



INSTITUTO POLITÉCNICO DE BEJA

Escola Superior de Tecnologia e Gestão

Mestrado em Contabilidade e Finanças



**O combate ao branqueamento de capitais à luz do Regime Geral
de Proteção de Dados (RGPD): informação, circuitos e
documentos de suporte**

Raquel Lourenço Guerreiro

Beja

2022

INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Contabilidade e Finanças

**O combate ao branqueamento de capitais à luz do Regime Geral
de Proteção de Dados (RGPD): informação, circuitos e
documentos de suporte**

**Dissertação de mestrado apresentada à Escola Superior de Tecnologia e
Gestão do Instituto Politécnico de Beja**

Elaborado por: Raquel Lourenço Guerreiro
Orientado por: Professor Doutor Carlos Manuel Lopes Borralho

Beja
2022

Agradecimentos

A primeira pessoa a quem dirijo os meus mais sinceros agradecimentos é ao Professor Doutor Carlos Borralho. Com o Professor Carlos Borralho recordei que adoro estudar, aprender e investigar. Inspirou-me e teve sempre as palavras de incentivo, no momento certo. É um professor muito completo e que respira a vontade de ensinar e também de aprender. É realmente uma pessoa inspiradora e um exemplo do que um professor deve ser, um exemplo para o seu aluno, um mestre sempre dedicado e altruísta.

A escolha deste tema foi bastante influenciada pela leitura do seu livro “Informação de Gestão de Processos de Negócio” e pela frequência das aulas de Gestão de Processos de Negócio e Informação, onde encontrámos pontos de interesse e temáticas de investigação em comum, pelo que a sua escolha como orientador já há muito estava feita, mesmo antes da escolha definitiva da temática de investigação.

Aos meus pais e marido pelo incentivo e pela disponibilidade de cuidarem dos meus filhos e colmatarem tão bem as minhas ausências.

À minha irmã e aos meus cunhados agradeço a revisões dos meus trabalhos, o espírito crítico e a disponibilidade sempre demonstrada.

Não posso ainda deixar de agradecer aos colaboradores do Banco BPI, que se disponibilizaram para a realização das entrevistas e questionários e me dedicaram parte do precioso tempo das suas agendas, e ao próprio banco que as autorizaram, e em particular ao Dr. André Henriques.

Sozinha não teria sido possível. Obrigada a todos.

Resumo

O Regulamento Geral de Proteção de Dados (RGPD), de aplicação obrigatória desde 25 de maio de 2018, criou nas empresas portuguesas a necessidade de realização de uma série de adaptações para cumprimento do regulamento. A matéria da proteção de dados é de relevância transversal a todas as sociedades, e onde o conflito de direitos, liberdades e garantias, está sempre patente, mas cuja aplicação e operacionalização podem condicionar a eficiência das organizações.

A prevenção e combate ao branqueamento de capitais e financiamento ao terrorismo é uma matéria igualmente atual e comum aos objetivos dos vários governos, num mundo cada vez mais globalizado e tecnológico, o que leva à necessária cooperação não só entre países, mas também entre as várias instituições públicas e privadas e os governos, com relevância para o sistema financeiro.

A operacionalização dos normativos que regem estas matérias não é assim dissociável da recolha e tratamento tempestivo de dados, bem como da existência de fluxos de trabalho que se pretendem, simultaneamente, eficientes e orientados para a efetivação dos direitos e dos deveres dos intervenientes. O presente estudo visa aferir se a entrada em vigor do RGPD alterou a atividade bancária, no que toca ao combate ao branqueamento de capitais e financiamento ao terrorismo e a realização de propostas de melhoria à implementação, facilitação e operacionalização da conjugação destas duas figuras na atividade bancária, na ótica da eficiência.

Relativamente ao método seguiu-se uma estratégia de investigação de estudo de caso, de natureza mista, tendo-se assumido um posicionamento ontológico relativista e um posicionamento epistemológico interpretativista.

Para recolha de dados, para além da observação e análise de documentos, recorreu-se à realização de entrevistas e questionários. O tratamento dos dados recolhidos foi feito com recurso à técnica de análise categorial de conteúdo e testes estatísticos não paramétricos.

O trabalho desenvolvido permitiu a identificação de tarefas que podem ser padronizadas ou mesmo eliminadas, bem como a sinalização de propostas de melhoria que permitem por sua vez o aumento da eficiência, no sentido de como a combinação de práticas bancárias permitem minimizar o consumo de recursos mantendo resultados ou, em alternativa, que permitam os melhores resultados mantendo o consumo de recursos, tendo sempre por base a operacionalização dos normativos que se pretenderam estudar.

Palavras-chave: Regulamento Geral de Proteção de Dados Pessoais; Branqueamento de Capitais e Financiamento ao Terrorismo; Sigilo Bancário; Eficiência.

Abstract

The General Data Protection Regulation (GDPR), entered into force on 25th May 2018, created in the portuguese companies the need to adopt several adaptations in order to accomplish this regulation. The data protection subject has a transversal relevance in all societies and where the conflict of rights, freedoms and guarantees is always present, but his application and operation can conditionate the efficiency of the organizations.

The prevention and fight against the money laundering is an equally current issue and it's a common goal of many governments, in an increasingly globalized and technological world, what leads to the need for cooperation not only between countries, but also between the public and private institutions and the governments, especially in the financial system.

The practical application of the laws cannot be dissociated from the timely collection and processing of data, as well as the existence of workflows that are intended to be, simultaneously, efficient, and oriented towards the realization of the rights and duties of those involved. The present study aims to assess whether the entry into force of the GDPR changed banking activity, regarding the fight against money laundering and terrorist financing and aims to make proposals to improve the implementation, facilitation, and operationalization of the combination of these two figures in the bank activity, from the point of view of efficiency.

Regarding the method domain, a case study investigation strategy was followed. This work assumes a relativist ontological position and an interpretive epistemological position.

For data collection, in addition to the observation and documents analysis, interviews and questionnaires were carried out. The treatment of the collected data was done by using the technique of categorical content analysis and nonparametric statistical tests.

The work that we have developed made possible to identify tasks that can be standardized or even eliminated, as well as the identification of improvement proposals that will allow the increase of efficiency in terms of how the combination of bank practices will minimize the resources consumption, maintaining the same results, or otherwise, that better results can be achieved, maintaining the same resource consumption, always regarding the operationalization of the rules and legislation that we intent to study.

Keywords: General Data Protection Regulation; Money Laundering and Terrorist Financing; Bank Secrecy; Efficiency.

