantagens competitivas, mas levanta preocupações sobre privacidade. O'Neil (2016, p. 89) alerta sobre os perigos do uso de algoritmos preditivos, que podem ser explorados para manipulação ou discriminação, se não forem regulados de forma eficaz. O uso intensivo de dados também exige cuidados para não violar o sigilo bancário e os direitos dos clientes à privacidade.

A crescente interconexão entre serviços financeiros digitais, como aplicativos de pagamento e plataformas de *crowdfunding*, cria riscos para a proteção do sigilo bancário. Carr (2008, p. 201) ressalta que a digitalização global dos serviços financeiros exige que as instituições reformulem suas práticas de segurança para proteger dados em um ambiente cada vez mais integrado e acessível.

A terceirização de serviços financeiros para fornecedores externos é uma prática comum, mas o compartilhamento de dados com terceiros pode aumentar o risco de violação de sigilo bancário. Naughton (2017, p. 58) alerta que as instituições devem implementar acordos rigorosos de compartilhamento de dados e aderir a protocolos de segurança que garantam que seus parceiros sigam os mesmos padrões de proteção de dados.

A procura por serviços personalizados e experiências bancárias aprimoradas levou as instituições a coletarem e utilizarem mais informações pessoais. O desafio está em encontrar o equilíbrio entre a personalização dos serviços e o respeito pela privacidade. Zuboff (2019, p. 296) destaca que o uso excessivo de dados pode resultar em vigilância desnecessária e invasiva, comprometendo o sigilo bancário.

Os desafios trazidos pela era digital obrigam as instituições financeiras e os reguladores a se adaptarem continuamente às mudanças tecnológicas e às novas expetativas dos

consumidores. O sigilo bancário, um pilar fundamental da confiança no setor financeiro, enfrenta pressões significativas com a crescente digitalização e a evolução das tecnologias de informação. A abordagem para proteger a privacidade dos clientes deve evoluir para acompanhar as ameaças emergentes e as transformações no cenário financeiro, garantindo que o sigilo bancário seja preservado na era digital.

2.5. Privacidade financeira na era das Criptomoedas *e bitcoin*

Com o advento da *bitcoin* e de outras criptomoedas, surgem novas dinâmicas que desafiam as noções tradicionais de sigilo bancário. A *bitcoin*, em particular, é uma moeda digital descentralizada que permite transações *peer-to-peer*, ou ponto a ponto, onde os participantes trocam diretamente entre si, sem a necessidade de intermediários financeiros, como bancos ou instituições tradicionais (Nakamoto, 2008, p. 3).

As transações em *bitcoin* não são totalmente anónimas, mas pseudónimas. Isto significa que a identidade do utilizador é protegida pelo endereço da carteira digital, contudo, todas as transações são registadas publicamente no *blockchain*, oferecendo um nível de transparência e rastreabilidade. Meiklejohn et al. (2013, p. 17) destacam que, embora o pseudoanonimato proteja a identidade pessoal, a acessibilidade pública do registo cria possibilidades de ligação entre identidades digitais e informações pessoais, comprometendo a privacidade total.

A *bitcoin* também elimina a necessidade de intermediários financeiros. Como afirmado por Nakamoto (2008, p. 1), o principal objetivo da *bitcoin* é permitir pagamentos diretos entre partes, removendo a necessidade de uma entidade central para prevenir a duplicação de gastos. Este modelo rompe com o paradigma do sigilo bancário tradicional, em que as instituições financeiras têm a obrigação de proteger a privacidade dos seus clientes.

A natureza descentralizada da *bitcoin* coloca desafios significativos para os reguladores. Sem uma autoridade central, torna-se difícil aplicar leis relacionadas ao sigilo bancário e à supervisão de transações financeiras. Narayanan et al. (2016, p. 73) salientam que a transparência do *blockchain* cria um dilema entre a privacidade financeira e a necessidade de combater crimes financeiros, como o branqueamento de capitais e o financiamento de atividades ilícitas.

Embora a *bitcoin* ofereça um nível de privacidade, também atrai utilizadores envolvidos em atividades ilegais, como branqueamento de capitais e evasão fiscal. O relatório da Europol (2021, p. 45) sublinha como criminosos se aproveitam da dificuldade de rastrear transações sem intermediários para realizarem operações ilegais. Isto coloca em evidência as limitações do modelo descentralizado em garantir uma supervisão eficaz.

Por fim, a natureza pública do *blockchain* levanta preocupações sobre a proteção de dados. Todas as transações são visíveis para qualquer pessoa com acesso ao *blockchain*, o que pode colocar em risco a privacidade dos utilizadores, especialmente se os seus endereços digitais forem associados a identidades reais através de correlações com outras informações (Europol, 2021, p. 47).

Em suma, o surgimento da *bitcoin* e de outras criptomoedas desafia as noções tradicionais de sigilo bancário. Embora estas tecnologias ofereçam oportunidades, como o controlo pessoal sobre finanças, apresentam também desafios consideráveis, tanto em termos de privacidade dos utilizadores como para os reguladores que tentam aplicar as leis vigentes.

2.6. A relação da evasão fiscal e o sigilo bancário

O sigilo bancário é um princípio legal que protege a confidencialidade das informações financeiras dos clientes mantidas por instituições financeiras. Historicamente, este princípio foi utilizado como meio de resguardar a privacidade dos indivíduos, mas também pode ser explorado indevidamente para facilitar a evasão fiscal, permitindo que indivíduos ocultem as suas transações financeiras das autoridades competentes. Diversos estudos e autores, como Zucman (2015, p. 45) e Sharman (2017, p. 87), abordam o uso de jurisdições com leis restritivas de sigilo bancário para evitar o pagamento de impostos.

Uma das formas mais comuns de evasão fiscal facilitada pelo sigilo bancário envolve a ocultação de rendimentos não declarados. Indivíduos podem recorrer a contas secretas ou em paraísos fiscais (*offshore*) para esconder esses rendimentos, evitando que as autoridades fiscais descubram transações que, de outra forma, seriam tributáveis (Zucman, 2015, p. 52).

A confidencialidade dessas transações financeiras permite que os envolvidos não apenas escondam os seus ativos, mas também evitem a aplicação de tributos, um ponto central na análise de Picciotto (1999, p. 110) sobre a relação entre finanças globais e a tributação.

Outro ponto relevante é a realização de transferências e transações não registadas em contas bancárias secretas. Este procedimento impede que as transações sejam devidamente comunicadas às autoridades, criando um ambiente propício para a movimentação de fundos sem deixar rastros fiscais. Nesse sentido, autores como Palan, Murphy e Chavagneux (2010, p. 65) destacam a importância dos paraísos fiscais na facilitação de práticas de evasão fiscal, muitas vezes invisíveis aos sistemas regulatórios convencionais.

A evasão fiscal internacional é facilitada em jurisdições com elevado grau de sigilo bancário, que são comumente referidas como paraísos fiscais. Estes países possuem leis de divulgação financeira extremamente restritivas, permitindo que contribuintes transfiram os seus fundos para essas regiões com o objetivo de esconder as suas riquezas e evitar o pagamento de impostos.

Exemplos clássicos de paraísos fiscais incluem as Ilhas Cayman, que se destacam por não cobrarem impostos sobre rendimentos corporativos e pessoais, atraindo assim uma grande quantidade de capital. A Suíça também é frequentemente mencionada nessa categoria devido ao seu rigoroso sigilo bancário, que permite que indivíduos e empresas mantenham contas não identificadas (Zucman, 2015, p. 45). Outro exemplo é o Luxemburgo, famoso por suas leis fiscais favoráveis e a baixa tributação sobre rendimentos, tornando-se um destino preferido para multinacionais que buscam otimizar suas obrigações fiscais (Piketty, 2014, p. 220).

Singapura é uma jurisdição que combina uma economia robusta com um ambiente regulatório estável, oferecendo baixa tributação sobre rendimentos e leis de sigilo bancário que atraem investidores de todo o mundo (Sullivan, 2019, p. 112). O Panamá destaca-se por seu sistema *offshore* e por permitir que indivíduos mantenham a privacidade de suas contas bancárias, além de ter um regime fiscal vantajoso, sendo um exemplo notório no escândalo dos *Panama Papers* (Baker, 2016, p. 76).

As Bermudas são conhecidas por não cobrarem impostos sobre renda ou ganhos de capital, enquanto as Ilhas Virgens Britânicas atraem empresários com a ausência de imposto de rendimento, favorecendo a formação de empresas offshore e a manutenção de ativos (Hines, 2010, p. 34). Além disso, o Mônaco, famoso por não cobrar imposto de

rendimento pessoal e por seu sigilo bancário, tem atraído muitos milionários e investidores em busca de privacidade financeira.

Por fim, as Ilhas do Canal, como Jersey e Guernsey, possuem sistemas fiscais que favorecem tanto empresas quanto indivíduos, oferecendo sigilo bancário e uma abordagem regulatória flexível (Sharman, 2017, p. 89). O uso do sigilo bancário em jurisdições estrangeiras, como explorado por Sharman, torna-se uma ferramenta essencial para garantir a privacidade em transações que podem ser consideradas suspeitas, dificultando a supervisão fiscal e legal. Assim, a combinação de legislação favorável e sigilo bancário nessas jurisdições promove um ambiente propício para a evasão fiscal.

O sigilo bancário também complica a transparência em estruturas financeiras complexas, como empresas de fachada e fundos fiduciários. O estudo de Zucman (2015, p. 61) sobre paraísos fiscais argumenta que essas estruturas dificultam a deteção de atividades suspeitas ou ilegais pelas autoridades fiscais, obscurecendo a verdadeira natureza das transações e dos ativos envolvidos. Isto representa um desafio considerável para os sistemas de regulação internacional, que dependem da cooperação e troca de informações entre países.

Além disso, o sigilo bancário limita a supervisão eficaz das atividades financeiras dos contribuintes. A falta de acesso a informações precisas impede as autoridades fiscais de identificar com eficiência atividades de evasão fiscal e, consequentemente, aplicar as leis tributárias de forma eficaz. Segundo Ocampo e Stiglitz (2011, p. 123), a falta de transparência e cooperação entre sistemas bancários internacionais representa um dos maiores obstáculos à justiça fiscal global.

Para combater estes desafios, muitos países adotaram medidas rigorosas de regulamentação e cooperação internacional. Nos últimos anos, iniciativas como a Convenção Multilateral sobre Assistência Mútua Administrativa em Matéria Tributária e o *Common Reporting Standard* (CRS) da OCDE têm incentivado a troca de informações financeiras entre países, facilitando a deteção de práticas de evasão fiscal. Estas regulamentações visam enfraquecer o uso do sigilo bancário para finalidades ilícitas, aumentando a transparência e dificultando a ocultação de ativos.

Em suma, o sigilo bancário tem sido uma ferramenta tanto para proteger a privacidade dos indivíduos quanto para facilitar a evasão fiscal. A literatura sobre o tema, como a de

Zucman, Sharman e Palan, Murphy e Chavagneux, enfatiza a importância de regulamentações internacionais e acordos de cooperação para combater práticas abusivas que tiram proveito deste princípio. A relação entre evasão fiscal e sigilo bancário destaca a necessidade de políticas globais mais eficazes e transparentes para garantir o cumprimento das obrigações fiscais. Assim, os governos devem reforçar as suas legislações para prevenir o uso abusivo do sigilo bancário, garantindo que este não sirva como meio de ocultar atividades ilegais.

A monitorização e fiscalização também desempenham um papel fundamental no combate à evasão fiscal. Com o avanço da tecnologia, as autoridades fiscais podem recorrer à análise de grandes volumes de dados para identificar padrões de transações incomuns, facilitando a deteção de atividades suspeitas. Zucman (2015, p. 70) sugere que a auditoria de contribuintes de alto risco, aliada a investigações profundas, pode ajudar a combater práticas ilegais e fortalecer a capacidade de supervisão dos órgãos reguladores.

Em resumo, combater a evasão fiscal no contexto do sigilo bancário exige uma abordagem abrangente e coordenada, que inclua medidas legais, regulamentares, de monitorização e fiscalização, além de cooperação internacional, educação financeira e a aplicação de incentivos e sanções. Tais medidas devem ser implementadas de forma sincronizada e contínua para assegurar a sua eficácia a longo prazo, conforme defendido por Zucman (2015, p. 73).

2.7. O levantamento do sigilo bancário em Portugal e Angola

Em Portugal, o direito ao sigilo bancário está protegido pelo artigo 26.º, n.º 1, da CRP. Este artigo reconhece a todos os cidadãos o direito à reserva da intimidade da vida privada e familiar, protegendo informações sensíveis, incluindo as de caráter financeiro. O sigilo bancário é um princípio que garante que as informações relacionadas com as contas de particulares ou entidades corporativas sejam mantidas confidenciais pelas instituições financeiras. Estas instituições não podem divulgar tais informações a terceiros sem o consentimento do cliente, exceto em circunstâncias legalmente previstas, como investigações judiciais ou fiscais, conforme estipulado no artigo 63.º da Lei Geral Tributária.

O levantamento do sigilo bancário em Portugal e Angola desempenha um papel crucial na interseção entre a proteção da privacidade individual e a necessidade de combate a crimes financeiros.

Segundo Cordeiro (2017, p. 103), o sigilo bancário em Portugal desempenha um papel essencial na proteção da privacidade dos clientes, sendo uma extensão do direito à privacidade, consagrado pela CRP no artigo 26.º, que garante a proteção da vida privada e dos dados pessoais. No entanto, essa proteção não é absoluta. Existem circunstâncias nas quais o sigilo bancário pode ser levantado, especialmente quando outros interesses públicos relevantes se sobrepõem à necessidade de privacidade.

O Supremo Tribunal de Justiça, em diversas decisões, tem reiterado que o levantamento do sigilo bancário só pode ocorrer em situações excecionais, com base em fundamentos sólidos que justifiquem a quebra dessa confidencialidade. Um exemplo claro é o Acórdão n.º 206/13, de 14 de março de 2013 do Diário da República e no *site* da Jurisprudência do Supremo Tribunal de Justiça, no qual o tribunal destacou que a quebra do sigilo bancário deve sempre obedecer ao princípio da proporcionalidade, ou seja, deve ser adequada, necessária e proporcional ao interesse público em causa. Este acórdão reforçou que, embora o sigilo bancário seja um direito fundamental dos clientes, ele não pode ser invocado para obstruir a justiça ou proteger atividades ilícitas. O levantamento do sigilo só pode ocorrer quando há um interesse público preponderante, como em investigações criminais ou fiscais, o que reforça a ideia de que o sigilo bancário não pode ser um obstáculo à investigação de crimes ou à administração da justiça, desde que o seu levantamento seja devidamente justificado e proporcional à gravidade dos fatos em questão.

O artigo 101.º da CRP, estabelece que o sistema financeiro deve ser estruturado de forma a garantir a segurança das poupanças e a aplicação adequada dos meios financeiros para o desenvolvimento económico. Este princípio sublinha o equilíbrio que o legislador português procura alcançar entre a proteção da privacidade dos cidadãos e a necessidade de fiscalização e controlo financeiro pelo Estado. Segundo Gouveia (2020, p. 154), a legislação portuguesa sobre o levantamento do sigilo bancário tem evoluído de modo a responder às exigências internacionais no combate a crimes financeiros. A Lei n.º 83/2017, de 18 de agosto, que estabelece medidas de combate ao branqueamento de capitais e ao financiamento do terrorismo, é um exemplo desse progresso, reforçando as

obrigações das instituições financeiras em matéria de prevenção do branqueamento de capitais e financiamento ao terrorismo, em conformidade com as imposições da EU e as recomendações do Grupo de Ação Financeira Internacional (GAFI).

Em Angola, o regime de sigilo bancário está previsto na Lei das Instituições Financeiras (Lei n.º 12/05, de 23 de setembro), que estipula a confidencialidade das instituições financeiras relativamente às informações dos seus clientes. Contudo, essa confidencialidade pode ser levantada em situações específicas, como por requisição judicial ou no âmbito de investigações relacionadas com crimes financeiros. Almeida Santos (2019, p. 89) afirma que a legislação angolana tem sofrido alterações significativas com o objetivo de alinhar o país às normas internacionais, nomeadamente na prevenção do financiamento ao terrorismo e no combate ao branqueamento de capitais. O BNA tem desempenhado um papel fundamental neste esforço, intensificando as suas atividades de supervisão e promovendo uma maior transparência no setor bancário.

Em Angola, o levantamento do sigilo bancário é regulamentado pela Lei n.º 12/2015, de 17 de junho, conhecida como Lei das Instituições Financeiras. De acordo com o artigo 69.º desta lei, o sigilo bancário só pode ser levantado mediante uma decisão judicial devidamente fundamentada, assegurando a proteção dos direitos dos clientes e o respeito pelo devido processo legal. Essa exigência de autorização judicial visa garantir que o levantamento do sigilo seja feito de forma legítima e proporcional ao interesse público em questão.

Essa medida é frequentemente utilizada em investigações de crimes graves, como corrupção e desvio de fundos, onde o acesso às informações bancárias é crucial para rastrear fluxos financeiros ilícitos. Pinto (2021, p. 131) sublinha que, no contexto das reformas recentes de combate à corrupção, o sigilo bancário tem sido levantado com maior frequência, refletindo o compromisso de Angola em aderir às normas do GAFI. A implementação das recomendações do GAFI tem permitido uma maior flexibilidade por parte das autoridades angolanas no levantamento do sigilo bancário, especialmente em casos de crimes económicos graves, como a corrupção de alto nível.

Portanto, em Angola, o sigilo bancário, embora seja um direito importante que protege a privacidade dos clientes, pode ser quebrado quando há uma necessidade legítima de

investigação, garantindo-se sempre que o procedimento seja respaldado por uma decisão judicial fundamentada e que respeite os direitos fundamentais dos envolvidos.

A evolução dos regimes jurídicos em ambos os países ilustram a tensão entre a proteção da privacidade financeira e a necessidade de combater crimes que afetam a integridade do sistema financeiro. Tanto Portugal quanto Angola têm vindo a adaptar-se a um cenário global em que a cooperação internacional é essencial para o combate à criminalidade financeira. A troca de informações entre jurisdições, facilitada por acordos como a Convenção Multilateral sobre Assistência Mútua Administrativa em Matéria Tributária, tem sido fundamental para o sucesso dessas políticas. Em Portugal, a ratificação da convenção pela Lei n.º 119/2019, de 18 de setembro, reflete o empenho do país em aumentar a transparência financeira.

O sigilo bancário é um princípio fundamental nas relações entre as instituições financeiras e os seus clientes, destinado a proteger a confidencialidade das informações financeiras, conforme detalhado por Sturzenegger (2003, p. 58). De acordo com Becho (2017, p. 96), a proteção dos dados financeiros dos clientes é essencial para manter a confiança no sistema bancário e evitar a exposição indevida de informações privadas. Isso inclui manter em segredo detalhes sobre contas, transações, investimentos e outros dados sensíveis fornecidos pelos clientes às instituições financeiras.