1.	INTRODUÇÃO.....	1
1.1	QUESTÃO DE INVESTIGAÇÃO E OBJETIVOS.....	2
1.2	ESTRUTURA DA DISSERTAÇÃO	4
2.	REVISÃO DA LITERATURA.....	6
2.1	PROTEÇÃO DE DADOS PESSOAIS	6
2.1.1	<i>Enquadramento e evolução do processo legislativo</i>	<i>8</i>
2.1.2	<i>Direitos a proteger e princípios orientadores.....</i>	<i>12</i>
2.1.3	<i>A necessidade de ponderação de interesses e o risco da discricionariedade</i>	<i>16</i>
2.1.4	<i>O tratamento de dados pessoais nos bancos.....</i>	<i>17</i>
2.2	SIGILO BANCÁRIO	20
2.2.1	<i>Enquadramento e evolução do processo legislativo</i>	<i>20</i>
2.2.2	<i>Sigilo bancário e direito à reserva da intimidade da vida privada: restrições, violação e derrogação</i> <i>22</i>	
2.2.3	<i>A necessidade de ponderação de interesses e o risco de discricionariedade</i>	<i>25</i>
2.2.4	<i>O tratamento do sigilo nos bancos.....</i>	<i>27</i>
2.3	BRANQUEAMENTO DE CAPITAIS E FINANCIAMENTO AO TERRORISMO	27
2.3.1	<i>Enquadramento e evolução do processo legislativo</i>	<i>28</i>
2.3.2	<i>O dever de identificação e diligência.....</i>	<i>33</i>
2.3.3	<i>As limitações no combate ao branqueamento de capitais nos bancos.....</i>	<i>34</i>
2.4	O SETOR BANCÁRIO PORTUGUÊS: ENTIDADES REGULADORAS, DE SUPERVISÃO E PROCESSO LEGISLATIVO	38
2.5	FATORES CRÍTICOS NA COMPATIBILIZAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS, SIGILO BANCÁRIO E COMBATE AO BC/FT ...	39
2.5.1	<i>No domínio dos diplomas legais.....</i>	<i>39</i>
2.5.2	<i>No domínio da eficiência dos fluxos de trabalho.....</i>	<i>44</i>
2.5.3	<i>No domínio da informação: registos e documentos de suporte.....</i>	<i>45</i>
2.6	SÍNTESE.....	55
3.	MÉTODO.....	58
3.1	O CONTINUUM DA ABORDAGEM QUALITATIVA À QUANTITATIVA	59
3.2	O ESTUDO DE CASO COMO ESTRATÉGIA DE INVESTIGAÇÃO	62
3.3	DESENHO DE INVESTIGAÇÃO	64
3.4	TÉCNICAS DE RECOLHA DE DADOS	66
3.5	TÉCNICAS DE ANÁLISE DE DADOS	72
3.6	SÍNTESE.....	80
4.	RESULTADOS.....	81
4.1	O BANCO BPI SA	81
4.2	ANÁLISE QUALITATIVA.....	81
4.2.1	<i>Importância da compatibilização dos diplomas.....</i>	<i>84</i>
4.2.2	<i>Fatores críticos na implementação (RGPD, LBC e Sigilo Bancário).....</i>	<i>92</i>
4.2.3	<i>Aumento da eficiência associada a dados a recolher, momentos e fluxos</i>	<i>97</i>
4.2.4	<i>Redução da eficiência associada a dados a recolher, momentos e fluxos</i>	<i>104</i>
4.3	ANÁLISE QUANTITATIVA	111
4.4	SÍNTESE.....	116
5.	CONCLUSÕES	117
5.1	RESPOSTA ÀS QUESTÕES DE INVESTIGAÇÃO.....	117
5.1.1	<i>Questão 1</i>	<i>118</i>
5.1.2	<i>Questão 2</i>	<i>121</i>
5.2	LIMITAÇÕES E INVESTIGAÇÃO FUTURA	122
6.	BIBLIOGRAFIA	124
7.	ANEXOS	132

Índice de quadros

Quadro 1: Novos direitos dos titulares de dados	15
Quadro 2: Deveres preventivos	34
Quadro 3: Perspetivas e variáveis a considerar na aplicação do RGPD, BC/FT e Sigilo Bancário	49
Quadro 4: Vantagens e desvantagens da metodologia qualitativa	60
Quadro 5: Vantagens e desvantagens da abordagem quantitativa.....	61
Quadro 6: Ficheiro de Dados.....	78

Índice de figuras

Figura 1: Entidade reguladoras e de supervisão	38
Figura 2: Fases do estudo de caso	65
Figura 3: Desenho de investigação.....	66
Figura 4: Caracterização dos entrevistados	82
Figura 5: Nuvem de palavras.....	83

Lista de abreviaturas e siglas

ABC – Anti branqueamento de capitais

AEPD – Autoridade Europeia para a Proteção de Dados

AT – Autoridade Tributária

BC/FT – Branqueamento de Capitais e Financiamento ao Terrorismo

BdP – Banco de Portugal

BE – Beneficiário Efetivo

Comissão BC/FT – Comissão de Coordenação das Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CEDH – Convenção Europeia dos Direitos do Homem

CEPD – Comité Europeu para a Proteção de Dados

CMVM – Comissão do Mercado de Valores Mobiliários

CNPD – Comissão Nacional de Proteção de Dados

CP – Código Penal

CRP – Constituição da República Portuguesa

DPO – Data Protection Officer

GAFI – Grupo de Ação Financeira

KYC – *Know Your Customer*

KYP – *Know Your Process*

KYT – *Know Your Transaction*

LBC/FT – Lei de combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo

LGT – Lei Geral Tributária

PEP – Pessoa Politicamente Exposta

PQE – Prova de Qualidade de Emigrante

RCBE – Regime Central do Beneficiário Efetivo

RGICSF – Regime Geral das Instituições de Crédito e Sociedades Financeiras

RGPD – Regulamento Geral de Proteção de Dados

SI – Sistemas de informação

UE – União Europeia

1. Introdução

Através de um estudo de caso pretende-se discutir os efeitos do Regulamento Geral de Proteção de Dados (RGPD) e da Lei de combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo (LBC/FT) na eficiência dos processos de negócio de um banco. No estudo empírico é efetuado o levantamento de circuitos de dados, registos, documentos e momentos que permitem a operacionalização dos normativos subjacentes, numa ótica de eficiência, elemento fundamental da gestão. Naturalmente, aqui, a eficiência traduz o fulcro do trabalho, por ser entendida como condição necessária, ainda que não suficiente, para permitir alcançar os propósitos determinados nos diplomas legais.

A atualidade e pertinência da temática, pela recente publicação do RGPD, de aplicação obrigatória desde 25 de maio de 2018, e a necessária adaptação que as empresas portuguesas e, em particular os bancos portugueses, se veem obrigados a realizar para cumprimento do regulamento, foram elementos decisivos na escolha do tema. Além de a temática da proteção de dados pessoais ser sensível e de a sua relevância ser transversal a toda a sociedade, onde o conflito de interesses e de direitos existe sempre.

De igual relevância e atualidade é a prevenção do Branqueamento de Capitais e do Financiamento ao Terrorismo (BC/FT), que vincula países, instituições públicas e privadas, exigindo a constante cooperação entre as entidades sujeitas. Os bancos são um dos principais atores no combate a este tipo de criminalidade, sendo igualmente um meio bastante utilizado pelos autores deste crime.