No entanto, o sigilo bancário não é absoluto e pode ser levantado em certas situações, especialmente quando há indícios de práticas ilícitas, como o branqueamento de capitais ou o financiamento do terrorismo. Nesses casos, as instituições financeiras são legalmente obrigadas a colaborar com as autoridades, fornecendo informações para investigações criminais ou por ordem judicial. Sturzenegger (2003, p. 64) também enfatiza que a quebra do sigilo bancário é essencial para que o Estado possa investigar crimes financeiros sem comprometer a integridade do sistema bancário.

Frota (2018, p. 143) complementa que o sigilo bancário não protege apenas os interesses dos bancos e do sistema financeiro, mas também funciona como uma salvaguarda para os consumidores, garantindo que as suas informações não sejam utilizadas de forma indevida ou expostas a terceiros sem o seu consentimento. No entanto, ele observa que, em casos de crimes graves, como corrupção ou evasão fiscal, o direito ao sigilo pode ser legitimamente violado.

Capítulo 3. Jurisprudência e casos em Angola e Portugal

O sigilo bancário é um mecanismo essencial de proteção da privacidade financeira dos indivíduos e empresas, mas, em diversas ocasiões, tem sido levantado para permitir investigações de crimes financeiros. Tanto em Angola quanto em Portugal, os desafios de equilibrar a confidencialidade bancária com a necessidade de combater crimes como a corrupção, o branqueamento de capitais e a evasão fiscal têm gerado casos notáveis.

3.1. Quebra do sigilo bancário no contexto penal português

O sigilo bancário é uma das garantias fundamentais do cliente na relação com as instituições financeiras, assegurando a privacidade sobre informações relativas às suas operações financeiras. No entanto, no âmbito do direito penal, tal garantia não é absoluta e pode ser limitada diante da necessidade de uma investigação criminal eficaz. O acórdão do Tribunal da Relação de Lisboa (n.º 7278/20.1T9LSB) exemplifica o tratamento jurídico desta questão, analisando a interação entre o RGICSF, o CPP e os interesses em conflito. O artigo 135.º do CPP estabelece o regime jurídico aplicável à quebra de sigilo bancário no contexto penal, dividido em duas fases distintas:

3.1.1. Legitimidade da Escusa

Conforme o n.º 2 do artigo 135.º do CPP, a primeira análise foca-se na legitimidade da recusa da instituição bancária ou entidade sujeita a sigilo em fornecer os dados solicitados. Esta fase não avalia ainda o mérito da proteção do sigilo, mas verifica se a escusa se fundamenta adequadamente na legislação vigente, como o artigo 80.º do RGICSF, que protege as informações bancárias mediante o dever de segredo profissional. Cabe ao tribunal de primeira instância decidir sobre esta questão inicial.

3.1.2. Justificação da escusa e o princípio do interesse prevalente e a ponderação de valores

Se a escusa for considerada legítima, a decisão passa para o Tribunal da Relação, que, nos termos do n.º 3 do artigo 135.º, avalia os motivos apresentados pela entidade para justificar a manutenção do sigilo. Nesta etapa, aplica-se o princípio do interesse prevalente, ponderando a gravidade do crime investigado, a relevância das informações

bancárias e os direitos fundamentais em jogo. A quebra do sigilo será ordenada apenas se a sua necessidade for demonstrada como imprescindível para a investigação penal.

No caso do princípio do interesse prevalente, este é essencial na decisão sobre a quebra do sigilo bancário, orientando o tribunal a determinar qual interesse jurídico deve prevalecer no caso concreto. O sigilo pode ser relativizado em nome da descoberta da verdade material, sobretudo em situações que envolvam crimes graves, como abuso de confiança, branqueamento de capitais ou financiamento ao terrorismo.

3.2. Análise de casos concretos

No caso analisado, o Banco de Portugal recusou fornecer dados de responsabilidades de crédito de uma investigada, alegando sigilo bancário conforme o artigo 80.º do RGICSF. Tal escusa foi considerada legítima pelo tribunal de primeira instância. Contudo, o Tribunal da Relação entendeu que as informações solicitadas eram imprescindíveis para apurar a denúncia de abuso de confiança por parte da investigada, cuja conduta poderia configurar crime grave com impacto direto no sistema financeiro. Assim, o interesse público na boa administração da justiça e no exercício do *jus puniendi* prevaleceu sobre a proteção do sigilo bancário. Porém, a decisão final determinou que o sigilo bancário deveria ser quebrado, uma vez que os interesses da investigação penal superaram os motivos apresentados para a proteção do sigilo, reforçando a necessidade de atender aos requisitos processuais e à proporcionalidade na obtenção de provas. Por fim, este regime demonstra o esforço do legislador em compatibilizar os direitos individuais com os interesses coletivos, assegurando que a quebra do sigilo apenas ocorra quando absolutamente necessária para a realização da justiça penal. Acórdão do Tribunal da Relação de Lisboa de 20 de janeiro de 2021 (Processo nº 7278/20.1T9LSB-AL1-3) do Diário da República.

3.2.1 Caso Banco Nacional de Angola (2017)

Em 2017, o Banco Nacional de Angola (BNA) ordenou o levantamento do sigilo bancário de várias instituições financeiras como parte de uma investigação sobre transferências ilegais de fundos para o exterior. As investigações revelaram irregularidades em várias transações bancárias, resultando na recuperação de milhões de dólares que haviam sido

desviados. Segundo Santos (2019, p. 134), este caso representou um marco na luta contra a corrupção em Angola, sublinhando a relevância do levantamento do sigilo bancário para identificar operações financeiras ilícitas.

3.2.2. Operação Resgate (2018)

Em 2018, as autoridades angolanas, no âmbito da Operação "Resgate", realizaram uma série de investigações direcionadas ao combate à corrupção e ao desvio de fundos públicos. O levantamento do sigilo bancário foi uma ferramenta essencial para rastrear transferências suspeitas e identificar os responsáveis pelo desvio de recursos. Segundo Pinto (2020, p. 142), o sucesso desta operação deveu-se à colaboração entre o Banco Nacional de Angola e várias instituições internacionais de supervisão bancária, com ênfase na transparência financeira e na partilha de informações.

3.2.3. Caso BPN (2008)

Um dos casos mais emblemáticos em Portugal foi o colapso do Banco Português de Negócios (BPN) em 2008, que levou a uma investigação em larga escala sobre fraudes financeiras. O levantamento do sigilo bancário de diversos gestores e acionistas foi crucial para expor práticas ilícitas, como o branqueamento de capitais e a evasão fiscal. De acordo com Menezes Cordeiro (2019, p. 215), o caso BPN evidenciou as fragilidades do sistema bancário português, levando a reformas significativas no regime de supervisão e regulação bancária.

3.2.4. Caso Montepio Geral (2016)

Em 2016, as autoridades fiscais portuguesas, em colaboração com o Banco de Portugal, conseguiram o levantamento do sigilo bancário de vários clientes do Banco Montepio Geral no contexto de uma investigação sobre evasão fiscal e fraudes financeiras. Este caso ilustrou como o levantamento do sigilo bancário pode ser utilizado para combater práticas ilícitas e promover a justiça fiscal. Segundo Bacelar Gouveia (2020, p. 178), a ação judicial reforçou o papel das autoridades fiscais e da supervisão bancária em equilibrar a proteção do sigilo com as necessidades de fiscalização.

3.2.5. Caso Banco Espírito Santo Angola (BESA)

Em 2014, o Banco Espírito Santo Angola (BESA), uma subsidiária do Banco Espírito Santo (BES), foi envolvido num escândalo de corrupção e má gestão, com implicações para o sigilo bancário. As investigações conduzidas pelas autoridades angolanas levaram à descoberta de práticas irregulares e violações da confidencialidade bancária, culminando em acusações criminais. O caso revelou o uso indevido de informação financeira e levantou questões sobre a eficácia da legislação bancária angolana em proteger a privacidade dos clientes, enquanto permitiu a descoberta de atividades ilegais.

3.2.6. Caso Operação Marquês

Um dos casos mais emblemáticos em Portugal relacionados com o levantamento do sigilo bancário é a Operação Marquês, uma investigação de grande escala que envolve figuras públicas de renome, incluindo o ex-Primeiro-Ministro José Sócrates. A investigação, que teve início em 2014, está centrada em alegações de corrupção, branqueamento de capitais e outros crimes financeiros. Durante o processo, o sigilo bancário de várias contas foi levantado para permitir às autoridades aceder a informação financeira crítica, essencial para apurar a origem dos fundos e as movimentações associadas aos crimes sob investigação. Este caso ilustra o equilíbrio entre a proteção do sigilo bancário e a necessidade de combater crimes de natureza financeira.

3.2.7. Investigações da Autoridade Tributária e Aduaneira (2017)

Em 2017, a Autoridade Tributária e Aduaneira (AT) de Portugal iniciou uma série de investigações que resultaram no levantamento do sigilo bancário de contribuintes suspeitos de envolvimento em esquemas de fraude fiscal e branqueamento de capitais. Essas investigações foram fundamentais para identificar ativos ocultos e transações internacionais não declaradas. De acordo com Nogueira (2021, p. 233), o uso do levantamento do sigilo bancário permitiu à AT recuperar milhões de euros perdidos para a evasão fiscal.

Entre 2022 e 2023, Portugal registou um aumento nos casos de levantamento do sigilo bancário no âmbito de investigações fiscais e financeiras. De acordo com o Relatório Anual de Atividades da Autoridade Tributária e Aduaneira (AT) de 2023, houve um incremento de 13% nos processos em que foi solicitado o levantamento do sigilo bancário

(AT, 2023, p. 45). Este aumento reflete a intensificação dos esforços para combater a evasão fiscal e o branqueamento de capitais.

O Tribunal Constitucional português, no Acórdão n.º 391/2022, analisou a constitucionalidade do levantamento do sigilo bancário pela administração tributária sem autorização prévia de um juiz. O Tribunal concluiu que, embora o sigilo bancário esteja protegido pelo direito à reserva da intimidade da vida privada (artigo 26.º da Constituição da República Portuguesa), a sua quebra pode ser justificada pelo interesse público na eficácia do sistema tributário, desde que sejam respeitados os princípios da proporcionalidade e da necessidade (Tribunal Constitucional, 2022, p. 12).

Segundo Mendes (2023, p. 87), esta decisão reforça a legitimidade da administração tributária em aceder a informações bancárias para verificar a conformidade fiscal dos contribuintes, equilibrando a proteção da privacidade com a necessidade de combater a fraude e a evasão fiscal.

Portanto, o sigilo bancário continua a ser uma ferramenta essencial para proteger os direitos dos clientes em Angola e Portugal. No entanto, tanto a legislação angolana quanto a portuguesa preveem exceções que permitem o levantamento deste sigilo em determinadas circunstâncias, como em investigações de crimes financeiros. O desafio reside em equilibrar a proteção da privacidade dos clientes com a aplicação da lei e a prevenção de atividades ilegais. Casos como o do BESA em Angola e a Operação Marquês em Portugal demonstram a relevância desta questão, destacando a importância de uma regulamentação eficaz e de uma aplicação criteriosa das exceções ao sigilo bancário.

3.3. Implicações legais e jurídicas em Angola e Portugal

Em ambos os países, o levantamento do sigilo bancário é sempre considerado uma medida excecional, que só pode ser autorizada quando existem indícios claros de crime ou fraude. Segundo Andrade (2020, p. 132), a legislação portuguesa estabelece que o levantamento do sigilo bancário pode ser solicitado por autoridades fiscais, judiciais ou pelo Banco de Portugal, desde que haja um fundamento legal robusto que evite abusos. Em Portugal, esta medida é frequentemente usada em investigações relacionadas com crimes graves, como a corrupção, o branqueamento de capitais e a evasão fiscal, garantindo que apenas em situações legalmente justificadas seja permitida a quebra do sigilo.

Em Angola, a supervisão do Banco Nacional de Angola tem-se tornado mais rigorosa, especialmente após a crise económica e as investigações relacionadas a corrupção de altos trabalhadores do Estado. Conforme Santos (2019, p. 98), as reformas no setor bancário angolano foram intensificadas com o objetivo de combater práticas financeiras ilícitas, como o desvio de fundos públicos e o financiamento de atividades criminosas. Neste contexto, o levantamento do sigilo bancário tem sido uma ferramenta indispensável para as autoridades, permitindo a investigação eficaz de crimes financeiros.

O sigilo bancário em Angola é regulado principalmente pela Lei n.º 12/05, de 23 de setembro, conhecida como a Lei dos Serviços Financeiros. Esta lei estabelece os direitos e obrigações das instituições financeiras no que toca à proteção da informação dos seus clientes, bem como as exceções em que tal sigilo pode ser levantado, como em casos de investigações judiciais ou criminais, sempre com autorização de um juiz.

A Lei n.º 5/2002, de 11 de janeiro, nos seus artigos 2.º, 3.º e 4.º estabelece medidas específicas para o combate ao crime organizado, à corrupção e ao branqueamento de capitais, permitindo, nestes casos, a quebra do sigilo bancário. O Ministério Público pode solicitar a quebra do sigilo em investigações que envolvam crimes graves, como o terrorismo, o tráfico de drogas e o branqueamento de capitais, desde que haja indícios suficientes. Este pedido deve ser autorizado por um juiz competente, garantindo que o levantamento do sigilo seja feito de forma proporcional e justificada. As instituições financeiras são obrigadas a colaborar com as autoridades judiciais e fiscais quando estas solicitam informações no âmbito de um processo legal. A não cooperação pode resultar em sanções graves, incluindo multas e responsabilização criminal.

Esses exemplos demonstram que, embora o sigilo bancário seja fundamental para proteger a privacidade dos clientes, ele deve ser equilibrado com a necessidade de combater crimes financeiros. Tanto em Angola como em Portugal, o levantamento do sigilo bancário tem desempenhado um papel vital na investigação de crimes como a evasão fiscal, a corrupção e o branqueamento de capitais, contribuindo para o reforço da confiança no sistema financeiro.

A legislação relacionada com o combate ao branqueamento de capitais e ao financiamento do terrorismo em Portugal é vasta e baseada em normas nacionais e internacionais. Os principais diplomas incluem:

A Lei n.º 83/2017, de 18 de agosto – Estabelece medidas de combate ao branqueamento de capitais e ao financiamento do terrorismo, transpondo diversas diretivas europeias sobre o tema, como a 4.ª Diretiva (UE) 2015/849, 20 de maio de 2015, pelo Parlamento Europeu e pelo Conselho da União Europeia. Esta lei é a principal peça legislativa em Portugal no que diz respeito à prevenção do branqueamento de capitais e ao financiamento do terrorismo.

A Lei n.º 89/2017, de 21 de agosto – Cria o Regime Jurídico do Registo Central de Beneficiário Efetivo (RCBE), uma medida complementar que visa aumentar a transparência sobre a titularidade das entidades, permitindo identificar as pessoas singulares que detêm o controlo das mesmas.

A Lei n.º 97/2017, de 23 de agosto – Regula a aplicação de medidas restritivas aprovadas pelo Conselho de Segurança das Nações Unidas ou pela União Europeia, em matéria de combate ao terrorismo e à proliferação de armas de destruição maciça.

O Regulamento (UE) 2015/847, do Parlamento Europeu e do Conselho, de 20 de maio de 2015, trata das transferências de fundos no sentido de prevenir, detetar e investigar o branqueamento de capitais e o financiamento do terrorismo.

Além disso, em termos de cooperação internacional, Portugal está vinculado às recomendações do Grupo de Ação Financeira Internacional (GAFI), que estabelece normas globais para o combate ao branqueamento de capitais e financiamento do terrorismo.

Estas legislações integram-se num esforço mais amplo de combate ao crime financeiro, obrigando as instituições bancárias e financeiras a implementar mecanismos rigorosos de verificação de identidade, monitorização de transações suspeitas e reporte obrigatório às autoridades competentes. Portanto, verifica-se a necessidade de Angola melhorar a nível de regulamentação e prática nas ações referente ao sigilo.

3.4. Críticas ao sigilo bancário nas relações jurídicas com os clientes

O sigilo bancário é amplamente reconhecido como um princípio fundamental para a proteção da privacidade dos clientes e para a promoção da confiança no sistema financeiro. No entanto, este princípio enfrenta diversas críticas e desafios no contexto das

relações jurídicas com os clientes. Uma das principais críticas ao sigilo bancário é a facilitação de atividades ilegais, como a evasão fiscal, o branqueamento de capitais, a corrupção e o financiamento do terrorismo. De acordo com Silva (2020, p. 145), a falta de transparência nas transações financeiras pode dificultar a deteção e investigação de tais atividades criminosas.

Além disso, há argumentos que apontam para desigualdades na aplicação da lei. Conforme argumenta Pereira (2018, p. 78), o sigilo bancário pode permitir que indivíduos e organizações com maiores recursos financeiros evitem a deteção e a responsabilização por atividades ilícitas, enquanto indivíduos e organizações com menos recursos podem ser mais suscetíveis a investigações, levando a uma aplicação desigual da lei.

Outro ponto de crítica refere-se à proteção dos interesses privados em detrimento do interesse público. Santos (2019, p. 90) sugere que o sigilo bancário pode representar uma proteção excessiva dos interesses privados dos clientes, comprometendo o interesse público na garantia da aplicação da lei, transparência financeira e justiça fiscal. Esta falta de transparência e responsabilização nas práticas de confidencialidade dos bancos pode, conforme destacado por Oliveira (2021, p. 110), minar a responsabilização das instituições financeiras e dificultar uma supervisão eficaz por parte dos reguladores e do público.

As implicações para a segurança financeira global também são uma preocupação significativa. De acordo com Costa e Almeida (2022, p. 203), o sigilo bancário em certas jurisdições pode permitir que indivíduos e empresas ocultem ativos ilícitos em contas *offshore*, comprometendo os esforços internacionais para combater a evasão fiscal e o branqueamento de capitais, o que pode ter um impacto negativo na segurança financeira global.

Por fim, o sigilo bancário cria uma tensão entre a proteção da privacidade do cliente e a necessidade de garantir a segurança nacional, a aplicação da lei e a prevenção de atividades ilegais. Conforme argumenta Ribeiro (2023, p. 65), esta tensão ressalta a complexidade do debate sobre o sigilo bancário e a necessidade de encontrar um equilíbrio adequado entre a proteção da privacidade do cliente e o interesse público em assegurar transparência e conformidade. Governos e instituições financeiras

frequentemente buscam abordagens regulamentares e tecnológicas para conciliar essas preocupações concorrentes.

3.5. Riscos associados à nova era digital e atuais mudanças

Com a crescente digitalização dos serviços bancários, novos riscos emergiram, incluindo ameaças cibernéticas, violações de dados e o uso indevido de dados pessoais por terceiros. Brynjolfsson e McAfee (2017, p. 67) afirmam que a digitalização, enquanto traz conveniência, também aumenta a vulnerabilidade das instituições financeiras a ataques cibernéticos. *Hackers* podem explorar falhas nos sistemas para obter acesso a informações sensíveis, resultando em fraudes financeiras e roubo de identidade.

Outro risco significativo é o compartilhamento de dados entre instituições financeiras e terceiros, especialmente com a implementação da *Open Banking* em muitas jurisdições. Embora isso estimule inovação e competição, também expõe os dados dos clientes a novos riscos, como o tratamento inadequado por empresas menos regulamentadas ou com menos recursos (Zarsky, 2016, p. 23).

3.5.1. Adequação das legislações às mudanças digitais

As legislações em Portugal e Angola estão-se adaptando gradualmente a nova era digital, mas ainda existem lacunas. O RGPD europeu, que entrou em vigor em 2018, é um exemplo de esforço significativo para atualizar as leis de privacidade e proteger os consumidores na era digital. De acordo com o RGPD, as instituições financeiras são responsáveis por garantir que os dados dos clientes sejam processados de maneira justa e transparente, além de implementar medidas técnicas adequadas para proteger esses dados contra acessos não autorizados (Mersch, 2018, p. 54).

No entanto, como Gomber et al. (2017, p. 102) observam, a aplicação de regulamentos internacionais pode ser inconsistente, especialmente em países em desenvolvimento, onde a legislação de proteção de dados ainda está em fase inicial. Enquanto a Europa e os Estados Unidos avançaram na criação de regulamentações adequadas, muitos países ainda enfrentam desafios para adaptar as suas leis ao rápido avanço da digitalização financeira.

3.6. Desafios futuros

As legislações precisarão evoluir continuamente para acompanhar o rápido desenvolvimento da tecnologia. A inteligência artificial (IA) e o *big data* são exemplos de tecnologias emergentes que, segundo Schatsky et al. (2018, p. 89), podem gerar novos desafios para a proteção de dados. Embora essas tecnologias permitam melhorias na segurança e eficiência, elas levantam questões éticas sobre o uso e a privacidade dos dados coletados, muitas vezes sem o conhecimento total dos consumidores.

As instituições financeiras têm adotado uma série de tecnologias e medidas regulatórias para garantir a privacidade e a segurança dos dados dos clientes, mas os riscos associados à era digital continuam a crescer. Legislações como o RGPD e o *California Consumer Protections Act (*CCPA) oferecem uma estrutura robusta de proteção, mas ainda há lacunas, especialmente em países com legislação menos desenvolvida. Para mitigar esses riscos, será crucial que tanto as instituições financeiras quanto os legisladores continuem a evoluir em resposta aos desafios tecnológicos emergentes.

Homem (2014, p. 214) também contribui para a discussão, afirmando que o sigilo bancário está vinculado ao dever de confidencialidade das instituições financeiras, mas deve ser equilibrado com o interesse público, especialmente no combate a crimes financeiros. Ele aponta que a legislação moderna em várias jurisdições, como Portugal e Brasil, já prevê mecanismos que permitem às autoridades aceder informações bancárias em situações excecionais, respeitando os limites legais e constitucionais.

3.7. Melhorias no sigilo bancário nas relações jurídicas com os clientes

O sigilo bancário nas transações realizadas pelos clientes é um tema de extrema relevância, enfrentando desafios que demandam aprimoramentos para proteger a privacidade financeira dos clientes e promover a transparência e o *compliance* que se refere ao conjunto de práticas, regras e controles internos adotados por uma empresa para assegurar que suas atividades estejam em conformidade com as leis, regulamentos e normas internas. Assim, várias áreas podem ser melhoradas para alcançar esse equilíbrio.

A educação e sensibilização envolvem o investimento em programas destinados a conscientizar tanto os clientes quanto os trabalhadores bancários sobre a importância do sigilo bancário, seus direitos e responsabilidades, além das consequências da violação

desse sigilo. Gonçalves (2017, p. 32) destaca a necessidade de um entendimento mais profundo por parte dos envolvidos, o que contribui para a redução de incidentes de violação de privacidade.

A tecnologia e a segurança cibernética desempenham um papel crucial. Implementar medidas robustas de segurança cibernética, como tecnologia de criptografia, autenticação multifatorial e monitoramento proativo de atividades suspeitas, é essencial para proteger as informações financeiras dos clientes contra ameaças como *hackers*, *phishing* e violações de dados. Segundo Barbosa (2020, p. 56), o avanço das tecnologias digitais exige uma atualização constante das práticas de segurança para mitigar riscos emergentes.

Promover a transparência e a responsabilização, por meio da divulgação clara das políticas de sigilo bancário e da responsabilização por violações, tanto por parte das instituições financeiras quanto de indivíduos, é essencial para manter a confiança dos clientes. Martins (2018, p. 48) argumenta que a clareza nas políticas de sigilo e a aplicação rigorosa de sanções para violadores são medidas indispensáveis para a integridade do sistema financeiro.

Melhorar as leis e regulamentos é uma área crítica. A revisão e atualização das leis de sigilo bancário são necessárias para que sejam abrangentes e adequadas aos desafios modernos, como a utilização de tecnologias digitais e criptomoedas. Costa (2019, p. 77) enfatiza a importância de um arcabouço regulatório que acompanhe as inovações tecnológicas e as novas práticas do mercado financeiro.

A proteção de dados e a privacidade devem ser reforçadas, garantindo que as informações financeiras dos clientes sejam tratadas com o devido cuidado e segurança. Isso inclui limitar o compartilhamento de informações com terceiros sem o consentimento do cliente, alinhando-se às leis de proteção de dados. Conforme apontado por Silva (2021, p. 61), a implementação de leis mais rígidas e de políticas internas de proteção de dados nas instituições financeiras é um passo necessário para assegurar a privacidade dos clientes.

A transparência financeira pode ser promovida através de relatórios regulares e verificáveis sobre as práticas de confidencialidade dos bancos, incluindo estatísticas sobre pedidos de divulgação legais e regulamentares. De acordo com Almeida (2016, p. 19), tais relatórios não apenas aumentam a confiança dos clientes, mas também fornecem uma visão mais clara das práticas de *compliance* das instituições.

Finalmente, a cooperação internacional é vital para combater a evasão fiscal, o branqueamento de capitais e outras atividades ilegais que podem ser facilitadas pelo sigilo bancário em diferentes países. Martins e Costa (2018, p. 89) sugerem que a cooperação e a partilha de informações entre jurisdições são essenciais para enfrentar esses desafios de forma eficaz e coordenada.

Capítulo 4. Análise e apresentação dos dados

O sigilo bancário tem sido um princípio fundamental no relacionamento entre instituições financeiras e seus clientes. No entanto, com o avanço das tecnologias digitais, a natureza dessa proteção passou a enfrentar novos desafios. A presente discussão baseia-se em três hipóteses que tratam da eficácia das medidas implementadas pelas instituições financeiras, da conscientização dos consumidores e do impacto das tecnologias emergentes na proteção do sigilo bancário.

Nos últimos anos, as instituições financeiras têm adotado uma série de medidas tecnológicas e regulatórias para fortalecer o sigilo bancário dos seus clientes. De acordo com Arner et al. (2017, p. 19), a digitalização do setor bancário trouxe uma série de inovações, incluindo criptografia avançada, autenticação multifatorial e o uso de algoritmos de deteção de fraudes para proteger dados sensíveis. Essas soluções tecnológicas, aliadas a políticas de conformidade com a legislação como o RGPD na UE, são projetadas para garantir a privacidade e a segurança das transações financeiras.

A falta de conscientização torna os clientes mais vulneráveis a riscos de segurança. Este fenómeno é particularmente preocupante em contextos onde os consumidores utilizam serviços bancários digitais sem adotar práticas básicas de segurança, como a utilização de senhas fortes ou autenticação multifatorial. Segundo um estudo de Javelin Strategy & Research (2020, p. 37), os consumidores tendem a subestimar os riscos associados à utilização de plataformas digitais para transações financeiras, o que aumenta a exposição a fraudes.

O estudo de Gai et al. (2018, p. 45) argumenta que as instituições financeiras têm um papel fundamental na educação dos consumidores sobre a importância de proteger as suas informações bancárias. No entanto, muitas vezes as campanhas de conscientização são limitadas e não alcançam todo o público-alvo de maneira eficaz, o que resulta em uma lacuna significativa na perceção dos riscos associados ao uso de serviços bancários digitais.

O uso de tecnologias emergentes, como IA e *big data*, no setor bancário tem proporcionado avanços significativos na deteção de fraudes e na análise preditiva de

comportamento de clientes. Segundo Brynjolfsson & McAfee (2017, p. 63), a IA permite que os bancos processem grandes volumes de dados em tempo real, identifiquem padrões de comportamento anómalos e melhorem a segurança das transações financeiras.

Porém, o uso dessas tecnologias também apresenta novos desafios para o sigilo bancário. Uma das principais preocupações é que, ao coletar e processar grandes volumes de dados, as instituições financeiras podem inadvertidamente expor informações sensíveis dos clientes. Zarsky (2016, p. 84) afirma que, embora o *big data* possa melhorar a segurança, ele também pode criar riscos de violação de privacidade, pois o processamento de dados em larga escala muitas vezes resulta na criação de perfis detalhados dos clientes, que podem ser vulneráveis a acessos indevidos.

Além disso, a automação de processos através da IA pode gerar situações em que decisões sobre dados financeiros são tomadas sem supervisão humana direta. Isso pode levar a erros na proteção dos dados ou até mesmo a brechas de segurança, como discutido por Schatsky, Muraskin & Gurumurthy (2018, p. 102). Estes autores apontam que, embora as ferramentas de IA ofereçam eficiência e precisão, a dependência excessiva delas sem a devida supervisão humana pode resultar em consequências imprevistas para o sigilo bancário.

As instituições bancárias têm feito progressos significativos na implementação de medidas de proteção ao sigilo bancário na era digital. No entanto, lacunas legislativas e a falta de conscientização dos consumidores ainda são desafios importantes. Além disso, embora tecnologias emergentes como IA e *big data* ofereçam melhorias na segurança, elas também introduzem novos riscos para a privacidade dos dados bancários. A proteção eficaz do sigilo bancário requer um equilíbrio entre inovação tecnológica, robustez regulatória e uma educação mais ampla dos consumidores sobre os riscos e suas responsabilidades.

4.1. Medidas para a implementação do sigilo bancário

As instituições financeiras têm implementado diversas estratégias e tecnologias para garantir a privacidade e a segurança das informações dos clientes. As práticas incluem a adoção de tecnologias avançadas, políticas de conformidade com regulamentos internacionais de proteção de dados e formação contínua de trabalhadores.

De acordo com Fernandes, Rodrigues e Silva (2019), as instituições financeiras utilizam tecnologias de ponta para proteger os dados dos clientes, como criptografia, *firewall*s e sistemas de deteção de intrusões. A criptografia garante que as informações sejam ilegíveis para terceiros não autorizados durante a transmissão e o armazenamento. Além disso, métodos como a autenticação multifatorial (MFA) e a biometria (impressão digital, reconhecimento facial) estão sendo amplamente adotados para adicionar camadas adicionais de segurança.

Além das tecnologias de segurança, a conformidade regulatória é um aspeto fundamental. O RGPD na UE e a Lei de Privacidade do Consumidor da Califórnia (CCPA) nos Estados Unidos são exemplos de regulamentações que visam proteger os dados pessoais dos consumidores. Arner, Barberis e Buckley (2017) afirmam que as instituições financeiras devem cumprir essas regulamentações, que incluem requisitos para notificar os clientes em caso de violação de dados e para garantir que o consentimento explícito seja obtido antes do compartilhamento de dados.

Os trabalhadores das instituições financeiras desempenham um papel essencial na manutenção da segurança e privacidade das informações. Gai et al. (2018) destacam que muitas violações de segurança ocorrem devido a erros humanos. Assim, as instituições têm investido em programas de formação contínua para garantir que os seus colaboradores estejam preparados para lidar com ameaças cibernéticas e respeitar os procedimentos de segurança.

Autores como Costa (2016, p. 45) e Martins (2019, p. 32) defendem que, diante das exigências do combate ao crime e à corrupção, o sigilo bancário deve ser constantemente reavaliado para se adaptar às necessidades contemporâneas, sem, contudo, comprometer a confiança essencial para o funcionamento do sistema financeiro.

4.1.1. Resultados

O presente capítulo, centra-se na análise da informação recolhida através do inquérito desenvolvido para os fins desta investigação. Inicialmente, procede-se a uma caracterização detalhada dos dados e dos elementos necessários para a sua análise. Em seguida, os dados são apresentados e discutidos, estabelecendo-se uma correlação entre as respostas obtidas e as orientações da literatura especializada.

Foram recolhidas, ao todo, 120 respostas através do inquérito desenvolvido na plataforma Google Forms. Destas, 70 respostas foram de clientes e 50 de trabalhadores bancários, todas consideradas válidas para análise. A amostra, composta exclusivamente por indivíduos com contas bancárias, assegura a relevância dos dados face ao objeto do estudo. Esta abordagem, sustentada em metodologias de inquérito como defendido por Saunders, Lewis e Thornhill (2019), permite garantir a validade e a fiabilidade dos dados recolhidos. Esses autores destacam que a amostragem direcionada, especialmente quando focada em grupos específicos, como trabalhadores de instituições bancárias, contribui para uma análise mais precisa e contextualizada, particularmente no que se refere ao sigilo bancário e à confidencialidade dos dados.

De acordo com McKinney e Yoos (p. 581, 2014), o recurso a respostas de profissionais do sector bancário fornece *insights* valiosos sobre a prática do sigilo bancário, contribuindo para uma compreensão aprofundada dos desafios enfrentados na era digital. No presente estudo, ao examinar as respostas dos inquiridos, verificou-se que não foram identificadas respostas inválidas; deste modo, as 120 respostas recolhidas são consideradas pertinentes para a análise e para a obtenção de informações relevantes.

4.2 Resultado dos trabalhadores

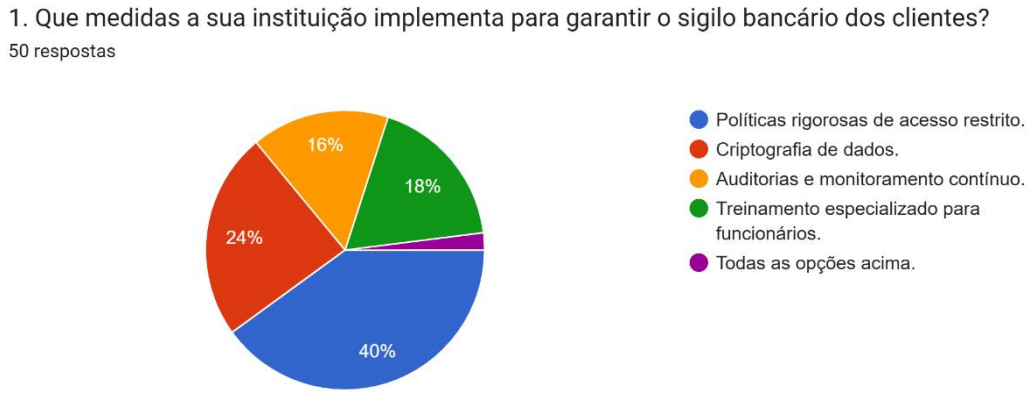

Gráfico 4.2.1. Medidas institucionais implementadas para garantir o sigilo bancário dos clientes.

A pesquisa revelou que 40% dos participantes apontam políticas rigorosas de acesso restrito como a principal medida de segurança em instituições bancárias, destacando a importância do controle de acesso às informações sensíveis. Outros 24% indicam a criptografia de dados como essencial para proteger informações contra acessos indevidos. Já 16% mencionam auditorias e monitorização contínua para identificar e corrigir vulnerabilidades, enquanto 18% ressaltam a importância da formação dos trabalhadores para lidar com dados de forma segura. Apenas 2% afirmam que todas essas medidas são adotadas em conjunto, sugerindo uma abordagem integrada para a segurança bancária.

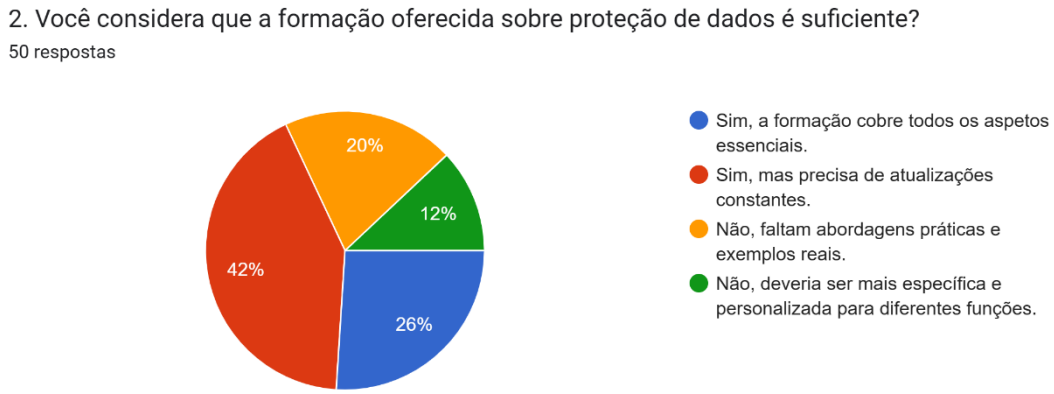

Gráfico 4.2.1.2. Consideração sobre a formação oferecida da proteção de dados.

Neste caso, apenas 12% dos participantes acreditam que a formação atual cobre todos os aspetos essenciais da proteção de dados, indicando que poucos trabalhadores consideram a formação totalmente satisfatória; no entanto, 26% dos inquiridos consideram a formação adequada, mas destacam a necessidade de atualizações frequentes para acompanhar novas ameaças e tecnologias; ademais, 42% dos participantes sentem falta de abordagens práticas e exemplos reais na formação, o que sugere a importância de incluir simulações e estudos de caso para uma aprendizagem mais eficaz. Além disso, 20% dos inquiridos acreditam que a formação deveria ser adaptada para diferentes funções na instituição, de forma a tornar o conteúdo mais relevante para as responsabilidades de cada trabalhador, demonstrando que a proteção de dados exige tanto medidas técnicas quanto uma formação adequada e atualizada para os trabalhadores.

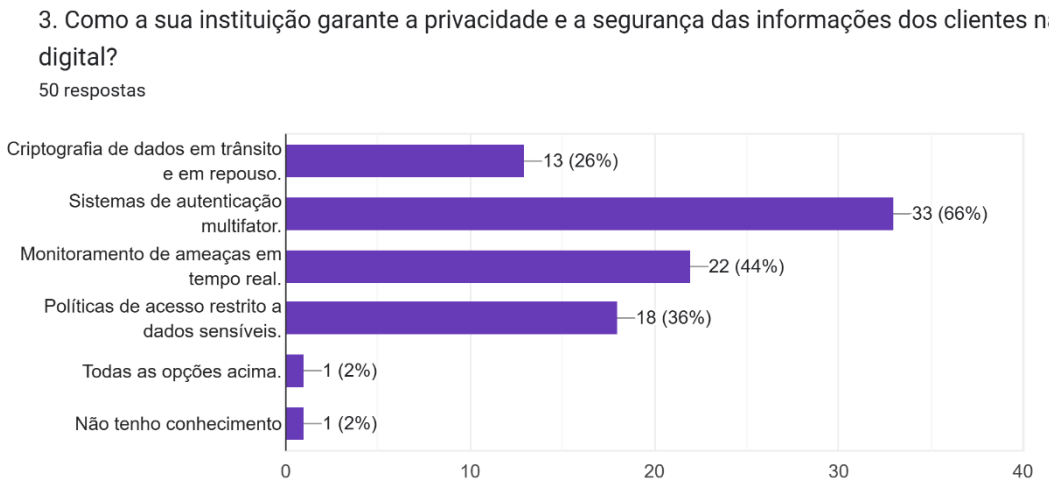

Gráfico 4.2.1.3. Garantia da privacidade e segurança das informações dos clientes na era digital.