A atividade bancária envolve a recolha, tratamento e armazenamento de dados dos clientes, dados esses que são usados para vários fins, como fins comerciais, publicidade e marketing, concessão de crédito, entre outros. A posse destes dados e a possibilidade da sua cedência pode consubstanciar uma violação do RGPD e por sua vez a violação do segredo bancário. Face a esta necessidade de proteção dos dados pessoais e à crescente política de combate ao BC/FT é essencial que haja adaptações na estrutura das organizações e nos fluxos de trabalho, com os custos associados e com eventuais alterações no relacionamento com os clientes.

Quer o RGPD quer o regime da prevenção ao BC/FT obrigam à recolha, registo e arquivo de documentos de suporte e informação, cujo cumprimento pelos bancos é o único meio de evitar as sanções legalmente previstas. Esta perspetiva de análise dos processos, os mecanismos de operacionalização e a sua conformidade com as normas é a que pretendemos adotar e investigar.

Não fica alheia a esta escolha o facto de a autora ser colaboradora na instituição bancária em estudo, o banco BPI, estando desperta e lidando com estas temáticas no seu dia a dia, situação que suscita a curiosidade e interesse, sendo também facilitadora no acesso a informação, numa perspetiva prática e útil para a instituição bancária e os seus colaboradores.

O sigilo bancário surge neste estudo quase como que uma temática obrigatória, como instituto

basilar a todo o sistema bancário, colaboradores e seus clientes, instituto este que está obrigatoriamente subjacente ao RGPD e ao BC/FT. Ainda que o sigilo bancário não viesse a ter um tratamento autónomo, nunca poderia ser esquecido pelo facto de a autora ser colaboradora de uma instituição bancária, para além de investigadora.

Depois de aferida a recetividade do banco BPI, pretendeu-se a realização de um estudo exaustivo que não só permitisse a conclusão com sucesso do grau de mestre em contabilidade e finanças, mas que fosse um trabalho útil e um contributo real para a entidade em questão e outros bancos, por analogia, na ótica da melhoria de eficiência, como um dos pilares da gestão.

A metodologia de análise escolhida, tendo por base os objetivos propostos foi de tipologia mista. Escolhemos o estudo de caso como estratégia de investigação, de abordagem mista e como técnicas de recolha de dados optou-se pela realização de entrevistas e questionários, para além da observação e da análise documental.

O ponto de partida da nossa dissertação foi uma visita ao estado da arte, tendo como objetivo principal perceber as problemáticas discutidas na doutrina.

As técnicas de análise de dados foram diversas tendo em consideração a avaliação mista pretendida, sendo que na avaliação qualitativa utilizámos a análise categorial de conteúdo, combinando o uso de grelhas com o *software* N-VIVO para compilação e interpretação inicial dos dados obtidos com recurso a entrevistas semiestruturadas. Tendo sempre por base as questões de investigação e objetivos definidos, na análise quantitativa foram realizados testes estatísticos aos dados apurados, com recurso aos 77 questionários que foram respondidos.

1.1 Questão de investigação e objetivos

Nesta investigação importa começar por apresentar a questão de partida, bem como os objetivos gerais e os específicos que sustentam o trabalho desenvolvido.

São aqui assumidas duas questões de investigação, especificamente:

- Como maximizar a eficiência na compatibilização da operacionalização do RGPD, com o sigilo bancário e com as restrições inerentes ao branqueamento de capitais, na entidade bancária objeto de estudo?
- Existem diferenças entre grupos quanto à forma como percecionam a compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário?

As questões assumidas ponderam a eficiência como a combinação de práticas bancárias que permitam minimizar o consumo de recursos mantendo resultados ou, em alternativa, que permitam os melhores resultados mantendo o consumo de recursos. Procura-se assim entender como otimizar a

aplicação prática dos normativos legalmente impostos, na entidade bancária considerada.

Segundo Marconi e Lakatos (2003) os objetivos gerais sustentam uma visão global e abrangente do tema de pesquisa. Assim, partindo das questões anteriores, os objetivos gerais aqui assumidos são os seguintes:

- Sistematizar a legislação europeia e a sua transposição para o ordenamento jurídico português em matéria de proteção de dados pessoais e BC/FT;
- Analisar as implicações da aplicação simultânea do RGPD, do sigilo bancário e da Lei de combate ao BC/FT;
- Ponderar a aplicação dos diferentes normativos na atividade bancária;
- Ponderar as fronteiras do sigilo bancário à luz do novo RGPD;
- Ponderar a necessidade de compatibilização entre o RGPD e o cumprimento dos requisitos impostos pela LBC/FT.

De acordo com Marconi e Lakatos (2003), os objetivos específicos apresentam um caráter mais concreto e delimitado, auxiliam o alcance do objetivo geral e ajudam a aplicá-lo a situações particulares.

Assim, a operacionalização dos normativos não é dissociável da recolha e tratamento tempestivo de dados, bem como da existência de fluxos de trabalho que se pretendem, simultaneamente, eficientes e orientados para a efetivação dos direitos e dos deveres dos intervenientes. Dessa forma são expressos os seguintes objetivos específicos:

- Elencar e caracterizar os dados a recolher, os momentos, os documentos e os fluxos de informação que permitam cumprir o RGPD e a Lei de combate ao BC/FT;
- Enumerar os fatores críticos na implementação simultânea do RGPD, sigilo bancário e Lei de combate ao BC/FT;
- Descrever e analisar fluxos de informação associados à operacionalização simultânea do RGPD e Lei de combate ao BC/FT;
- Aferir a existência, ou não, de diferenças na perceção de compatibilização, dificuldade na compatibilização, e eficiência na aplicação, do Regulamento Geral de Proteção de Dados com a Lei de combate ao BC/FT e com o sigilo bancário.

A perceção de compatibilização representa aqui a necessidade mais ampla de cumprimentos dos normativos legais. Já a dificuldade na compatibilização é entendida enquanto esforço requerido na realização de tarefas. Finalmente a eficiência, sinaliza a articulação de meios que, comparativamente a alternativas, permita fazer mais com os mesmos recursos ou, com menos recursos, fazer o mesmo.

Definidos que estão, as questões de investigação, bem como os objetivos gerais e específicos, a

presente dissertação será estruturada conforme se descreve no ponto seguinte.

1.2 Estrutura da dissertação

O relato da investigação realizada encontra-se estruturado em cinco capítulos, concretamente: Introdução, Revisão da literatura, Método, Resultados e Conclusões.

No capítulo 1 – Introdução – pretende-se dar a conhecer, resumidamente, qual a temática a abordar, as motivações para a sua escolha e a importância e pertinência do objeto de estudo. São reveladas nos subcapítulos as questões da investigação, os objetivos gerais e específicos que se pretendem alcançar, tal como a estrutura da dissertação.

O capítulo 2 – Revisão da literatura – encontra-se dividido em seis subcapítulos, individualizando o RGPD, o sigilo bancário e o BC/FT para, de seguida, enumerar potenciais fatores críticos na sua aplicação simultânea e compatibilização. Desta forma, em cada um dos subcapítulos, apresentam-se os elementos preponderantes de cada um dos enquadramentos legais aqui objeto de estudo. O primeiro subcapítulo é dedicado à proteção de dados pessoais, onde se fará o seu enquadramento legal e respetiva evolução, serão elencados os direitos que se visam proteger e os princípios orientadores do RGPD. Dada a diversidade de direitos que devem ser protegidos será abordada a necessidade de ponderação de interesses e o risco da eventual discricionariedade. Por último, e partindo sempre do geral para o específico será feita uma abordagem ao tratamento de dados pessoais nos bancos.

O segundo subcapítulo é referente ao sigilo bancário, onde também se fará o seu enquadramento legal e respetiva evolução. O sigilo bancário, podendo colocar em causa o direito à reserva da intimidade da vida privada, será analisado ainda sob o ponto de vista das derrogações, o que nos leva, tal como em relação à proteção de dados pessoais, à necessidade de ponderação de interesses e ao risco da eventual discricionariedade. Por último, e partindo uma vez mais do geral para o específico, será feita uma abordagem ao tratamento do sigilo bancário pelas entidades bancárias.

O BC/FT é tratado no terceiro subcapítulo, com uma abordagem semelhante à dos subcapítulos anteriores, dando-se ainda enfoque aos deveres de identificação e diligência, entre outros.

Seguem-se o quarto e o quinto subcapítulos, onde se comparam os referenciais com vista à identificação dos fatores críticos na compatibilização da proteção de dados pessoais, sigilo bancário e combate ao BC/FT. Esta abordagem é feita em três domínios: dos diplomas legais, da eficiência dos fluxos de trabalho e da informação: registos e documentos de suporte. É ainda feita uma breve abordagem ao sistema bancário em Portugal.

Por último, ainda no capítulo 2, apresenta-se uma síntese conclusiva dos três referenciais em estudo.

No capítulo 3 – Método – cada um dos seis subcapítulos pretende demonstrar o caminho seguido

no presente estudo. Neste capítulo é fundamentada a opção de recurso à estratégia de investigação baseada em estudo de caso, apresenta-se o desenho de investigação e caracterizam-se as técnicas de recolha de dados adotadas, bem como as técnicas de análise de dados. É ainda feita referência à abordagem mista.

O capítulo 4 – Resultados – apresenta e discute os dados recolhidos, descrevendo a aplicação das técnicas de análise de dados e procedendo à sua sistematização.

Por último, o capítulo 5 – Conclusões – é estruturado em dois subcapítulos, sendo que o primeiro pretende dar resposta às questões de investigação, alinhamento com os objetivos e sequência de procedimentos desenvolvidos. O segundo subcapítulo revela as limitações encontradas e apresenta sugestões para eventuais investigações futuras.

2. Revisão da literatura

A revisão da literatura aqui apresentada tem subjacente as matérias da proteção de dados pessoais, do sigilo bancário e do BC/FT. Para cada um dos três referenciais é apresentado um breve enquadramento e evolução do processo legislativo, os interesses a acautelar e o tratamento de dados e informação que lhe está associado. O propósito, no final deste capítulo, é o de inventariar os elementos críticos na aplicação dos normativos, no tratamento de dados e nos fluxos de trabalho a desenvolver. Esse tratamento de dados pode apresentar distintos níveis de eficiência, consoante a quantidade de dados, a redundância da recolha, os momentos, o formato dessa recolha, a reutilização de dados recolhidos, entre outros possíveis determinantes. A eficiência é assim indissociável dos sistemas de informação (SI) e do controlo de gestão. A “eficiência centra-se nos meios, na combinação de recursos” onde a recolha de dados e a geração de informação podem potenciar, ou dificultar, a realização de fluxos de trabalho, bem como o consequente alcance de resultados que os normativos aqui objeto de estudo assumem (Borrinho, 2018, p. 38). Também Silva C. P. (2010, p. 30) se refere à eficiência como tendo “subjacente a consideração da existência de um conjunto de agentes económicos que utilizam recursos (“inputs”) para produzir vários resultados (“outputs”), através de um processo produtivo. Os agentes mais eficientes são aqueles que para uma dada dotação de recursos (entenda-se “*status quo*”) utilizam menor quantidade de fatores por unidade de produto ou, que maximizam os outputs de forma a conseguir atingir um nível que seja mais favorável”.

No ponto seguinte efetua-se o enquadramento da matéria relativa à proteção de dados pessoais.

2.1 Proteção de dados pessoais

O RGPD estabelece no considerando n.º 1 que “a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental”. Existe assim o titular dos dados, cidadão merecedor de toda a proteção em toda a sua amplitude, e por outro lado, existem as empresas e organizações públicas e privadas a quem é imposta a obrigatoriedade de fazer cumprir essa proteção, no que aos dados pessoais diz respeito. Segundo Gonçalves (2003) existem dois interesses que se confrontam, o do próprio indivíduo que pretende ver as suas informações salvaguardadas e os interesses das entidades públicas ou privadas que pretendem prosseguir a sua atividade com eficiência. Cumpre-nos indagar o que são os dados pessoais, o que são direitos fundamentais e porque devem ser protegidos. Alguns esclarecimentos surgem do próprio RGPD e das definições que nos dá, mas será necessário recorrer ao estado da arte para um maior aprofundamento e compreensão.

De acordo com o art.º 4.º n.º 1 do RGPD são dados pessoais toda a “informação relativa a uma pessoa singular identificada ou identificável”. Magalhães e Pereira (2020) consideram que não existe uma lista taxativa com todos os dados que se consideram pessoais, tendo o legislador optado por uma definição bastante ampla do conceito de dados pessoais. Note-se, como afirma Cordeiro A. B. (2018, p.

1) que este conceito “vive um processo de mutação constante e que exige, fruto de avanços tecnológicos, aperfeiçoamentos cirúrgicos pontuais”.

Segundo o mesmo autor o conceito de informação pessoal abrange todos os aspetos relativos à pessoa, quer sejam familiares ou sociais, privados ou públicos, físicos ou mentais, e dá-nos exemplos – nome, data de nascimento, morada, características físicas como peso, género ou cor do cabelo, considerações íntimas que incluem crenças, posições profissionais ou académicas, títulos e graus ou estatutos profissionais e laborais, entre outros. Refere ainda a irrelevância da veracidade dos dados compilados e tratados e a aplicabilidade do RGPD, independentemente do formato em que a informação foi recolhida e do suporte em que está armazenada. No mesmo sentido, Magalhães e Pereira (2020) referem que o RGPD não tem vocação de se aplicar a todo e qualquer tratamento de dados, mas apenas ao tratamento de dados pessoais (onde não são abrangidos os dados das pessoas coletivas) que é realizado por meios total ou parcialmente automatizados, ou por meios não automatizados, desde que contidos em ficheiros ou se destinem a constar num ficheiro (conjunto estruturado de dados acessíveis em função de determinados critérios). Assim, consideram que tratamento de dados é qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem recurso a meios automatizados, sinalizando os seguintes:

- Recolha de dados;
- Registo desses dados;
- Organização de dados;
- Conservação;
- Adaptação ou alteração;
- Recuperação;
- Consulta;
- Utilização;
- Comparação ou interconexão;
- Apagamento;
- Destruição.