A autenticação multifator é a medida de segurança mais popular, escolhida por 66% dos inquiridos, aumentando a proteção contra acessos não autorizados. Aproximadamente 44% consideram essencial o monitoramento contínuo de ameaças em tempo real, enquanto 36% veem as políticas de acesso restrito a dados sensíveis como uma estratégia importante. A criptografia de dados em trânsito e em repouso é adotada por 26% dos participantes, garantindo a proteção das informações. Apenas 2% dos inquiridos afirmaram aplicar todas essas medidas em conjunto, e outros 2% não têm conhecimento das práticas de segurança adotadas.

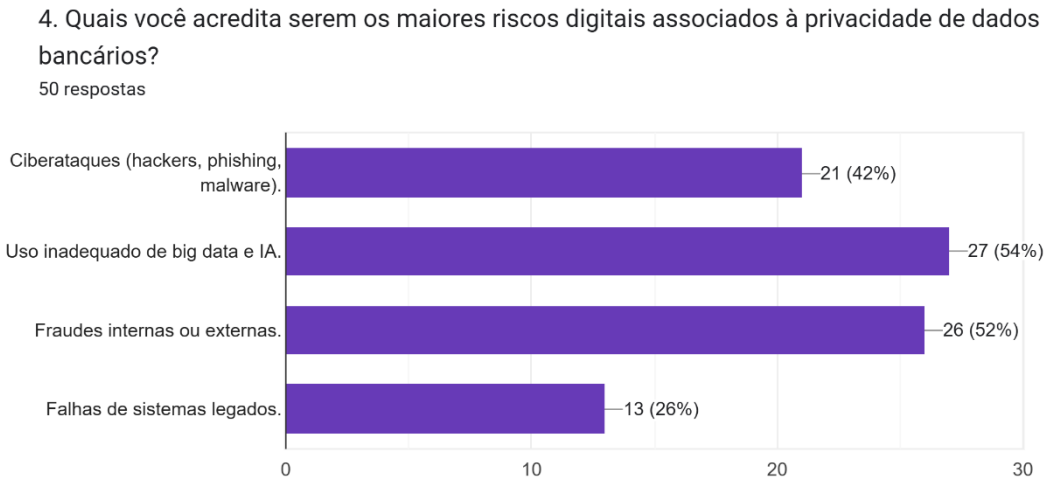

Gráfico 4.2.1.4. Maiores riscos digitais associados à privacidade de dados bancários.

O uso inadequado de *big data* e IA foi a opção mais escolhida, indicada por 54% dos participantes, evidenciando uma preocupação significativa com o potencial de uso indevido de *big data* e inteligência artificial (IA) para manipular ou expor dados bancários de forma não autorizada. As fraudes, sejam internas ou externas, foram apontadas por 52% dos participantes como um dos maiores riscos identificados, o que revela a perceção de que ataques maliciosos podem surgir tanto de colaboradores como de agentes externos. Os ciberataques, incluindo métodos como *phishing e malware*, foram considerados um risco significativo por 42% dos participantes, uma vez que visam o acesso a informações confidenciais. Por fim, 26% dos participantes demonstraram preocupação com as falhas de sistemas legados, observando que sistemas bancários desatualizados podem ser vulneráveis a falhas e ataques, comprometendo a privacidade dos dados.

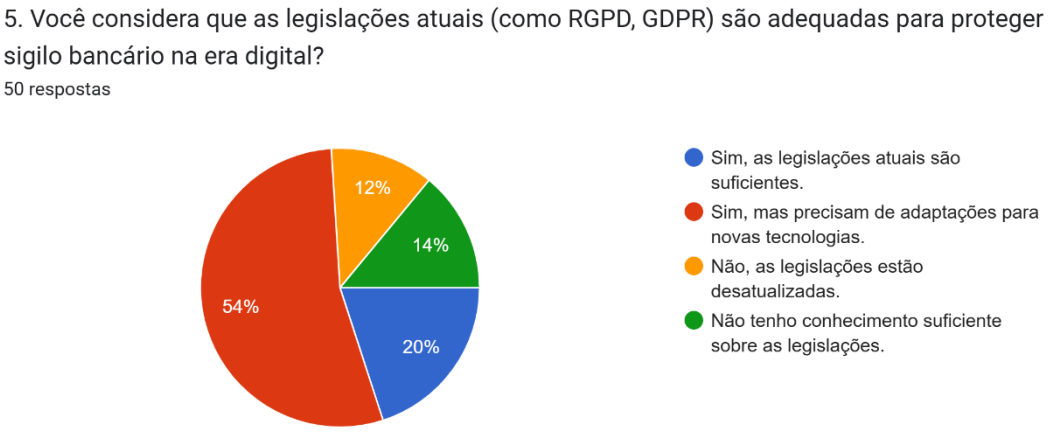

Gráfico 4.2.1.5. Legislações atuais para a proteção do sigilo bancário.

A maioria dos participantes, representando 54%, manifesta a perceção de que as legislações atuais, embora ainda relevantes, necessitam de adaptações para se alinharem ao avanço tecnológico e aos novos desafios impostos pela era digital. Esses inquiridos entendem que, sem atualizações regulares, as normas vigentes podem se tornar insuficientes para mitigar os riscos associados ao uso de tecnologias emergentes no setor bancário. Em contrapartida, 20% dos participantes acreditam que as leis atuais já são adequadas para assegurar a proteção dos dados bancários, indicando uma confiança na robustez das normas existentes para enfrentar os desafios de segurança e privacidade. No entanto, 14% dos inquiridos consideram que as legislações estão desatualizadas e, portanto, ineficazes para lidar com as ameaças digitais contemporâneas, sugerindo que o arcabouço jurídico precisa de uma reforma mais substancial. Por fim, 12% dos participantes assumem não ter conhecimento suficiente para opinar sobre a adequação das legislações vigentes, o que aponta para uma lacuna informativa e potencial necessidade de maior sensibilização sobre o papel das normas no cenário digital.

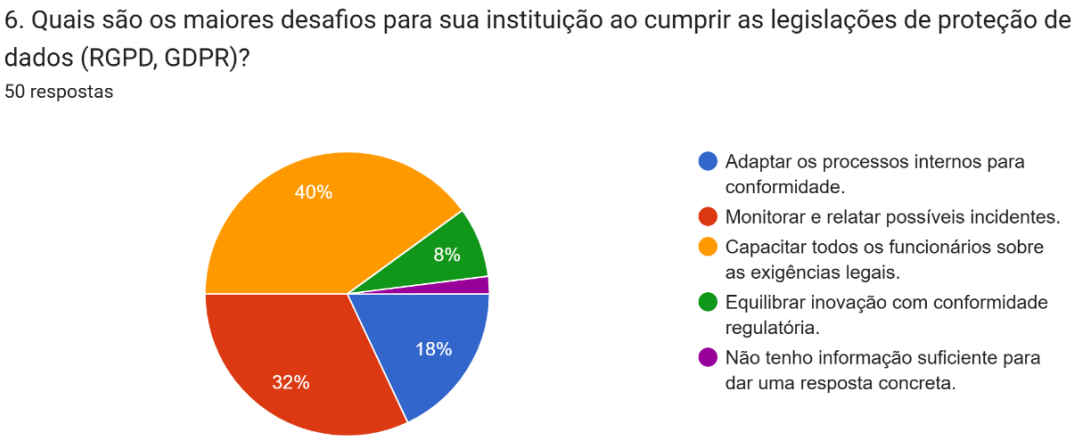

Gráfico 4.2.1.6. Desafios para a instituição e cumprimento das legislações.

A resposta mais escolhida, com 40%, indica que, para a maioria, o maior desafio é monitorizar continuamente o sistema e relatar incidentes de segurança ou de conformidade. Este processo pode ser exigente, especialmente devido à necessidade de resposta rápida e precisa. Em seguida, 32% dos participantes consideram que é desafiador garantir que todos os colaboradores estejam devidamente treinados e informados sobre as obrigações legais em relação à proteção de dados, sendo necessária uma formação contínua para assegurar a compreensão das práticas de conformidade. Para 18%, adaptar processos internos de modo a alinhar-se com os requisitos do RGPD é um grande desafio, envolvendo muitas vezes mudanças estruturais e operacionais na organização. Além disso, 8% indicaram a dificuldade de equilibrar a inovação com as exigências regulamentares, pois a conformidade pode limitar certas iniciativas de inovação. Apenas 2% dos inquiridos indicaram falta de conhecimento sobre o tema, o que sugere um bom nível de entendimento entre os outros participantes.

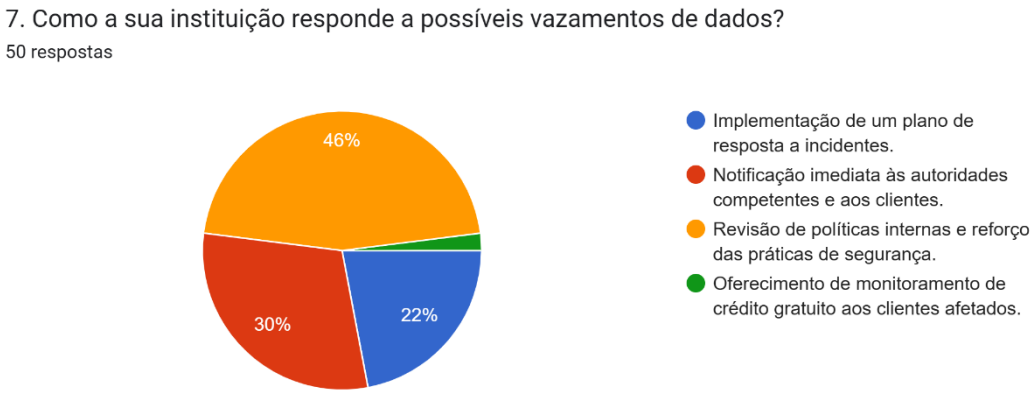

Gráfico 4.21.7. Vazamentos de dados

De acordo com os dados apresentados, 46% dos participantes afirmam que a ação mais comum adotada pelas instituições em caso de vazamento de dados é notificar imediatamente as autoridades competentes e os clientes afetados. Esta resposta reflete uma prioridade clara na comunicação rápida e eficaz com as partes envolvidas, garantindo a transparência e a mitigação de danos decorrentes do incidente. A segunda resposta mais comum, com 30% dos participantes, é a revisão das políticas internas e o reforço das práticas de segurança, o que sugere uma abordagem proativa para melhorar a proteção de dados e evitar a recorrência de falhas de segurança. Uma parcela significativa, 22%, menciona que as instituições implementam um plano de resposta a incidentes, um aspeto fundamental para uma gestão organizada e estruturada diante de situações de crise. Por outro lado, apenas 2% dos participantes indicam que as instituições oferecem monitoramento de crédito gratuito aos clientes afetados, o que, embora relevante, parece ser uma medida menos prioritária em comparação com outras ações.

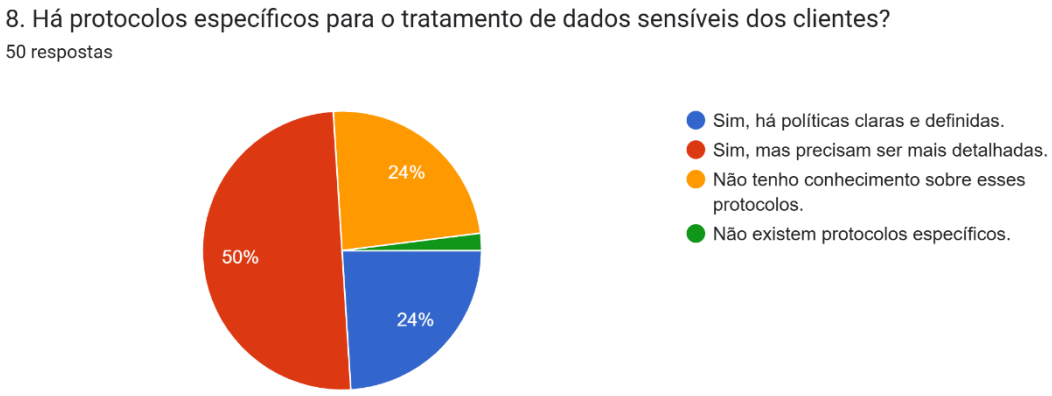

Gráfico4.2.1.8. Tratamento de dados sensíveis dos clientes.

Em relação às políticas e protocolos para o tratamento de dados sensíveis, os resultados mostram que 50% dos participantes acreditam que existem políticas estabelecidas, mas que estas necessitam de um maior grau de detalhamento. Este dado revela uma preocupação com a clareza e a abrangência das políticas, sugerindo que, apesar da existência de diretrizes, muitas delas carecem de especificidade e profundidade suficientes para garantir uma gestão eficaz e segura dos dados sensíveis. Outros 24% dos participantes afirmam que existem políticas claras e bem definidas, indicando que algumas instituições já adotaram um conjunto robusto de normas e procedimentos. No entanto, outro grupo igualmente significativo de 24% dos participantes relatam não ter conhecimento sobre esses protocolos, o que aponta para uma possível falta de comunicação interna e de formação sobre as políticas de proteção de dados sensíveis. Este dado é preocupante, pois revela que um número considerável de colaboradores ou *stakeholders*, pode não estar completamente ciente das políticas e práticas em vigor, o que compromete a eficácia de sua implementação. Por fim, 2% dos participantes indicam que não existem protocolos específicos para o tratamento de dados sensíveis nas instituições em questão. Este número, embora reduzido, destaca a ausência de uma estrutura formalizada para o tratamento e a proteção desses dados, o que pode ser um risco considerável para a segurança e conformidade regulatória.

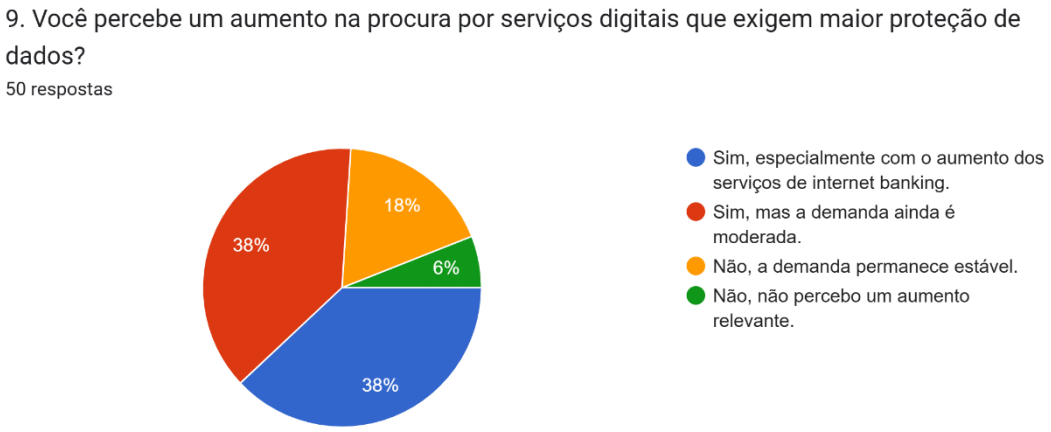

Gráfico 4.2.1.9. Procura por serviços digitais e proteção de dados.

Os resultados indicam que 38% dos participantes percebem um aumento significativo na procura por serviços digitais, com destaque para o crescimento do *internet banking*, o que, por sua vez, exige uma atenção redobrada à segurança e à proteção dos dados pessoais dos utilizadores. Outro grupo significativo, também com 38% dos participantes, observa um aumento na procura, mas considera que a expansão ainda é moderada. Para esse grupo, o crescimento no uso de serviços digitais ocorre de forma mais gradual e controlada, o que pode refletir uma adaptação progressiva dos consumidores e das empresas ao ambiente digital. Por outro lado, 18% dos participantes indicam que não notam um aumento relevante na demanda, sugerindo que a procura pelos serviços digitais permanece estável, sem um crescimento expressivo. Finalmente, uma pequena parcela de 6% dos participantes afirma que a procura permanece estável, sem qualquer variação percetível, permanecendo dentro de um padrão de uso relativamente constante.

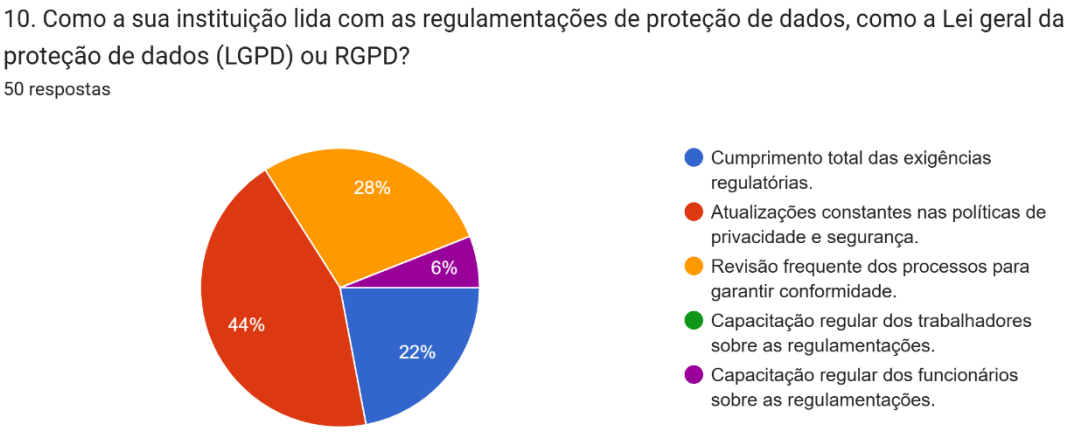

Gráfico 4.2.1.5. Regulamentações de proteção de dados, como LGPD ou RGPD.

Os dados indicam que, 44% afirmam que a maioria das instituições realiza atualizações constantes nas políticas de privacidade e segurança. Isso sugere um compromisso contínuo em adaptar as políticas às mudanças nas regulamentações. Uma parcela significativa de 28% dos participantes indica que a instituição realiza revisões frequentes dos processos internos para assegurar que os procedimentos estejam em conformidade com a legislação de proteção de dados. Outros, 22% mencionam que a instituição cumpre totalmente as exigências regulatórias, cumprindo rigorosamente os requisitos do RGPD e outras regulamentações aplicáveis. Por fim, 6% dos participantes destaca que a instituição promove capacitação regular dos trabalhadores sobre as regulamentações de proteção de dados.