Importa considerar que “a definição dos dados pessoais (...) tem de cobrir todos os dados relativos a qualquer pessoa que esteja identificada, isolada, ou puder ser identificada ou isolada — seja pelo responsável pelo tratamento dos dados ou por qualquer outra parte” (Buttarelli, 2018, p. 2). Ainda segundo este autor e, na ótica das entidades que devem salvaguardar as informações, deverá haver controlo e fiscalização que assegurem o respeito das regras, o aumento de recursos e instrumentos fortes que permitam igualar a sua capacidade com o crescimento dos negócios baseados em dados.

Como já referido é o próprio RGPD que se refere à proteção de dados como um direito fundamental, e quando se fala em direitos fundamentais estamos no nível de tutela dada pelas constituições dos estados, pela Carta dos Direitos Fundamentais da União Europeia (CDFUE) e pela Convenção Europeia dos Direitos do Homem (CEDH). Esta foi adotada em 1950, pelo Conselho da Europa, tendo entrado em vigor em 1953 e tutela o direito à proteção de dados pessoais, prevendo no

seu art.º 8.º que “Todas as pessoas têm direito à proteção de dados de carácter pessoal que lhes digam respeito”. Melo (2019) refere que foi com base na CEDH e na Convenção 108, no contexto do Conselho da Europa, que a UE e os países da Europa desenvolveram o direito à proteção de dados e, em Portugal refere a Constituição da República Portuguesa (CRP) e a Diretiva 95/46/CE no âmbito do Direito da UE.

A CRP dispõe no art.º 35.º que “todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam”. Para Canotilho e Moreira (2014) estão aqui consagrados o direito de acesso e retificação dos registos informáticos, o direito ao sigilo em relação aos responsáveis de ficheiros automatizados e a terceiros, direito à sua interconexão e o direito ao não tratamento de certos tipos de dados pessoais.

Desta forma e antes de avançarmos para o enquadramento e evolução legislativa até à implementação do RGPD cumpra-nos apenas referir, conforme sugerido por Magalhães e Pereira, (2020) que o RGPD é um marco fundamental na regulação do tratamento de dados pessoais e pretende dar resposta aos desafios gerados pela evolução das novas tecnologias e pela globalização dos mercados. Referem assim que “Após vários anos de utilização massiva da rede para comunicar, comprar, promover produtos e aproximar as pessoas e as empresas, fica o sentimento de insegurança que resulta dessas relações virtuais, tendo considerado essencial devolver às pessoas singulares o controlo da utilização que é feita dos seus dados pessoais, devendo ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas”.

O RGPD reflete assim, a vontade do Parlamento Europeu e do Conselho da União Europeia em implementar um normativo sólido e coerente, de aplicação rigorosa e que permita gerar confiança, essencial ao desenvolvimento da economia digital no conjunto do mercado interno. Também em Portugal a proteção de dados tem o seu expoente máximo com a entrada em vigor do RGPD, contudo é matéria que há muito é discutida e de alguma forma protegida. Faremos de seguida uma viagem à sua origem e evolução.

2.1.1 Enquadramento e evolução do processo legislativo

O período pós 2.^a Guerra Mundial pode ser considerado como o ponto de partida para a tomada da consciência coletiva para necessidade de consagrar, sob o ponto de vista legal, o direito à vida privada, como forma de impedir a intrusão de governos e elementos do poder na esfera privada dos cidadãos (Guerreiro, 2018). A existência de bases de dados com dados pessoais que permitiram a ingerência de governos na vida privada dos cidadãos e a sua perseguição e discriminação tornou necessária a proteção do cidadão comum ao nível dos seus dados pessoais. Acresce o grande desenvolvimento das tecnologias de informação na década de setenta e a sua potencial utilização

também por entidades privadas. Segundo Raimundo (2012), a chegada da era da informática, em muito responsável pela sociedade em que coexistimos hoje e a facilidade de transmissão de dados, resultou na concessão de dignidade constitucional à proteção de dados pessoais.

No âmbito internacional, a Declaração Universal dos Direitos do Homem adotada pela Assembleia Geral das Nações Unidas, em 1948, foi, segundo Teves (2019), pioneira na consagração do direito à privacidade de cada indivíduo, tal como a Convenção Europeia dos Direitos do Homem, adotada em 1950 pelo Conselho da Europa, foi o primeiro instrumento jurídico vinculativo de direito internacional em matéria de direitos humanos, e o primeiro a consagrar o direito à privacidade.

A Convenção 108 (Convenção do Conselho Europeu para a Proteção dos Indivíduos face ao tratamento automático de dados pessoais) foi assinada em 28 de janeiro de 1981 e visou a sua aplicação ao setor público e ao setor privado aquando do tratamento de dados pessoais, como forma de proteção dos cidadãos contra abusos na sua recolha e tratamento, constituindo, segundo Guerreiro (2018), um marco histórico relevante no domínio da proteção de dados. As partes signatárias estão assim vinculadas a proteger os dados de carácter pessoal de todas as pessoas singulares que se encontrem no seu território, independentemente da sua nacionalidade. Em 2001 foi adotado um Protocolo Adicional com o intuito de estabelecer a obrigatoriedade de autoridades nacionais de supervisão e regular os fluxos de dados entre fronteiras.

Apesar da sua grande importância como indicadora dos princípios estruturantes em matéria de proteção de dados e de ser a principal fonte de inspiração da legislação que se lhe seguiu, a Convenção foi, por si só, ineficiente dada a necessidade de ser implementada internamente pelos estados signatários, de carecer de efeito direto e não poder ser invocada contra entidades privadas (Guerreiro, 2018).

No que concerne à evolução legislativa no contexto europeu Teves (2019) refere-se ainda à Carta dos Direitos Fundamentais da União Europeia, adotada em 2000 pelo Parlamento Europeu, pelo Conselho e pela Comissão, como mais um marco na consagração da proteção de pessoas singulares relativamente ao tratamento de dados pessoais. A Carta tornou-se vinculativa para os Estados-Membros com a entrada em vigor do Tratado de Lisboa, em dezembro de 2009.

A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 é o normativo principal que regulou a matéria de proteção de dados pessoais e livre circulação, no que toca a pessoas singulares até 25 de maio de 2018, e emerge pela crescente necessidade de harmonizar os normativos internos dos Estados-Membros face ao crescimento exponencial do mercado interno (Considerandos 3, 5 e 7 da Diretiva), demonstrando não só uma preocupação económica, mas também ética e social com livre circulação de dados na proteção dos cidadãos. A diretiva visa a proteção das liberdades e dos direitos fundamentais no que que concerne aos dados pessoais, com o intuito também de proteger e impulsionar o mercado único da comunidade, numa perspetiva de crescimento económico. A diretiva denota já uma preocupação com a transferência de dados para os países que não pertencem à

União Europeia (UE) e decreta a proibição da transferência de dados para aqueles que não garantam um nível de proteção adequada (Duarte S. A., 2018).