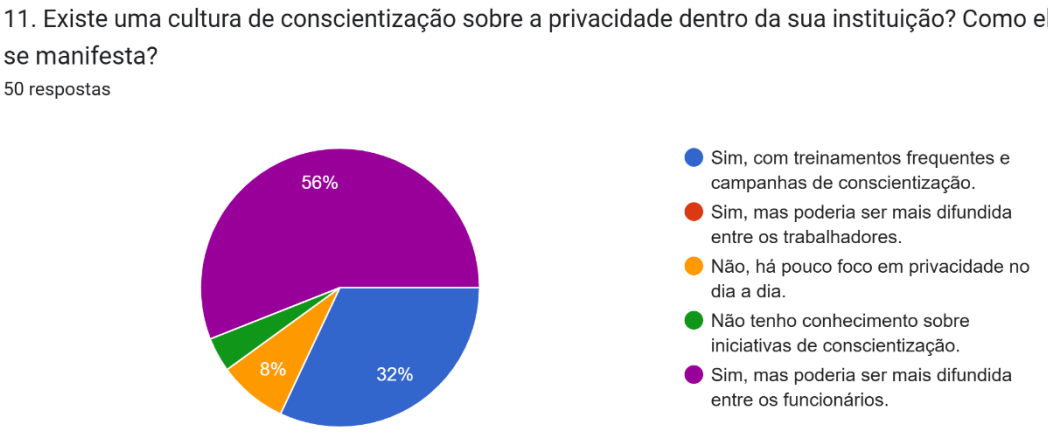

Gráfico 4.2.1.6. Conscientização sobre a privacidade na instituição.

Observa-se que 56% dos inquiridos indicam que, embora haja alguma cultura de privacidade, esta poderia ser mais difundida entre os trabalhadores. Esse dado revela uma perceção de que a sensibilização sobre a privacidade existe, mas carece de maior abrangência e profundidade no quotidiano dos trabalhadores. Por outro lado, 32% afirmam que existem treinamentos frequentes e campanhas de consciencialização na sua instituição, indicando um esforço significativo de algumas organizações em promover a cultura de privacidade. No entanto, 8% dos inquiridos referem que a privacidade não é uma prioridade no seu local de trabalho, enquanto 4% declararam não ter conhecimento sobre qualquer iniciativa de consciencialização, o que indica uma comunicação mais clara sobre as iniciativas já existentes.

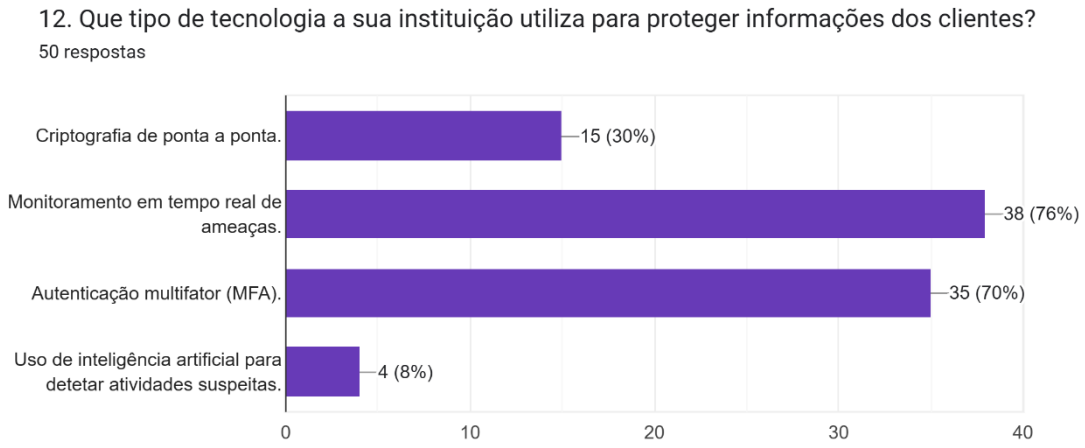

Gráfico 4.2.1.7. Proteção das informações dos clientes.

A maioria das instituições utiliza o monitoramento em tempo real de ameaças 76% para identificar e mitigar possíveis ataques cibernéticos de forma imediata. A autenticação multifator 70% também é amplamente adotada, pois reforça a segurança ao exigir múltiplas formas de verificação de identidade antes de conceder acesso às informações. Aproximadamente um terço das instituições, 30% recorre à criptografia de ponta a ponta para proteger os dados durante a transmissão, garantindo que apenas o destinatário autorizado possa acedê-los. Em contraste, o uso de inteligência artificial para detetar atividades suspeitas ainda é limitado, sendo adotado por apenas 8% das instituições, o que indica que essa tecnologia ainda se encontra em fase inicial de implementação.

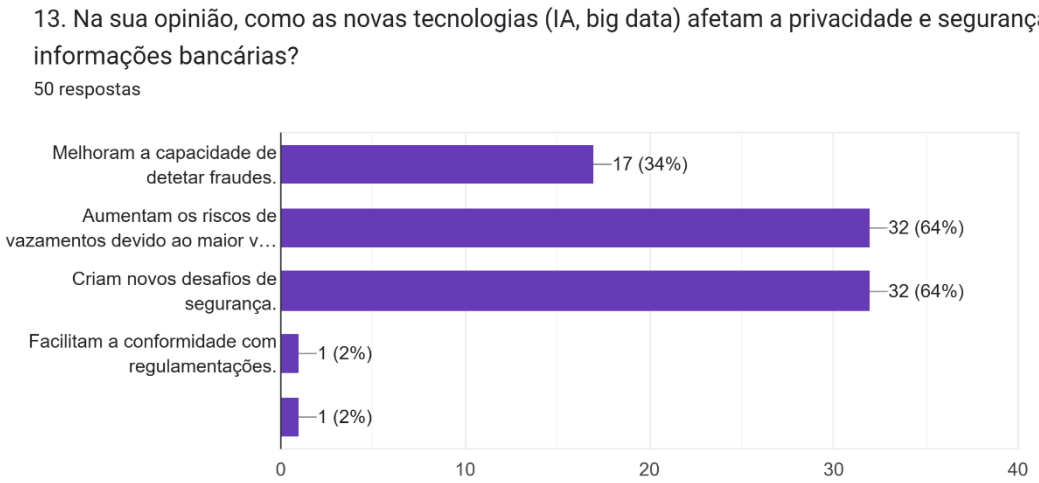

Gráfico 4.2.1.8. Novas tecnologias e a segurança das informações bancárias.

Com o aumento do volume de dados gerados pelas novas tecnologias, 64% dos participantes consideram que os riscos de vazamentos de informações também aumentam, uma vez que há mais dados a serem protegidos. Além disso, 64% reconhecem que as novas tecnologias criam desafios de segurança, exigindo o desenvolvimento de soluções inovadoras para mitigar esses riscos. Por outro lado, cerca de 34% dos participantes acreditam que essas tecnologias contribuem para melhorar a capacidade de detetar fraudes, permitindo respostas mais rápidas e eficazes a tentativas de fraude. Apenas uma pequena fração de 2% vê essas tecnologias como facilitadoras da conformidade com as regulamentações, destacando que, embora a segurança seja reforçada, o alinhamento com as normas regulatórias ainda representa um desafio secundário para muitas organizações.

4.2.2. Resultado dos clientes

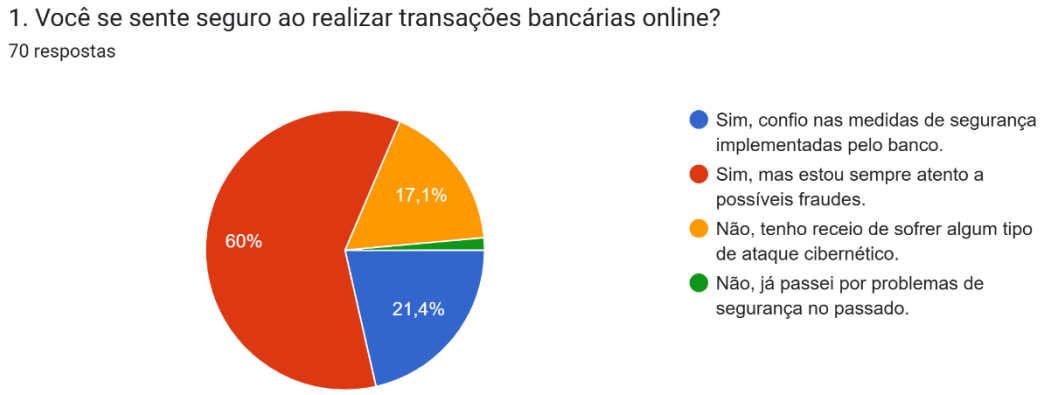

Gráfico 4.2.2.9. Segurança na realização de transações bancárias online.

Verifica-se que 60% dos participantes confiam nas medidas de segurança dos bancos, mas mantêm-se atentos a possíveis fraudes. Este número elevado sugere uma consciência generalizada dos riscos e a adoção de uma postura preventiva. Em contraste, 21,4% dos inquiridos confiam plenamente nas medidas de segurança implementadas pelo banco, sentindo-se seguros durante as transações. No entanto, 17,1% indicam receio de ataques cibernéticos, o que evidencia uma preocupação com o aumento das ameaças digitais. Apenas 1,4% dos participantes relataram experiências passadas de problemas de segurança, o que pode justificar uma desconfiança maior em relação às transações *online*.

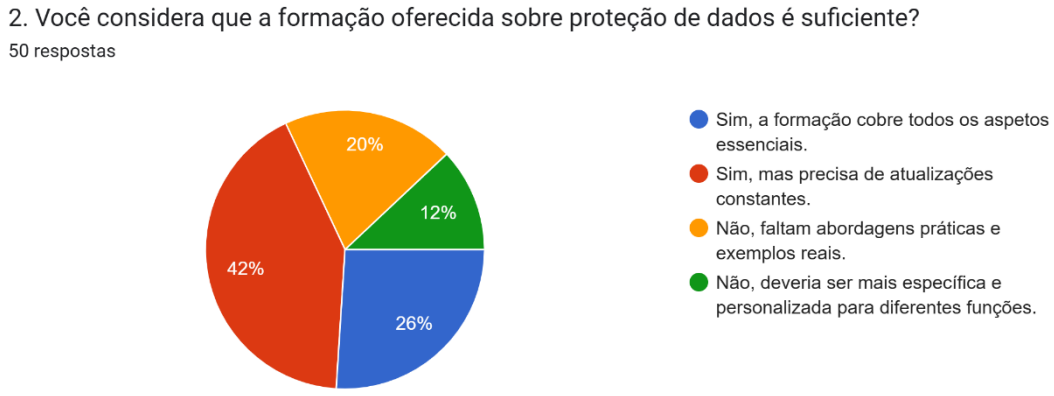

Gráfico 4.2.2.10. Formação aos trabalhadores.

A análise das respostas revela que uma parte significativa dos inquiridos, 42% considera que a formação oferecida não é suficiente, apontando a falta de abordagens práticas e exemplos reais como principais lacunas. Em contrapartida, 26% dos inquiridos afirmam que a formação cobre todos os aspetos essenciais, o que indica que para essa parcela, os tópicos abordados são adequados para as necessidades básicas da área. Por outro lado, 20% das respostas indicam que, embora a formação seja boa, ela exige atualizações constantes para se manter alinhada com as mudanças frequentes no campo da proteção de dados. Por fim, 12% dos participantes acreditam que a formação deveria ser mais específica e personalizada de acordo com as funções desempenhadas dentro da organização, sugerindo que a abordagem geral não atende plenamente às necessidades de cada perfil profissional. Em resumo, a maioria dos 42% inquiridos considera que a formação precisa ser aprimorada com abordagens mais práticas, enquanto apenas 26% acreditam que ela já cobre o necessário de forma adequada

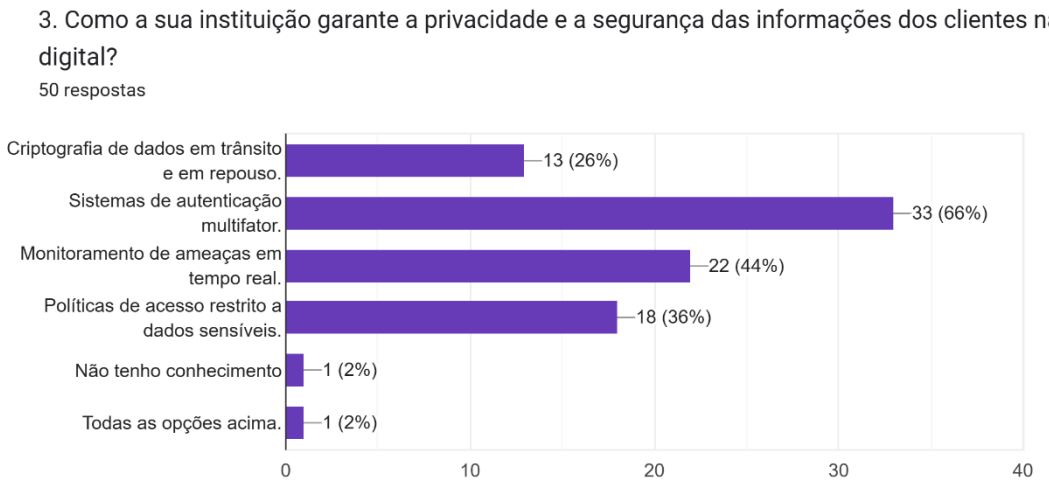

Gráfico 4.2.2.11. Privacidade e segurança.

Verifica-se que 66% dos participantes confirmam que a autenticação multifator é mais aplicada, mas precisa ainda melhorar a implementação. Em contraste, 44% dos inquiridos apresentam melhoramento de ameaças em tempo real nas medidas de segurança implementadas pelas instituições, sentindo-se seguros durante as transações. No entanto, 36%, garantem que apresentam políticas de acesso restrito a dados sensíveis indicam

capacidade para possíveis inconveniente. Apenas 2% dos participantes relataram que não têm conhecimento e 2% afirmam que todas são efetuadas nas suas instituições.

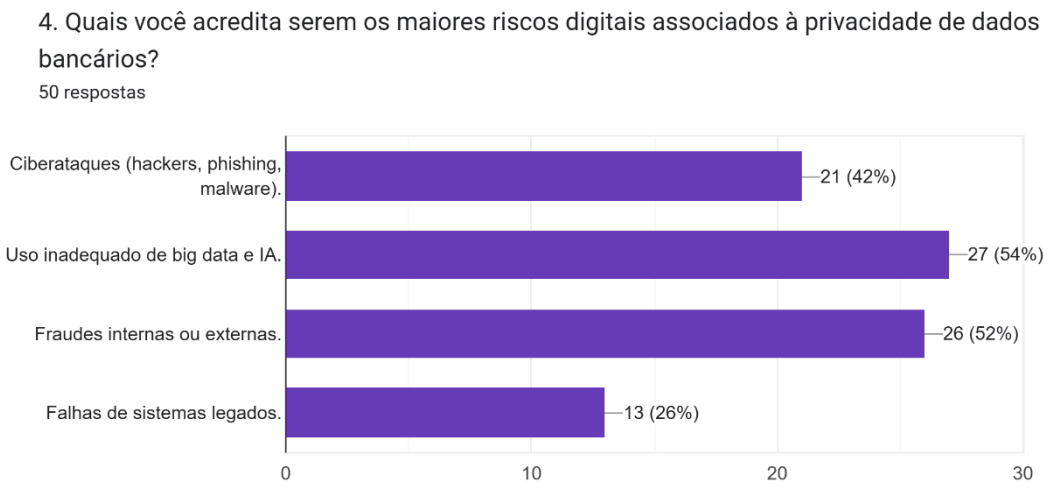

Gráfico 4.2.2.12. Riscos digitais associados à privacidade de dados bancários.

Observa-se que o uso inadequado de *big data* e IA é considerado o maior risco, apontado por 54% dos participantes, seguido pelas fraudes internas ou externas, com 52%, e pelos ciberataques, como *hackers*, *phishing e malware*, que correspondem a 42%. As falhas de sistemas legados foram o risco menos mencionado, com 26%. Estes dados sugerem uma preocupação predominante com o impacto das novas tecnologias e com as fraudes, que representam ameaças significativas à privacidade dos dados na era digital.

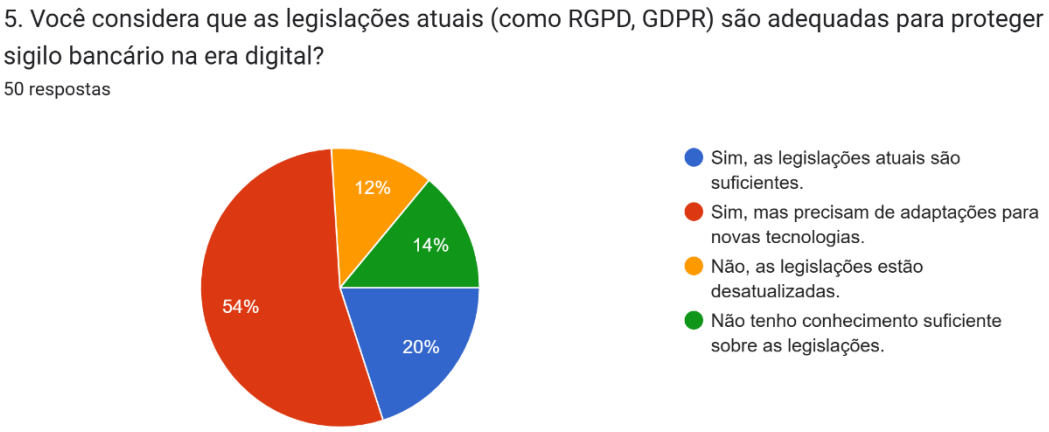

Gráfico 4.2.2.13. Leis adequadas para o sigilo bancário.

A maioria dos inquiridos, 54%, considera que as legislações precisam de adaptações para acompanhar as novas tecnologias, enquanto 20% avaliam que as normativas vigentes são suficientes. Por outro lado, 14% acreditam que as legislações estão desatualizadas, e 12% afirmam não ter conhecimento suficiente sobre o tema. Estes resultados refletem uma perceção geral de que, embora robustas, as legislações atuais carecem de atualizações para enfrentar de forma eficaz os desafios impostos pela era digital.

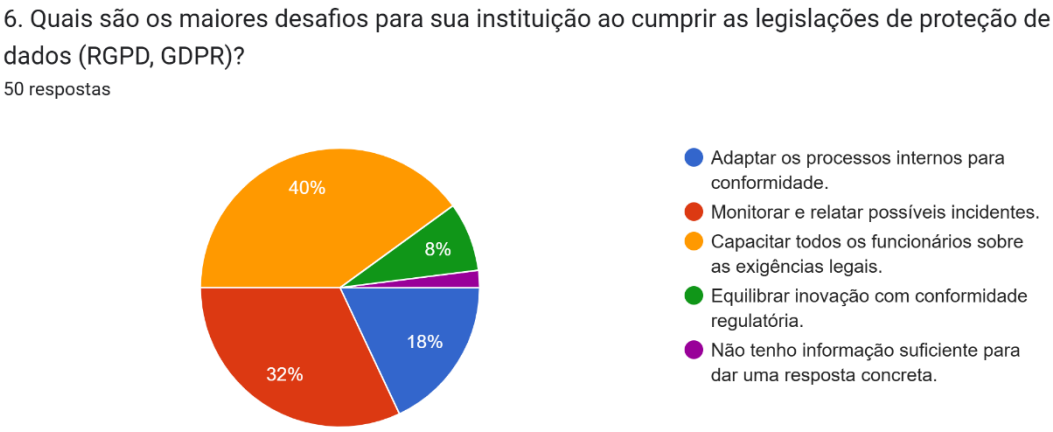

Gráfico 4.2.2.14. Desafios para o cumprimento das legislações de proteção de dados.

A maior dificuldade identificada foi a capacitação de todos os trabalhadores sobre as exigências legais, com 40% das respostas, o que evidencia a necessidade de formar os colaboradores para garantir a conformidade com as leis de proteção de dados. A segunda maior dificuldade, representando 32% das respostas, refere-se à monitorização e relato de possíveis incidentes, indicando a complexidade de manter uma vigilância constante e responder rapidamente a violações. Com 18% das respostas, adaptar os processos internos para conformidade também foi apontado como um desafio significativo, destacando a dificuldade de alinhar as operações internas com os requisitos regulatórios. Outras dificuldades incluem equilibrar inovação com conformidade regulatória, mencionada por 8% dos participantes, o que mostra o desafio de inovar sem comprometer a conformidade. Por fim, 2% dos inquiridos indicaram que não têm informação suficiente para dar uma resposta concreta.

Gráfico 4.2.2.15. Respostas a possíveis vazamentos de dados.

A mais comum, representando 46% das respostas, foi a revisão de políticas internas e reforço das práticas de segurança, indicando que, para muitas instituições, esta é a principal medida reativa a vazamentos. Notificação imediata às autoridades competentes e aos clientes foi a segunda medida mais mencionada, com 30% das respostas, sugerindo a importância dada à comunicação rápida em caso de incidente. A implementação de um plano de resposta a incidentes foi indicada por 22% dos participantes, evidenciando a preparação prévia para lidar com situações de vazamento. Apenas 2% dos inquiridos

afirmaram oferecer monitoramento de crédito gratuito aos clientes afetados, o que sugere que essa prática é menos comum ou não considerada prioritária.

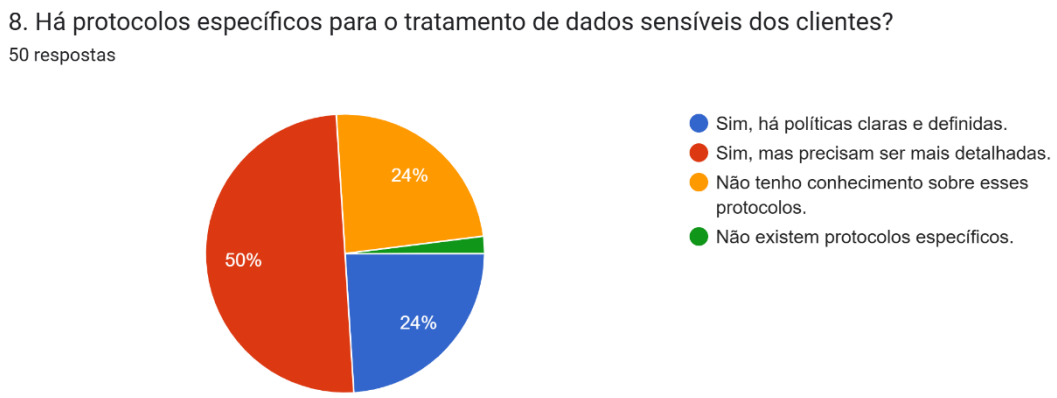

Gráfico 4.2.2.16. Protocolos específicos para tratamento de dados sensíveis dos clientes.

Observa-se que 24% dos participantes indicaram que há políticas claras e definidas para o tratamento desses dados, enquanto 50% afirmaram que, embora existam políticas, estas necessitam de maior detalhamento. Outros 24% dos inquiridos afirmaram desconhecer a existência de tais protocolos, e apenas uma pequena fração, representada por 2% das respostas, respondeu que não há protocolos específicos. Estes dados revelam que, embora exista alguma preocupação com a proteção de dados sensíveis, há uma lacuna na implementação e clareza desses protocolos, o que pode sugerir uma necessidade de reforço e comunicação interna sobre as políticas de proteção de dados.

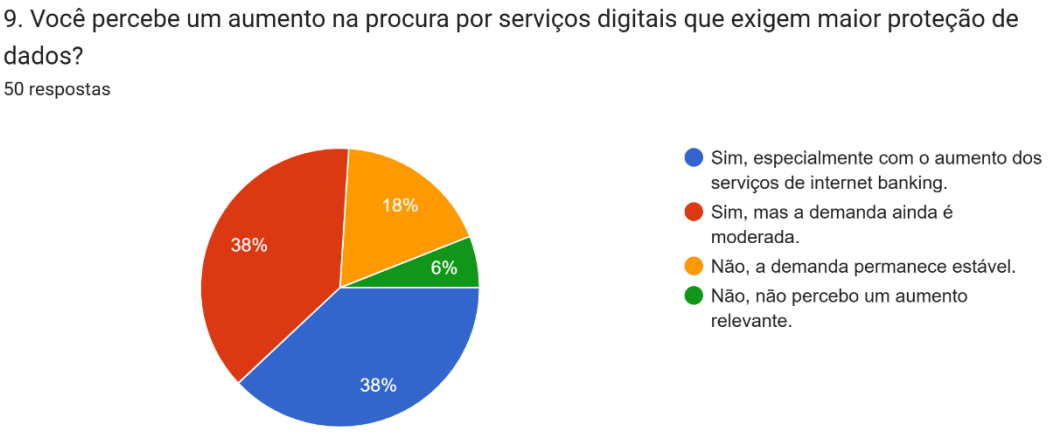

Gráfico 4.2.2.17. Procura por serviços digitais.

Verifica-se que 38% dos participantes notaram um aumento na procura, especialmente devido ao crescimento dos serviços de *internet banking*, enquanto uma outra parcela de 38% indicou que, embora a procura esteja a crescer, a demanda ainda é considerada moderada. Apenas 18% afirmaram não notar uma variação significativa na procura, e 6% não percebem qualquer aumento relevante. Estes resultados mostram uma tendência crescente para a procura de serviços digitais, impulsionada pela popularização do *internet banking*, o que, por sua vez, exige um reforço nas medidas de proteção de dados para acompanhar a expansão desse tipo de serviço.

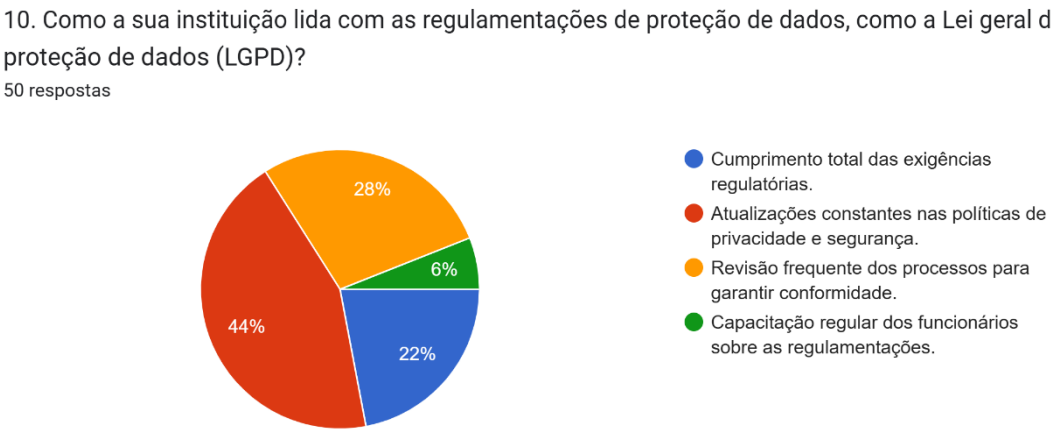

Gráfico 4.2.2.18. Regulamentações de proteção de dados.

Observa-se que apenas 22% das instituições indicam um cumprimento total das exigências regulatórias do RGPD. A maioria dos inquiridos, 44%, afirma que realizam atualizações constantes nas políticas de privacidade e segurança, evidenciando uma adaptação contínua, mas não necessariamente completa, aos requisitos legais. Além disso, 28% reportam uma revisão frequente dos processos para garantir conformidade, o que sugere uma abordagem proactiva em verificar e ajustar práticas, enquanto apenas 6% das respostas mencionam uma capacitação regular dos trabalhadores sobre as regulamentações.

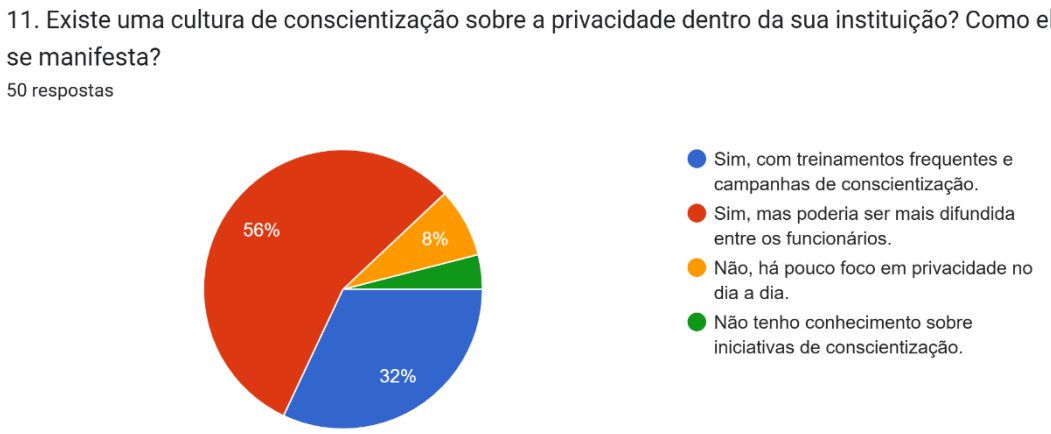

Gráfico 4.2.2.19. Cultura de conscientização sobre privacidade.

Os dados mostram que 56% dos inquiridos consideram que há pouco foco em privacidade no dia a dia, indicando uma lacuna significativa na prática da cultura de privacidade. Em contraste, 32% afirmam que a instituição promove treinamentos frequentes e campanhas de sensibilização, sugerindo uma minoria de organizações que incorpora uma cultura ativa de proteção de dados. Por outro lado, 8% reconhecem a existência de iniciativas de privacidade, mas acreditam que poderiam ser mais difundidas entre os trabalhadores. Finalmente, 4% dos inquiridos declaram não ter conhecimento de quaisquer iniciativas de consciencialização.

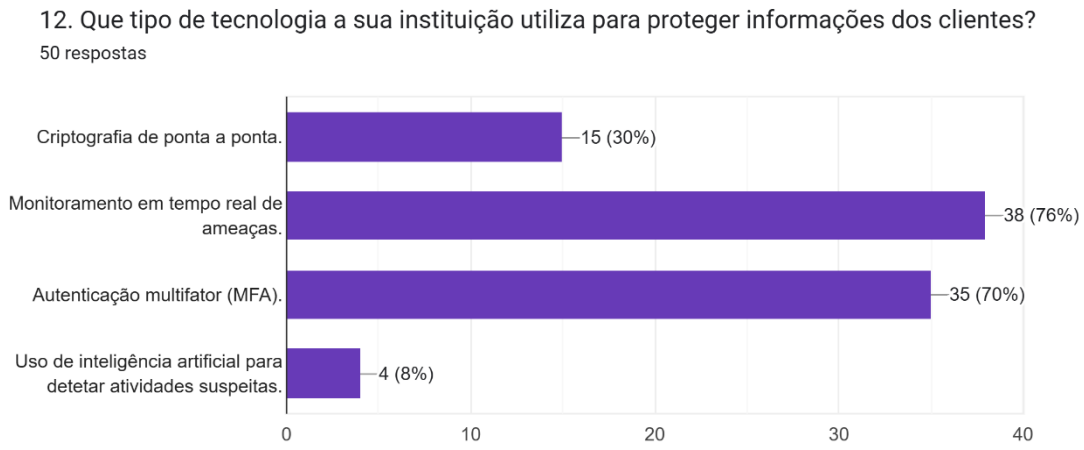

Gráfico 4.2.2.20. Tecnologia utilizada para proteção de informações de clientes.

Neste caso, a opção mais escolhida foi o monitoramento em tempo real de ameaças, representando 76% das respostas, o que indica uma ênfase na deteção imediata de riscos e intrusões. Em seguida, autenticação multifator (MFA) foi mencionada por 70% das instituições, destacando-se como uma prática relevante para aumentar a segurança no acesso a dados sensíveis. Criptografia de ponta a ponta foi utilizada por 30% das instituições, refletindo um esforço de proteção dos dados durante a transmissão. Por fim, o uso de inteligência artificial para detetar atividades suspeitas foi mencionado por apenas 8% das respostas, sugerindo que esta tecnologia é menos comum ou ainda emergente na proteção de informações dos clientes.

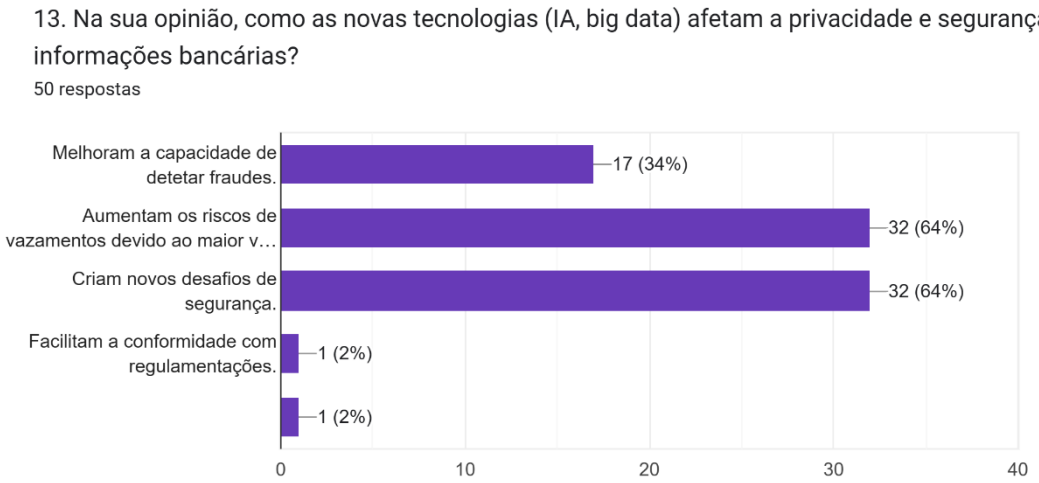

Gráfico 4.2.2.21. Impacto das novas tecnologias na privacidade e segurança das informações bancárias.

A maioria dos inquiridos (64%) considera que essas tecnologias aumentam os riscos de vazamentos de dados devido ao maior volume de informações e criam desafios de segurança. Para 34% dos participantes, essas tecnologias melhoram a capacidade de detetar fraudes. Apenas 2% veem como principal impacto a facilitação da conformidade com regulamentações. Estes dados indicam que, apesar dos benefícios na deteção de fraudes, prevalece a perceção de que as novas tecnologias trazem maiores riscos e desafios de segurança para a proteção de dados bancários.

4.3. Discussão de resultados

Os resultados obtidos indicam que as instituições bancárias recorrem a uma combinação de práticas e tecnologias para assegurar a confidencialidade e a segurança dos dados dos seus clientes. Entre as principais medidas destacam-se as políticas de acesso restrito, a utilização de criptografia, a autenticação multifator e o monitoramento em tempo real. Estas estratégias refletem um compromisso com a cibersegurança, essencial num cenário em que as ameaças digitais se tornam mais frequentes e sofisticadas.

No âmbito da formação sobre proteção de dados, observa-se que, apesar de reconhecida como essencial, necessita de reformulação. Sugere-se a inclusão de atualizações regulares, uma abordagem prática e uma adaptação às especificidades das funções desempenhadas pelos diferentes colaboradores. Este esforço é fundamental para garantir a eficácia e a abrangência das formações oferecidas.

As instituições enfrentam ainda desafios relacionados com a comunicação e a clareza das suas políticas de segurança. Em muitos casos, os protocolos existentes não são suficientemente detalhados ou conhecidos por trabalhadores e clientes. A lacuna identificada aponta para a necessidade de melhorar a transparência, reforçar a formação contínua e estabelecer normas claras, garantindo que todos compreendam os procedimentos exigidos.

Os gráficos analisados revelam um aumento significativo na procura por serviços digitais, o que acentua a necessidade de reforçar as medidas de proteção de dados. Para lidar com este crescimento, as instituições adotam estratégias que incluem a revisão frequente das suas políticas e a adaptação contínua às regulamentações, com destaque para o RGPD. Contudo, algumas instituições ainda carecem de iniciativas robustas para apoio aos clientes em casos de incidentes, como o monitoramento de crédito após vazamentos de dados.

Relativamente ao tratamento de dados sensíveis, verifica-se que, embora existam políticas estabelecidas, estas frequentemente carecem de detalhamento e comunicação eficaz. A falta de conhecimento interno sobre os protocolos existentes representa um desafio, sublinhando a importância de uma formação contínua e orientada às necessidades reais das equipas.

Os resultados também evidenciam que as instituições bancárias enfrentam obstáculos na monitorização de incidentes e na capacitação dos colaboradores, aspetos fundamentais para a manutenção da conformidade com o RGPD. Adicionalmente, há uma perceção generalizada de que as legislações atuais, apesar de sólidas, necessitam de atualizações para enfrentar os desafios trazidos pela digitalização, como o uso de *big data,* inteligência artificial e a mitigação de fraudes e ciberataques.

Por fim, as instituições demonstram um esforço contínuo para se alinharem às regulamentações em vigor, através da revisão regular de processos e da atualização de políticas de segurança e privacidade. No entanto, a formação de colaboradores, embora reconhecida como prioritária, permanece uma área que exige maior investimento, de modo a garantir uma conformidade eficaz e abrangente. Estes resultados sublinham a necessidade de promover uma cultura de privacidade e de reforçar a disseminação da consciência sobre práticas seguras no tratamento de dados.

Com base nas hipóteses formuladas, nos objetivos delineados e nos resultados obtidos através do questionário e da análise dos inquéritos, é possível apresentar as seguintes conclusões principais:

4.4. Correlação das hipóteses com os resultados

H1: Medidas adequadas para proteger o sigilo bancário, mas lacunas legislativas significativas

Os resultados indicam que as instituições bancárias têm implementado uma combinação de tecnologias e políticas para proteger o sigilo bancário, como autenticação multifator, criptografia e monitorização em tempo real. Contudo, verifica-se que tanto em Portugal quanto em Angola, as legislações existentes necessitam de revisões e atualizações para acompanhar os avanços tecnológicos e responder aos desafios da era digital. Esta conclusão confirma parcialmente a hipótese, evidenciando esforços relevantes, mas destacando lacunas nas regulamentações.

H2: Insuficiência na consciencialização dos consumidores sobre o sigilo bancário

Os dados indicam que muitos clientes têm um conhecimento limitado sobre os seus direitos de privacidade e as implicações do sigilo bancário nas transações digitais. A falta de clareza e de comunicação eficaz por parte das instituições reforça a necessidade de

programas educativos e campanhas informativas. Esta hipótese é amplamente confirmada, destacando a vulnerabilidade dos clientes devido à baixa consciencialização.