Sendo uma diretiva, pretendia-se a harmonização legislativa quanto a esta temática, obrigando a uma transposição pelos Estados-Membros. Em Portugal, a Diretiva 95/46/CE foi transposta pela Lei n.º 67/98, de 26 de outubro, Lei da Proteção de Dados Pessoais. Para Branco (2018, p. 7) “foi, indubitavelmente, a Diretiva 95/64/CE que desbravou o caminho que possibilitou e originou a aprovação do RGPD”. No mesmo sentido, Teves (2019) considera a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, a base do desenvolvimento das legislações nacionais de cada Estado-Membro no que toca à proteção de dados.

Contudo, as diferentes transposições realizadas pelos diversos países, a crescente evolução da economia digital e a constante partilha de informação a nível internacional levaram à necessidade de adoção do RGPD, como forma de unificar as práticas, aumentar a transparência em matéria de dados pessoais e efetivar a sua proteção.

O RGPD, revoga a Diretiva 95/46/CE e, sendo um regulamento, é de aplicação direta nos Estados-Membro, não necessitando de transposição. Visa para além da referida harmonização, a uniformização legislativa. Existiu um período de transição de dois anos, desde a sua aprovação definitiva a 14 de abril de 2016, sendo de aplicação obrigatória a partir de 25 de maio de 2018 (Duarte, 2019).

O RGPD surge com a necessária reformulação e inovação dos normativos existentes, numa UE de livre circulação de pessoas e bens e num contexto de avanço e desenvolvimento tecnológico, em que o acesso e o controlo de dados pessoais são uma constante, bem como o seu uso indevido pelas organizações. A rápida evolução tecnológica e a globalização criam novos desafios em matéria de proteção de dados pessoais, uma vez que estes são utilizados numa escala sem precedentes (Branco, 2018).

Segundo Duarte (2018, p. 27) “o regulamento tem como principais objetivos a harmonização, a cooperação e a coerência entre as Autoridades Nacionais, nesse sentido os artigos 62.º a 67.º. Constituir uma resposta à globalização e evitar *forum shopping*, ou seja, a escolha da jurisdição mais favorável dentro da União Europeia neste domínio e resulta como uma resposta ao reconhecimento da proteção de dados como uma matéria ao nível da União, depois do Tratado de Lisboa”. A mesma autora, referindo-se ao âmbito territorial do RGPD refere, citando o art.º 3.º do regulamento, que este se aplica também ao tratamento de dados feitos fora do território dos Estados-membros da UE, por responsáveis pelo tratamento e subcontratantes com estabelecimentos nestes, ao tratamento de dados de residentes na UE, por responsáveis pelo tratamento ou subcontratantes sem estabelecimentos na UE, se estes forem destinatários de ofertas de bens e serviços, mesmo sem pagamento direto, ou se existir controlo do seu comportamento. No mesmo sentido Cordeiro A. B. (2018), quanto à aplicação do RGPD aos sistemas de tecnologias da informação, aplicações e redes, em contexto empresarial ou corporativo e

organizacional.

A Lei n.º 58/2019 (e também a Lei n.º 59/2019), de 8 de agosto, é a nova lei de proteção de dados pessoais em Portugal e revoga a Lei n.º 67/98, de 26 de outubro. Apesar de o RGPD ser de aplicação direta no nosso país a Lei n.º 58/2019 vem assegurar a sua execução na ordem jurídica nacional, atendendo às cláusulas de abertura do RGPD, segundo Ramos C. C. (2020).

Existem três razões que são apontadas para justificar a existência desta lei (Universidade de Coimbra, 2021):

- O RGPD deixa aos Estados-Membros a decisão sobre algumas matérias específicas, tais como dados especialmente protegidos, tratamento de dados dos trabalhadores, idade mínima de menores, videovigilância e tratamento de dados de saúde e dados genéticos;
- O RGPD determina que cada Estado-Membro nomeie, por ato legislativo, a autoridade de controlo encarregue da fiscalização da sua aplicação;
- Entendem alguns autores que as contraordenações e os crimes são matéria da exclusiva competência da Assembleia da República. Logo, as contraordenações do RGPD não são diretamente aplicáveis, e têm de ser transpostas.

Devemos ainda dar aqui uma nota relativa à Deliberação 2019/494, e referir, “no entanto, que a CNPD, já na qualidade de autoridade de controlo nacional, manifestou uma frontal discordância com a aplicabilidade de diversas disposições daquele diploma... Considera assim a Comissão Nacional de Proteção de Dados (CNPD), que a adoção nacional de normas jurídicas em contradição com o previsto no RGPD viola o princípio do primado do direito da União e prejudica gravemente o funcionamento do mecanismo de coerência” (Ramos C. C., 2020).

Ao deliberar desaplicar 15 disposições da Lei n.º 58/2019, em prol do primado do direito comunitário, a CNPD, aplica-lhe de acordo com Teves (2019) uma rude golpe, implicando assim a aplicação direta do RGPD.

A CNPD justifica a sua posição “com o intuito de assegurar a transparência dos seus procedimentos decisórios futuros e nesta medida contribuir para a certeza e segurança jurídicas. Esclarece ainda que a não aplicação, em futuros casos concretos, das disposições legais acima referidas tem por consequência a aplicação direta das normas do RGPD que estavam a ser por aquelas manifestamente restringidas, contrariadas ou comprometidas no seu efeito útil”.

Relativamente à legitimidade para proceder à desaplicação da lei, a CNPD clarifica que “decorre do princípio do primado que, além dos tribunais nacionais, também as entidades administrativas estão obrigadas a desaplicar as normas nacionais que contrariam o direito da União Europeia, como o determinou expressamente o Tribunal de Justiça da União Europeia, no acórdão Fratelli Costanzo, que veio vincular todos os órgãos da Administração Pública ao dever de aplicar integralmente o direito da

União”.

Assim, a evolução do processo legislativo em matéria de proteção de dados na UE culminou com a entrada em vigor do RGPD, que nas palavras de Nunes (2019) tem como seu maior propósito a consumação de um espaço de liberdade, segurança e justiça, procurando o bem-estar das pessoas singulares, bem como o progresso e união na UE.

O Comité Europeu para a Proteção de Dados (CEPD) é um organismo europeu independente encarregado da aplicação do RGPD e tem sede em Bruxelas. Contribui para a aplicação coerente de regras em matéria de proteção de dados na UE e promove a cooperação entre as autoridades de proteção de dados da UE. (https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_pt, 2022). Como veremos mais adiante também este organismo já se pronunciou sobre a relação entre a proteção de dados e o BC/FT.

Entraremos de seguida mais profundamente na análise do RGPD, começando por identificar quais os direitos que este visa proteger e os seu princípios basilares.

2.1.2 Direitos a proteger e princípios orientadores

São vários os direitos que o RGPD visa proteger, principalmente o direito à reserva da intimidade da vida privada (direito de acesso, informação e oposição), mas também o direito à autodeterminação legislativa, limitação do tratamento, portabilidade de dados e esquecimento. O art.º 12.º elenca as regras para o exercício desses direitos e que as entidades responsáveis pelo tratamento dos dados devem ter ao seu alcance meios e técnicas que permitam o seu exercício.