H3: Impacto das tecnologias emergentes na segurança e nos desafios ao sigilo bancário

A introdução de tecnologias como *big data* e inteligência artificial tem proporcionado melhorias na monitorização e na prevenção de fraudes. No entanto, essas mesmas tecnologias também aumentam os riscos de utilização inadequada de dados e de ciberataques mais sofisticados. Este duplo impacto confirma a hipótese, apontando para a necessidade de um equilíbrio entre inovação tecnológica e reforço das medidas de segurança.

4.5. Avaliação do alcance dos objetivos

Objetivo Geral: Analisar as práticas de sigilo bancário na era digital

Este objetivo foi amplamente alcançado. A dissertação documentou as práticas adotadas pelas instituições bancárias, analisou os desafios específicos da era digital e identificou medidas de proteção e as limitações legislativas existentes.

Objetivos Específicos:

- Identificar medidas de proteção de dados

Foram destacadas práticas como criptografia, autenticação multifator, políticas de acesso restrito e monitorização em tempo real, alinhadas com os padrões de segurança da era digital.

- Examinar a perceção dos trabalhadores

Os trabalhadores reconhecem a relevância das práticas de proteção de dados, mas apontam insuficiências na formação contínua e na comunicação interna sobre políticas específicas, especialmente no contexto do RGPD.

- Avaliar o nível de consciencialização dos clientes

O baixo nível de conhecimento dos clientes sobre os seus direitos de privacidade e proteção de dados foi identificado como uma área de preocupação, reforçando a necessidade de iniciativas educativas.

- Investigar desafios relacionados às tecnologias emergentes

Foi comprovado que as tecnologias emergentes criam tanto oportunidades quanto desafios, destacando a necessidade de legislações adaptadas para lidar com riscos associados a *big data* e IA.

4.6. Considerações gerais dos resultados

As instituições bancárias, apesar de terem implementado medidas tecnológicas avançadas para assegurar o sigilo bancário, continuam a enfrentar desafios significativos, especialmente no que respeita à consciencialização dos clientes e à capacitação dos seus colaboradores. Estes dois fatores assumem um papel crucial na proteção de dados sensíveis, uma vez que o comportamento humano pode ser tanto uma barreira como uma vulnerabilidade no sistema.

A legislação aplicável, embora robusta em muitos aspetos, exige revisões e adaptações constantes para acompanhar a rápida evolução da era digital. O dinamismo inerente às tecnologias emergentes implica riscos que não se encontram contemplados em quadros normativos desatualizados. Assim, a atualização legislativa torna-se indispensável, não apenas para prevenir lacunas jurídicas, mas também para garantir um equilíbrio entre a proteção de direitos e a promoção da inovação tecnológica.

O aumento exponencial da procura por serviços bancários digitais destaca a necessidade de maior transparência por parte das instituições bancárias, tanto na comunicação com os clientes como na aplicação de medidas de segurança. Além disso, exige investimentos contínuos em cibersegurança, formação técnica dos colaboradores e iniciativas de educação financeira para os utilizadores.

Por último, o advento e a utilização de tecnologias emergentes, como inteligência artificial, *blockchain* e sistemas *peer-to-peer*, sugerem que o equilíbrio entre inovação e segurança será um dos pilares fundamentais para o futuro do sigilo bancário. Garantir esse equilíbrio não só preserva a confiança dos clientes, mas também promove a sustentabilidade e a competitividade do setor bancário num contexto global em constante transformação.

Considerações finais

O sigilo bancário é um princípio fundamental desde o início da atividade bancária, desempenhando um papel essencial na relação de confiança entre instituições financeiras e seus clientes. Essa relação de fidúcia é indispensável para a estabilidade do setor financeiro e, por extensão, de todo o sistema económico. Este trabalho teve como objetivo explorar a temática do sigilo bancário, destacando suas nuances, regulamentações e os desafios que envolvem sua aplicação. De forma geral, o sigilo bancário refere-se à obrigação das instituições financeiras de preservar todas as informações e dados referentes a seus clientes. Isso inclui transações bancárias, saldos, investimentos e informações financeiras, patrimoniais e fiscais. Em suma, o sigilo garante a privacidade do cliente em relação às suas operações financeiras. Contudo, essa obrigação não é absoluta, podendo ser levantada em situações específicas, como em casos de litígios criminais ou tributários.

Em Portugal, o sigilo bancário é regulado por diversos dispositivos legais, como os artigos 78.º a 84.º do Regime Geral das Instituições de Crédito e Sociedades Financeiras, aprovado pelo Decreto-Lei n.º 298/92, de 31 de dezembro. Além disso, outras legislações, como o Código Civil, o Código de Processo Penal e a Constituição da República Portuguesa, também abordam a proteção desse princípio. O sigilo bancário é visto como um pilar fundamental da relação fiduciária entre instituições financeiras e clientes, contribuindo para a solidez do setor financeiro e a confiança no sistema económico.

No entanto, como em muitas jurisdições, o sigilo bancário em Portugal não é uma regra absoluta. Em determinadas circunstâncias, o princípio da confidencialidade pode ser quebrado, especialmente em investigações criminais ou em litígios com a Autoridade Tributária. O levantamento indevido do sigilo bancário pode acarretar penalidades legais, além de manchar a reputação das instituições financeiras e de seus trabalhadores envolvidos.

De maneira semelhante, em Angola, o sigilo bancário também é protegido pela legislação local. O Banco Nacional de Angola (BNA) é o órgão regulador responsável pela supervisão do setor financeiro, estabelecendo diretrizes para a proteção das informações dos clientes. Assim como em Portugal, as instituições financeiras em Angola só podem divulgar dados de clientes com o consentimento expresso ou por ordem judicial. Contudo,

em ambos os países, existem exceções em casos de investigações criminais, permitindo a quebra do sigilo para atender a interesses maiores da justiça.

É importante ressaltar que o sigilo bancário, ao mesmo tempo em que assegura a privacidade dos clientes, pode entrar em conflito com o interesse público, especialmente em contextos de combate ao branqueamento de capitais e ao financiamento de atividades ilícitas. Portanto, a legislação em Portugal e Angola busca equilibrar esses dois polos, permitindo a quebra do sigilo apenas em situações estritamente regulamentadas e supervisionadas.

Em conclusão, o sigilo bancário é um elemento-chave na relação jurídica entre bancos e clientes, tanto em Portugal quanto em Angola. Embora a proteção da confidencialidade seja garantida pela lei, o equilíbrio entre a privacidade do cliente e o interesse público faz com que o sigilo bancário não seja um princípio absoluto.

Observa-se que, embora as novas tecnologias tragam benefícios como o aumento da capacidade de detetar fraudes, também acarretam desafios adicionais e aumentam os riscos de vazamento de dados. As instituições parecem estar investindo em medidas de segurança como o monitoramento em tempo real e a autenticação multifator para se adaptarem a essas mudanças, mas ainda há um uso limitado de inteligência artificial, o que pode indicar áreas para melhorias futuras.

Referências bibliográficas

Abrão. N. (2018). *Direito bancário*. 18ª edição. Brasil. Saraiva.

Abrantes, M. L. (2017). *Os pais da crise económica angolana*. Disponível em:

Os pais da crise económica angolana

Afonso. V. JR (2022). *O sigilo bancário. Exceções e tutela penal à luz da lei angolana e*

da jurisprudência portuguesa. Luanda. Disponível em o sigilo bancário. Exceções e tutela penal à luz da lei angolana e da jurisprudência portuguesa | valdano afonso jr. - academia.edu.

Almeida, J. P. (2018). *Sigilo Bancário e o Direito à Privacidade*. São Paulo: Editora Jurídica.

Almeida, L. F. (2016). *Transparência Financeira e Compliance*. Lisboa: Edições

Sílabo.

Almeida, P. (2018). *A Proteção dos Dados Bancários e o Sigilo Profissional* (p. 89).

Coimbra: Almedina.

Almeida Santos, L. (2019). *Regime Jurídico do Sigilo Bancário em Angola: Reformas e Desafios*. Porto Editora, p. 89.

Almeida, P. (2016). *Confidencialidade e Transparência no Setor Bancário*. P.19 Coimbra: Edições Jurídicas.

Andrade, M. V. (2019). *Os Direitos Fundamentais na Constituição Portuguesa*. 3ª ed. Coimbra Editora.

Andrade, A. (2019). *Direito Bancário: Entre a Privacidade e o Interesse Público* (p. 78). Coimbra: Almedina.

Andrade, M. (2020). *Direito Bancário em Portugal*. p. 132. Lisboa: Edições Jurídicas.

APA (2010). *Publication Manual of American Psychological Association.*

Washingthon, DC: APA.

Araújo, M. L. (2018). *O Direito ao Sigilo Bancário no Contexto das Investigações Fiscais*. Rio de Janeiro: Jurídica Press.

Araújo, R. (2018). *O Direito à Privacidade e a Supervisão Financeira* (p. 134). Lisboa: Edições Jurídicas.

Arner, D. W., Barberis, J. N., & Buckley, R. P. (2017). *FinTech, RegTech and the Reconceptualization of Financial Regulation*. Northwestern Journal of International Law & Business, 37(3), 371-413.

Attitudes Drive a New Era of Fraud Risk. Pleasanton, CA: Javelin Strategy & Research. p. 37.

Azevedo, M. E (2012). O Segredo Bancário e a Fiscalidade Na Ordem Jurídica Portuguesa. Lusíada.

Bacelar Gouveia, J. (2020). *Direito Constitucional Financeiro*. 4ª ed. Almedina.

Bacelar Gouveia, J. (2021). *Direito Constitucional*. 6ª ed. Almedina.

Baker, A. (2016). *The Panama Papers: Exposing the World's Corruption*. New York: PublicAffairs.

Barbosa, R. (2020). *Segurança Cibernética no Setor Bancário*. Lisboa: Edições Sílabo.

Barbas Homem, P. (2014). *O Direito Bancário e o Sigilo Profissional*. Coimbra: Coimbra Editora

Becho, R. L. (2017). *Direito Bancário*. São Paulo: Saraiva.

Bessis, J. (2015). *Risk Management in Banking*. Wiley.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). *Bitcoin: Economics, technology, and governance*. Journal of Economic Perspectives, 29(2), 213-238.

Brandeis, L. & Warren, S. (1890). *The Right to Privacy*. Harvard Law Review, 4(5),

193-220.

Bryans, D. (2014). *Bitcoin* and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal*, 89(1).

Berentsen, A., & Schär, F. (2018). A short introduction to the world of cryptocurrencies. *Federal Reserve Bank of St. Louis Review*, 100(1), 1-16.

Brynjolfsson, E., & McAfee, A. (2017). *The Business of Artificial Intelligence: What it Can — and Cannot — Do for Your Organization*. Harvard Business Review.

Cordeiro, A. M. (2019). *O Sigilo Bancário em Portugal: Limites e Quebra*. Almedina.

Carr, N. (2008). *The big switch: rewiring the world, from Edison to Google 1959.* Disponível em: The big switch : rewiring the world, from Edison to Google : Carr, Nicholas G., 1959- : Free Download, Borrow, and Streaming : Internet Archive

Cardoso, J. (2017). *Branqueamento de Capitais e Cooperação Internacional: Uma Perspectiva Angolana*. Luanda: Editora Jurídica

CORREIA, João. *A Transformação Digital no Sistema Bancário Angolano: Desafios e Oportunidades*. Luanda: Editora da Universidade Agostinho Neto, 2020.

Costa, J. M. (2019). *Regulação Financeira e Inovações Tecnológicas na Europa*. Lisboa: Leya.

Costa, J. (2016). *O sigilo bancário em Portugal: Limites e exceções.* Revista de Direito Financeiro, 32(4), 567-588

Constituição da República Portuguesa Anotada, Coimbra Editora, 2007, p. 465).

Constituição Portuguesa Anotada, Almedina, 2010, vol. I, p. 310

Cordeiro, A. M. (2017). *Direito Bancário em Portugal*. Almedina.

Cordeiro, A. M (2019). *O Sigilo Bancário e a Constituição*. Coimbra Editora.

Cunha, R. (2020). *A Proteção de Dados Financeiros e o Papel das Instituições*. Porto Alegre: Editora Bancária.

Calabrich, B.F. C. (2020). *O sigilo de dados bancários no brasil, ontem e hoje: entre o direito à intimidade e o dever de compartilhamento. Artigo.* Brasil

Canotilho, G. J. J, Moreira V. (2007). *Constituição da República Portuguesa anotada*. Vol. I, 4ª edição revista. Coimbra editora.

Cordeiro, A. *Sigilo Bancário*, Universidade de Coimbra, Boletim da Faculdade de Direito, Vol. 77, Coimbra.

Cordeiro, A. (2016). *Direito Bancário*. 6ª edição. Coimbra. Almedina.

Coelho, V. R.F. (2012). *Sigilo Bancário: Problemas Fiscais e Constitucionais.* Universidade Católica Portuguesa – Centro Regional do Porto Escola de Direito. Dissertação de mestrado, Porto. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/16054/1/16054.pdf

Costa, L., & Almeida, M. (2022). *Impactos do Sigilo Bancário na Segurança Financeira Global*. Revista de Finanças Internacionais, 15(3), 45- sixty.

Cordeiro, J. (2017). *A Privacidade e o Sigilo Bancário em Portugal*. Lisboa: Almedina.

Cordeiro, A. M. (2017). *Direito Bancário*. Almedina.

Ferreira, A. P., (2004). *Atividade Bancária - Coletânea de Legislação*. Lisboa - Quid Júris.

Fernandes, B., Rodrigues, J. J. P. C., & Silva, F. (2019). *Security issues in banking systems: The effect of cyberattacks*. Journal of Information Security and Applications, 45, 32-45.

Frota, M. (2018). *Direitos do Consumidor Bancário*. Lisboa: Almedina.

Daniel S. (2024). *Os Desafios de Privacidade na Era da Inteligência Artificial.*

Disponível em: Daniel Solove aborda os Desafios de Privacidade na Era da Inteligência Artificial (substack.com)

David, J. (2017). *The Cybersecurity Canon: Data and Goliath: The Hidden Battles to*

Collect Your Data and Control Your World. Disponível em: The Cybersecurity Canon: Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.

Dente, N. M. (2019). *O levantamento do sigilo bancário no regime especial de IVA de*

Caixa. Disponível em: O levantamento do sigilo bancário no regime (especial) de IVA de caixa

Europol. (2021). *Relatório sobre Criptoativos e Atividades Ilícitas* (*Bitcoin*).

Foley, S., Karlsen, J., & Putniņš, T. J. (2019). Sex, Drugs, and *Bitcoin*: How Much Illegal Activity Is Financed Through Cryptocurrencies? *The Review of Financial Studies*, 32(5), 1798-1853.

Ferreira, M. (2019). *Segurança Cibernética e o Sigilo Bancário: Desafios da Era Digital*. Lisboa: Editorial Universitária.

Fernandes, Carla. *O Sigilo Bancário na Era Digital: Desafios e Oportunidades em Angola*. Luanda: Editorial Nacional de Angola, 2021.

Garoupa, N. (2020). *Direito e Economia: Uma Introdução*. Almedina

Gai, K., Qiu, M., & Sun, X. (2018). A survey on fintech. *Journal of Network and*

Computer Applications, 103, 262-272.

Gil, A. C. (2002). *Métodos e técnicas de pesquisa social* (6ª ed.). São Paulo: Atlas.

Gil, A. C. (2019). *Como elaborar projetos de pesquisa* (6ª ed.). São Paulo: Atlas.

Global Economy. Ithaca: Cornell University Press.

GOMES, Ricardo. *Sigilo Bancário e Cooperação Internacional: Desafios e Implementações em Portugal e Angola*. Coimbra: Almedina, 2022

Gomber, P., Koch, J.-A., & Siering, M. (2017). *Digital finance and fintech: current research and future research directions*. Journal of Business Economics, 87(5), 537-580.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, W. (2017). *On the FinTech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services.* Journal of Management Information Systems, 35(3), 220-239.

Gonçalves, D., & Pinho, A. (2020). *Ataques Cibernéticos e a Fragilidade do Sistema Bancário*. Rio de Janeiro: Finanças e Direito.

Gonçalves, A.M. (2017). *Sigilo Bancário e Proteção de Dados: Desafios Atuais*. Coimbra: Almedina.

Habermas, J. (1992). *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. MIT Press.

Hines, J. R. (2010). *Treasure Islands: Tax Havens and the Men Who Stole the World*. New York: Portfolio.

Internet Archive ( ). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Disponível em*: Bitcoin*: Satoshi Nakamoto: Free Download, Borrow, and Streaming : Internet Archive

Javelin Strategy & Research. (2020). *2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis*. Aliança para Proteção de Identidade.

Kuner, C. (2017). *Transborder Data Flows and Data Privacy Law*. Oxford University

Press.

Lakatos, E. M., & Marconi, M. A. (2017). *Fundamentos de metodologia científica* (7ª ed.). São Paulo: Atlas.

Lima, T. (2021). *Consentimento Informado e a LGPD: Desafios no Setor Bancário*. São Paulo: Jurídica Editorial.

Lima, J. (2021). *Proteção de Dados e Privacidade: Desafios na Era Digital*. Lisboa: Almedina.

Luhmann, N. (1996). *Trust and Power*. Wiley.

Matias, S. A. (1999). *Direito bancário*. Coimbra. Almedina

contextos e tendências. (dissertação de mestrado, Lisboa, Portugal).

Marques, A. C.L (2016). *O sigilo bancário na relação jurídica fiscal.* Faculdade de Direito da Universidade Nova de Lisboa. Disponível em: https://run.unl.pt/bitstream/10362/19843/1/LopesMarques_2016.pdf.

Martins, C. (2018). *Transparência e Responsabilidade nas Instituições Financeiras*. Porto: Porto Editora.

Marques, J. P. (2016). *Direito Bancário e Financeiro*. Almedina.

Mendes, P. (2017). *Lavagem de Dinheiro e Sigilo Bancário: Um Estudo Comparado*. Coimbra Editora.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G., & Savage, S. (2013). A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In *Proceedings of the 2013 Conference on Internet Measurement Conference*.

Martins, Sofia & Costa, Pedro. (2018). *Cooperação Internacional no Combate à Evasão Fiscal*. Lisboa: Edições Sílabo.

Martins, F. (2018). *Responsabilidade dos Bancos e a Proteção de Dados*. Porto Alegre:

Revista de Direito Bancário.

Martins, P. (2019). *Privacidade e Interesse Público: A Dualidade do Sigilo Bancário.* Estudos de Direito Bancário, 45(2), 112-130.

Matias. P, J. (2001). *Manual de metodologia da pesquisa científica* (1ª ed.). São Paulo: Atlas.

Marques, A. C. L. *O sigilo bancário na relação jurídica fiscal*. Dissertação. Faculdade de Direito (Universidade Nova de Lisboa). Disponível em: https://run.unl.pt/bitstream/10362/19843/1/LopesMarques_2016.pdf

Marques, J. (2016). *Direito Bancário e Financeiro*. Almedina.

McKinney, E., & Yoos, C. J. (2014). Information about information: A taxonomy of views. *MIS Quarterly*, 38(3), 591-616.

Menezes Cordeiro, A. (2019). *Direito Bancário e Segredo Financeiro*. Coimbra Editora.