Não é demais referir os artigos 26.º e 35.º da CRP como garantes dos direitos de personalidade, onde se inclui o direito à reserva da intimidade da vida privada. Uma nota especial para os dados sensíveis previstos não só no n.º 3 do art.º 35.º da CRP, mas também no n.º 1 do art.º 7.º da Lei n.º 67/98 e n.º 1 do art.º 8º da Diretiva 95/46/CE, que merecem uma proteção especial, e que englobam por exemplo filiações partidárias, convicções religiosas ou filosóficas ou origem étnica e onde se incluem também para Queiroz (2007) os dados referentes à situação financeira e patrimonial.

A proteção da privacidade engloba assim o direito de acesso aos dados pessoais, o direito à informação e também o direito de oposição à sua recolha e difusão. Desta forma, o cidadão pode, sempre que queira, aceder aos dados registados, conhecer a identidade dos responsáveis, esclarecer a finalidade em causa, tendo direito inclusivamente à sua retificação ou atualização.

Para Melo (2019) este é um direito que se queda a montante de outros direitos, tornando-se, por isso, basilar no exercício de outros direitos, pois é aquele que permite o exercício posterior de outros. O direito de aceder permite que os próprios titulares validem o modo como a sua informação está a ser tratada, se foi ou não transmitida a outras entidades e que destino lhe foi dada.

O direito à portabilidade de dados está previsto no art.º 20.º do RGPD e “permite aos titulares dos dados receber os dados pessoais que tenham fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e transmitir esses dados a outro responsável pelo tratamento, sem impedimentos” (Melo, 2019, p. 55). Refere a mesma autora que este direito confere poderes de controlo do titular sobre os seus dados, uma vez que permite obter e reutilizar os seus dados pessoais em diferentes serviços e para finalidades próprias, independentemente da vontade do responsável inicial.

Muito ligada à utilização de meios informáticos para armazenamento de dados está o direito à autodeterminação informativa que visa a proteção do indivíduo quanto aos dados que sobre si possam circular, sendo que para Pinto (2002) o que este direito visa proteger é o interesse em controlar o conhecimento e a difusão de informação relacionada com a vida privada do indivíduo, ou seja, sobre factos com ele intimamente relacionados, bem como com o seu meio, preservando o seu anonimato e, quando necessário, a sua salvaguarda do acesso físico de terceiros, permitindo decidir o que os outros podem ou não saber a respeito de cada um de nós.

O direito ao esquecimento é um novo direito da era da internet, pois visa principalmente a proteção de dados dos utilizadores deste espaço. Historicamente teve um forte impulso em 2010 aquando da elaboração de duas cartas, como a participação da Secretária de Estado francesa Nathalie Kosciusko-Morizet, representantes de redes sociais, motores de buscas e outros, com o intuito de criar um código de conduta.

O direito ao esquecimento pretende dar ao cidadão a capacidade de impedir e eliminar a difusão de informação sobre si, quando não haja motivo legítimo para a sua manutenção. Note-se que este não é um direito absoluto, existindo algumas limitações legais como exercício de funções de interesse público, motivos de saúde pública ou investigação.

Como princípios subjacentes ao tratamento de dados pessoais podemos elencar como principais os seguintes:

- Princípio da licitude, lealdade e transparência, referido no art.º 5.º, n.º 1, al, a) – a licitude está intimamente relacionada com o conceito de legalidade e de consentimento, princípio basilar do RGPD e que terá tratamento autónomo mais à frente, ou seja, só poderá haver tratamento de dados se houver autorização expressa do titular dos dados pessoais; para além do consentimento o titular dos dados pessoais deverá saber que os dados fornecidos serão unicamente tratados para o fim subjacente à sua divulgação à entidade portadora dos mesmos, numa relação de lealdade e confiança, que permita a fácil verificação da conformidade dos processos. Esta relação quer-se também transparente, no sentido de o titular dos dados pessoais conhecer a quem está a fornecer informação, para que fins serão usados e poder obter a confirmação e comunicação dos

mesmos, num processo de fácil compreensão e acesso;

- Princípio da limitação das finalidades, à luz do art.º 5.º, n.º 1, al, b) e n.º 1 do art.º 35.º, in fine da CRP – que permite o controlo pelo cidadão dos fins para os quais são recolhidos os seus dados pessoais, numa delimitação clara dos objetivos. A finalidade da recolha de dados pessoais deve ser determinada, explícita e legítima, não podendo ter um fim diferente do acordado, não sendo considerado incompatível com essa finalidade o “tratamento posterior para fins de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos...”, art.º 89.º, n.º 1;
- Princípio da minimização de dados, implícito no art.º 5.º, n.º 1, al, c) e também denominado princípio da qualidade ou pertinência de dados – que assume que os dados fornecidos devem ser os adequados e limitados ao fim a que se destinam, e os estritamente pertinentes;
- Princípio da exatidão e atualidade, presente na alínea d) do art.º 5.º – que determina que os dados pessoais utilizados devem ser corretos e atualizados. A inexatidão e desatualização permitem ao cidadão que fornece os seus dados exigir à entidade responsável pelo seu tratamento a sua correção ou eliminação imediatas, devendo esta estar operacionalmente apta a fazê-lo em tempo útil;
- Princípio da limitação da conservação, previsto no art.º 5.º, n.º 1, al, e) – que expressa que para além das exceções para fins de arquivo de interesse público, investigação científica, histórica ou estatística, os dados pessoais apenas devem ser conservados durante o tempo estritamente necessário à prossecução dos fins para os quais foram recolhidos;
- Princípio da integridade e confidencialidade, art.º 5.º, n.º 1, al, f) – que indica que as entidades que recolhem e conservam dados pessoais devem estar dotadas de meios e técnicas que permitam um tratamento seguro, que evite fugas e partilhas abusivas e não autorizadas;
- Princípio da responsabilidade, previsto no art.º 5.º, n.º 2 – dirigido especificamente ao responsável pelo tratamento de dados e ao subcontratante (art.º 4.º, n.º 8), como entidades intimamente relacionadas que devem conseguir demonstrar a conformidade da sua atuação, a qualquer momento a qualquer entidade ou público em geral;
- Princípio do consentimento está definido nos art.º 4.º, n.º 11 e 7.º – que é um dos princípios mais importantes, por ser basilar do RGPD, e que legitima o tratamento dos dados pessoais e sem o qual todos os outros perderiam o seu sentido. Por isso, o titular dos dados pessoais deve expressar explicitamente que conhece e autoriza o tratamento

dos seus dados, e deve ser conhecedor da identidade do responsável pelo tratamento de dados e a da finalidade da sua recolha. O consentimento pode ser retirado a qualquer momento pelo titular dos dados, através da mesma forma pela qual foi prestado.

Em resumo, após a entrada no novo RGPD são reconhecidos novos direitos aos titulares de dados pessoais, e em particular ao cliente bancário, que podemos resumir no seguinte quadro.