Mersch, Y. (2018). Financial innovation and central bank policies. *Journal of Banking & Finance*, 78, 1-12.

Mersch, Y. (2018). The European Central Bank and the new normal of banking regulation. *Journal of Financial Regulation*, 4(2), 159-174.

Milne, G. R. (2016). Privacy and ethical issues in database/interactive marketing and public policy: a research framework and overview of the special issue. *Journal of Public Policy & Marketing*, 19(1), 1-6.

Milne, A. (2016). Consumer Data in the Financial Sector: Risk, Trust and Compliance. *Journal of Consumer Policy*, 39(2), 121-143.

Nogueira, J. A. (2021). *Fiscalidade e Justiça Tributária em Portugal*. Almedina.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://satoshi.nakamotoinstitute.org/emails/cryptography/1/

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press. https://archive.org/details/bitcoin-a-peer-to-peer-electronic-cash-system

Novais, J. R. (2019). *Constituição e Justiça Fiscal*. Almedina.

Nogueira, J. A. (2020). *Fiscalidade e Justiça Tributária*. Almedina.

Oliveira, R. (2021). *Transparência e Responsabilização nas Instituições Financeiras*. Editora Universitária.

Ocampo, J. A., & Stiglitz, J. E. (2011). *Time for a Visible Hand: Lessons from the 2008 World Financial Crisis*. Oxford University Press.

O'NEIL, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown. ISBN 9780553418811

Palan, R., Murphy, R., & Chavagneux, C. (2010). *Tax Havens: How Globalization Really Works*. Cornell University Press.

Pais, A. (2016). *Sigilo Bancário e Intervenção Fiscal: Uma Análise Crítica*. Almedina.

Picciotto, S. (1999). *International Business Taxation: A Study in the Internationalization of Business Regulation*. Quorum Books.

Pereira, A. (2001). *Metodologia da Investigação*. Lisboa: Edições Sílabo.

Pereira, A. (2018). *Desigualdades na Aplicação da Lei e Sigilo Bancário*. Journal de Direito e Sociedade, 12(2), 123-140.

Pires, C. A. B. (2013). *O consumidor e a comunicação do sector bancário em Portugal:*

Pinto, J. (2020). *A Luta Contra a Corrupção em Angola*. Leya.

Pinto, J. (2021). *A Transparência no Sistema Bancário Angolano*. Leya.

Pinheiro, C. (2019). *Privacidade Financeira e o Sigilo Bancário: Um Estudo Comparativo*. Lisboa: Instituto Jurídico.

Piteira, M. (2018). *Como fazer um trabalho académico* [Moodle]. Lisboa: ISCAL

Popper, K. R. (2002). *A lógica da pesquisa científica*. São Paulo: Cultrix.

Popper, K. (2002). *The Logic of Scientific Discovery*. London: Routledge.

Piketty, T. (2014). *Capital in the Twenty-First Century*. Cambridge: Harvard University Press.

Reis. R. (2018). *Fim do Sigilo Bancário*. Disponível em: Fim do Sigilo Bancário? - TGA

Ribeiro, F. (2023). *Privacidade vs. Segurança: O Debate sobre o Sigilo Bancário*. Estudos Jurídicos, 20(1), 89-105.

Rodrigues, M. (2015). *O Sistema Financeiro e o Combate ao Terrorismo em Angola*. Porto: Universidade do Porto.

Rodrigues, D. (2015). Código do Processo Tributário traz mais direitos mas precisa de Juízes. Disponível em: Código do Processo Tributário traz mais direitos mas 'precisa' de juízes.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students*. 8ª edição, Pearson Education Limited.

Santos, A. (2019). *O Sistema Financeiro Angolano: Regulação e Supervisão*. Almedina.

Santos, A. (2019). *Regulação Bancária em Angola: Desafios e Perspectivas*. Almedina.

Santos, J. (2019). *Interesses Privados e Públicos no Contexto do Sigilo Bancário*. Revista de Administração Pública, 53(4), 789-805.

Santos, A. C. (2014). *Direito Económico*. 7ª edição. Coimbra. Editora Almedina.

Nakamoto, S. (2008). *Bitcoin P2P e-cash paper.* Disponível em: Bitcoin P2P e-cash paper | Satoshi Nakamoto Institute

Shaxson, N. (2019). *The Finance Curse: How Global Finance is Making Us All Poorer*. Penguin Books

Sharman, J. C. (2017). *The Despot's Guide to Wealth Management: On the International Campaign against Grand Corruption*. Cornell University Press.

no regulamento nº. 2016/679 da União Europeia. (dissertação de mestrado). Universidade de Coimbra. Lisboa

Sharman, J. C. (2017). *The Money Laundry: Regulating Criminal Finance in the.*

Sawaris, A. (2017). *A tutela do direito à reserva sobre a intimidade da vida privada.*

Silva, A. (2013). *O Sigilo Bancário e as Exigências da Globalização*. Lisboa: Almedina.

Silva, T. (2020). *Atividades Ilícitas e a Proteção do Sigilo Bancário*. Revista Brasileira de Direito Financeiro, 8(1), 67.

Silva, A. P. (2021). *Proteção de Dados Pessoais no Setor Bancário*. Coimbra: Almedina.

Simas, P. (2019). "*O Sigilo Bancário e a Fiscalidade*". Revista de Direito Financeiro, 25(2), pp. 123-145.

Schatsky, D., Muraskin, C., & Gurumurthy, R. (2018). *Intelligent automation: How artificial intelligence is transforming the future of work*. Deloitte Insights.

Schwartz, P. (2019). "O Equilíbrio Entre Sigilo Bancário e Interesses Públicos". *Revista de Direito Tributário Contemporâneo*, 15(3), pp. 87-102.

Sturzenegger, L. C. (2003). *Sigilo Bancário e Sua Quebra no Direito Brasileiro*. São Paulo: Editora Revista dos Tribunais.

Sullivan, A. (2019). *The Economics of Tax Havens*. London: Routledge.

Tavares, D.P. 2021. *O Segredo Bancário Na Legislação Bancária De Angola, Cabo Verde Moçambique*. Disponívelem:https://run.unl.pt/bitstream/10362/19843/1/LopesMarques_2016.pdf.

Torres, H., (2016). *Português envolvido em escândalos de offshores*. Público. Disponível em: https://www.publico.pt/2016/04/03/mundo/noticia/portuguesenvolvido-em-fuga-de-informacao-sobre-offshores. Consultado em 25/10/2023.

Vasconcelos, M. P. *Direito bancário*. (2022). 4ª edição. Almedina. ISBN: 97894007357.

Vasques, S (2012). *Manual de Direito Fiscal*, Coimbra, Almedina, 2012

Vieira de Andrade, M. (2019). *Os Direitos Fundamentais na Constituição*. Coimbra Editora.

Williams, A. I. (2022). *Book Review - Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. Disponível em:* Book Review - Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World | American University, Washington, D.C.

Zarsky, T. Z. (2016). *Incompatible: The GDPR in the Age of Big Data*. Seton Hall Law Review, 47, 995-1020.

Zucman, G. (2015). *The Hidden Wealth of Nations: The Scourge of Tax Havens*. University of Chicago Press.

Zucman, G. (2017). *The Hidden Wealth of Nations: The Scourge of Tax Havens*. University of Chicago Press.

Zohar, A. (2020). *Data Privacy and Digital Banking: A New Paradigm*. Financial

Times Press.

Jurisprudência

Acórdão n.º 206/13. (2013). Jurisprudência do Supremo Tribunal de Justiça. Disponível em: www.stj.pt.

Acórdão (2020). *Processo nº 7278/20.1T9LSB-AL1-3*. Disponível em: Acordão de 2021-01-20 (Processo nº 7278/20.1T9LSB-AL1-3) | DR.

Acórdão do Tribunal da Relação de Coimbra. (2018). *Processo nº 1771/18.3T8PBL-B.C1*. Disponível em http://www.dgsi.pt/jtrc.nsf/8f.

Decreto-Lei n.º 298/92. (1992). *Regime Geral das Instituições de Crédito e Sociedades Financeiras*.

Tribunal da Relação de Guimarães. (2021). *Processo nº 3739/20.0T8BRGA.G1*. Disponível em http://www.gde.mj.pt/jtrg.nsf/86c.

Tribunal da Relação de Lisboa. (2021). *Processo nº 7278/20.1T9LSB-A L1-3*. Disponível em: https://jurisprudencia.pt/acordao/19917 2/

Legislação

– Lei n.º 37/2010, de 02 de setembro de Lisboa
– Decreto-Lei n.º 23/2019, de 30 de janeiro
– Lei n.º 16/10, de 15 de julho (Lei do Banco Nacional de Angola)
– Lei n.º 12/05, de 17 de junho (Lei de Bases do Sistema Financeiro)
– Lei nº 5/05 de 29 de julho (Lei do Sistema de Pagamentos de Angola)
– Decreto n.º 16/09/1886, de 20 de setembro (Código Penal)
– Decreto-Lei n.º 47344, de 25 de novembro de 1966 (Código Civil)
– Aviso do Banco Nacional de Angola n.º 05/2012, de 29 de março Código de conduta dos trabalhadores do Banco Nacional de Angola
– Lei N.º 16/10 De 15 de Julho. Disponível em: https://www.ine.gov.ao/Arquivos/Geral/Lei-do-Banco-Nacional-de-Angola.pdf)
– Lei nº 67/98, de 26 de outubro: Regula o sigilo bancário em Portugal.
– Regulamento Geral sobre a Proteção de Dados (RGPD) – Regulamento (UE) 2016/679: Regulamenta o tratamento de dados pessoais na União Europeia.
– Banco de Portugal: Publicações e regulamentações sobre sigilo bancário e segurança financeira.
– Autoridade Bancária Europeia (EBA): Normas e orientações sobre compliance no setor financeiro.
– Lei n.º 12/05, de 23 de setembro (Angola)
– Regime Geral das Instituições de Crédito e Sociedades Financeiras (Portugal)
– Código Penal Português
– Lei n.º 5/2002 de 11 de janeiro (Portugal)
– Relatórios do Banco Nacional de Angola (BNA) sobre regulação financeira
– Documentos judiciais relativos à Operação Marquês (Portugal)
– Regulamento (UE) n.º 679/2016, de 27 de Abril
– Lei n.º 5/2002, de 11 de janeiro. Diário da República n.º 9/2002, Série I-A de 2002-01-11. Disponível em: https://dre.pt/dre/detalhe/lei/5-2002-392861
– Lei N.º 16/10 de 15 de julho. Lei de Combate ao Branqueamento de Capitais e Financiamento do Terrorismo.
– Lei n.º 12/2015, de 17 de junho. Lei das Instituições Financeiras.

– Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD).
– Diário da República

Apêndices

Inquérito

Inquérito: Sigilo Bancário nas Relações das Instituições Bancárias com os seus Clientes na Era Digital

Objetivo: Este inquérito tem como objetivo compreender como as instituições financeiras garantem a privacidade e a segurança das informações de seus clientes, identificar os principais riscos da era digital e avaliar a adequação das legislações atuais para lidar com esses desafios.

---

1. Quais as medidas sua instituição implementa para garantir o sigilo bancário dos clientes?

- ( ) Políticas rigorosas de acesso restrito.
- ( ) Criptografia de dados.
- ( ) Auditorias e monitoramento contínuo.
- ( ) Treinamento especializado para trabalhadores.
- ( ) Outras: _____

2. Você considera que a formação oferecida sobre proteção de dados é suficiente?

- ( ) Sim, a formação cobre todos os aspetos essenciais.
- ( ) Sim, mas precisa de atualizações constantes.
- ( ) Não, faltam abordagens práticas e exemplos reais.
- ( ) Não, deveria ser mais específica e personalizada para diferentes funções.

3. Como sua instituição garante a privacidade e segurança das informações dos clientes na era digital?

- ( ) Criptografia de dados em trânsito e em repouso.
- ( ) Sistemas de autenticação multifator.
- ( ) Monitoramento de ameaças em tempo real.

- ( ) Políticas de acesso restrito a dados sensíveis.
- ( ) Outros: _____

4. Quais você acredita serem os maiores riscos digitais associados à privacidade de dados bancários?

- ( ) Ciberataques (*hackers, phishing, malware*).
- ( ) Uso inadequado de *big data* e IA.
- ( ) Fraudes internas ou externas.
- ( ) Falhas de sistemas legados.
- ( ) Outros: _____

5. Você considera que as legislações atuais (como RGPD, GDPR) são adequadas para proteger o sigilo bancário na era digital?

- ( ) Sim, as legislações atuais são suficientes.
- ( ) Sim, mas precisam de adaptações para novas tecnologias.
- ( ) Não, as legislações estão desatualizadas.
- ( ) Não tenho conhecimento suficiente sobre as legislações.

6. Quais são os maiores desafios para a sua instituição ao cumprir as legislações de proteção de dados (RGPD, GDPR)?

- ( ) Adaptar os processos internos para conformidade.
- ( ) Monitorar e relatar possíveis incidentes.
- ( ) Capacitar todos os trabalhadores sobre as exigências legais.
- ( ) Equilibrar inovação com conformidade regulatória.
- ( ) Outros: _____

7. Como a sua instituição responde a possíveis vazamentos de dados?

- ( ) Implementação de um plano de resposta a incidentes.
- ( ) Notificação imediata às autoridades competentes e aos clientes.

- ( ) Revisão de políticas internas e reforço das práticas de segurança.
- ( ) Oferecimento de monitoramento de crédito gratuito aos clientes afetados.
- ( ) Outros: _____

8. Há protocolos específicos para o tratamento de dados sensíveis dos clientes?

- ( ) Sim, há políticas claras e definidas.
- ( ) Sim, mas precisam ser mais detalhadas.
- ( ) Não tenho conhecimento sobre esses protocolos.
- ( ) Não existem protocolos específicos.

9. Você percebe um aumento na procura por serviços digitais que exigem maior proteção de dados?

- ( ) Sim, especialmente com o aumento dos serviços de internet banking.
- ( ) Sim, mas a demanda ainda é moderada.
- ( ) Não, a demanda permanece estável.
- ( ) Não, não percebo um aumento relevante.

10. Como sua instituição lida com as regulamentações de proteção de dados, como a LGPD ou RGPD?

- ( ) Cumprimento total das exigências regulatórias.
- ( ) Atualizações constantes nas políticas de privacidade e segurança.
- ( ) Revisão frequente dos processos para garantir conformidade.
- ( ) Capacitação regular dos trabalhadores sobre as regulamentações.
- ( ) Outros: _____

11. Existe uma cultura de conscientização sobre privacidade dentro da sua instituição? Como ela se manifesta?

- ( ) Sim, com treinamentos frequentes e campanhas de conscientização.
- ( ) Sim, mas poderia ser mais difundida entre os trabalhadores.

- ( ) Não, há pouco foco em privacidade no dia a dia.
- ( ) Não tenho conhecimento sobre iniciativas de conscientização.

12. Que tipo de tecnologia a sua instituição utiliza para proteger informações dos clientes?

- ( ) Criptografia de ponta a ponta.
- ( ) Monitoramento em tempo real de ameaças.
- ( ) Autenticação multifator (MFA).
- ( ) Uso de inteligência artificial para detetar atividades suspeitas.
- ( ) Outros: _____

13. Na sua opinião, como as novas tecnologias (IA, *big data*) afetam a privacidade e segurança das informações bancárias?

- ( ) Melhoram a capacidade de detetar fraudes.
- ( ) Aumentam os riscos de vazamentos devido ao maior volume de dados.
- ( ) Criam novos desafios de segurança.
- ( ) Facilitam a conformidade com regulamentações.
- ( ) Outros: _____

Para a População

Objetivo: Este inquérito busca compreender as perceções dos clientes sobre a privacidade e a segurança de suas informações bancárias, identificar os principais riscos na era digital e avaliar se as legislações atuais são suficientes para garantir a proteção dos dados.

---

1. Você se sente seguro ao realizar transações bancárias *online*?

- ( ) Sim, confio nas medidas de segurança implementadas pelo banco.
- ( ) Sim, mas estou sempre atento a possíveis fraudes.
- ( ) Não, tenho receio de sofrer algum tipo de ataque cibernético.
- ( ) Não, já passei por problemas de segurança no passado.

2. Você conhece os seus direitos em relação à proteção de dados pessoais?

- ( ) Sim, conheço bem meus direitos.
- ( ) Sim, mas tenho dúvidas sobre alguns aspetos.
- ( ) Não, não estou familiarizado com esses direitos.

3. Já teve alguma experiência negativa relacionada ao sigilo bancário?

- ( ) Sim, já tive problemas de segurança com minhas informações.
- ( ) Não, nunca tive experiências negativas.
- ( ) Prefiro não responder.
- Descrição: _____

4. Você confia na sua instituição financeira em relação à proteção de suas informações pessoais?

- ( ) Sim, confio plenamente.
- ( ) Sim, mas acho que sempre há riscos.
- ( ) Não, tenho minhas reservas quanto à segurança dos meus dados.

- ( ) Não, já tive problemas no passado.

5. Quais canais você utiliza para se informar sobre a segurança dos seus dados bancários?

- ( ) Informações no site oficial do banco.
- ( ) Atendimento ao cliente do banco.
- ( ) Reportagens e notícias sobre segurança bancária.
- ( ) Redes sociais e fóruns de discussão.
- ( ) Não procuro informações sobre o tema.

6. Na sua opinião, quais as medidas que deveriam ser tomadas pelas instituições para melhorar a segurança dos dados?

- ( ) Melhorar a comunicação com os clientes sobre práticas de segurança.
- ( ) Investir mais em tecnologia de segurança (IA, criptografia).
- ( ) Implementar autenticação em dois fatores para todas as transações.
- ( ) Realizar campanhas educativas sobre proteção de dados.
- ( ) Outras: _____

7. Você utiliza autenticação em dois fatores em suas contas bancárias?

- ( ) Sim, acredito que aumenta a segurança.
- ( ) Sim, mas acho um processo complicado.
- ( ) Não, não vejo necessidade.
- ( ) Não, porque não sei como ativar essa função.

8. Quais são as suas principais preocupações em relação ao sigilo bancário na era digital?

- ( ) Acesso não autorizado aos meus dados pessoais.
- ( ) Ciberataques e fraudes.
- ( ) Falha na proteção por parte do banco.

- ( ) Falta de informação clara sobre a segurança dos meus dados.
- ( ) Outras: _____

9. Acha que a legislação atual é suficiente para proteger seus dados bancários?

- ( ) Sim, acredito que as leis são adequadas e protegem bem os clientes.
- ( ) Sim, mas acredito que precisa de atualizações constantes.
- ( ) Não, acho que as leis não acompanham as novas tecnologias.
- ( ) Não tenho conhecimento suficiente para avaliar.

10. Como você acredita que a educação financeira pode ajudar na proteção do sigilo bancário?

- ( ) Ajudaria a identificar fraudes e golpes mais facilmente.
- ( ) Aumentaria a conscientização sobre a importância de proteger dados pessoais.
- ( ) Melhoraria o entendimento das medidas de segurança oferecidas pelos bancos.
- ( ) Não acredito que a educação financeira tenha grande impacto nesse aspeto.