Quadro 1: Novos direitos dos titulares de dados

Direito de Informação	Direito de os clientes serem informados sobre a finalidade do tratamento de dados, a quem podem ser comunicados, quais os direitos que lhes assistem e em que condições os podem exercer, bem como quais os dados que têm de fornecer obrigatoriamente.
Direito de Acesso	Direito de os clientes de acederem aos respetivos dados pessoais que tenham por si sido fornecidos, sem restrições, sem demoras ou custos excessivos, bem como quaisquer informações disponíveis sobre a origem desses dados.
Direito de Retificação	Direito de os clientes exigirem que os seus dados sejam exatos e atuais, podendo solicitar a sua retificação.
Direito de Eliminação ou esquecimento	Direito de os clientes exigirem eliminação dos seus dados pessoais dos registos quando os mesmos deixem de ser utilizados para as finalidades para que foram recolhidos, sem prejuízo dos prazos de retenção que por lei se imponha.
Direito de Oposição	Direito de os clientes se oporem, a seu pedido e gratuitamente ao tratamento dos seus dados pessoais, para efeitos de marketing direto, ou ainda quando o tratamento dos dados se fundamente no seu interesse legítimo.
Direito à Portabilidade	Direito de os clientes receberem os dados pessoais que tenham fornecido, numa formato estruturado, de uso corrente e de leitura automática, e transmitir esses dados a outro responsável pelo tratamento. Este direito tem a sua maior expressão no serviço de mudança de conta regulado na Lei n.º 105/2017, de 30 de agosto
Direito à Limitação do Tratamento	Direito que os clientes têm de, em determinadas circunstâncias, solicitarem a limitação do tratamento dos seus dados, nomeadamente quando contestem a exatidão dos seus dados pessoais, durante um período que permite ao banco verificar a sua exatidão, se o tratamento for ilícito e o cliente se opuser ao apagamento de dados, solicitando, em contrapartida, a limitação da sua utilização, ou quando o banco não precise dos dados pessoais do cliente para fins de tratamento, mas esses dados sejam requeridos pelo cliente para efeitos de declaração, exercício ou defesa de direito em processo judicial.
Direito de Reclamação junto da CNPD	Direito de apresentarem sem prejuízo de qualquer outra via de recurso administrativo ou judicial, uma reclamação a uma autoridade de controlo, em especial no Estado-Membro da sua residência habitual, do seu local de trabalho ou do local onde foi alegadamente praticada a infração, se o titular dos dados considerar que o tratamento dos dados pessoais que lhe diga respeito viola o RGPD e demais legislação nacional aplicável.

Fonte: Banco BPI (2021).

Os princípios e direitos ora elencados são estruturantes e basilares a toda a temática do RGPD, mas no caso concreto, poderá haver colisão entre eles que obrigue à sua análise e ponderação de interesses em causa, e eventual escolha e derrogação de uns em favor de outros. É essa a análise que faremos de seguida.

2.1.3 A necessidade de ponderação de interesses e o risco da discricionariedade

Falar em proteção de dados pessoais é, como atrás foi referido, falar em direitos, liberdades e garantias que merecem proteção legal. Mas dificilmente podemos falar em direitos absolutamente invioláveis pois existem não só limitações específicas a cada um dos direitos elencados, mas também limitações comuns a todos eles, conforme art.º 23.º do RGPD.

Se do lado do cidadão comum existem inúmeros direitos que merecem ser tutelados, também do lado das entidades que devem acautelar essa tutela existem interesses, princípios e domínios que por vezes se podem incompatibilizar ou sobrepor àqueles. Não é possível definir de forma inequívoca onde começa e acaba o direito à reserva da intimidade da vida privada, mas deve ser possível, segundo Ribeiro (2011) estabelecer aspetos em que, face à sua natureza, possibilitam uma ponderação e avaliação quando confrontados com outros valores.

Existe assim uma inegável necessidade de ponderação de interesses e direitos em oposição, pois se por um lado se visa proteger os direitos e liberdades individuais dos cidadãos, por outro existe liberdade de utilização e circulação de informação pessoal, cabendo a cada um o direito de optar que informações prestar e para que finalidades. Deve-se optar sempre, numa ótica de proporcionalidade, transparência e minimização do tratamento à proteção do bem mais importante que se visa proteger no caso concreto, uma vez que o direito à proteção de dados não é absoluto (Duarte, 2018).

O próprio RGPD enumera situações de interesse público da UE ou de um Estado-Membro, a segurança e defesa do Estado, interesses económicos, financeiros ou fiscais, defesa da independência judiciária, entre outros.

A discricionariedade no tratamento e na escolha dos bens a tutelar deve ser ao máximo evitada, e tal só é possível se houver legislação capaz de se adaptar e acompanhar a realidade que se altera de forma tão fugaz, face aos desenvolvimentos tecnológicos. O princípio da responsabilidade previsto no art.º 5.º, n.º 2 do RGPD visa vincular as empresas a utilizar mecanismos e sistemas adequados à manipulação de dados pessoais que possam ser testados e controlados quanto ao cumprimento das obrigações legais, como forma não só de atuação em caso de incumprimento, mas também de supervisão, de uma forma genérica.

A matéria que regula a proteção de dados na UE vai muito além dos princípios basilares orientadores, pois “o legislador europeu procurou não alterar, assim, as fundações da proteção de dados, mas os meios e mecanismos que os operacionalizam, na procura de uma maior eficácia prática e material observação e cumprimentos dos seus princípios” (Guerreiro, 2018, p. 98).

Em suma, o estado deve ser o protetor e guardião dos direitos, liberdades e garantias, onde se inclui a tutela da reserva da intimidade da vida privada e o direito à informação e liberdade de expressão, que não podem ser protegidos como direitos absolutos. Desta forma, em caso de conflito entre direitos

fundamentais terá sempre de haver ponderação dos princípios e direitos fundamentais em presença e em conflito, com vista à proteção da sociedade e da segurança jurídica, prevalecendo o princípio de maior valor de acordo com o caso concreto, liberdades individuais e conjuntura social, ou mesmo económica.

Se numa ótica estritamente jurídica não há outra forma que não a ponderação de interesses à luz do princípio da proporcionalidade, já numa ótica de operacionalidade quanto mais for possível determinar, discriminar e perceber os processos de tratamento de dados mais facilmente se evita a discricionariedade. Deverá ser possível um acesso rápido e intuitivo, eficaz e preferencialmente uniforme entre as várias entidades, para proteção e segurança dos titulares dos dados pessoais e da própria entidade que os trata, podendo demonstrar facilmente o cumprimento das normas. A adaptação e inovação, nomeadamente tecnológica será essencial à segurança da informação e um meio de combate à discricionariedade.

De seguida, e entrando no caso particular das entidades bancárias, veremos como por estas é feito o tratamento dos dados pessoais.

2.1.4 O tratamento de dados pessoais nos bancos

Conforme refere Mendes P. A. (2018) a conformidade com o RGPD é obrigatória para todas as organizações que processem ou armazenem dados de cidadãos, dentro e fora da UE. Os bancos, como empresas privadas que são, estão sujeitas ao RGPD e a sua implementação causou obviamente impacto nestas organizações ao nível dos recursos financeiros, humanos, tecnológicos, de processos e metodologias. Ainda para este autor, o RGPD, conforme o tipo de dados pessoais e os processos que os tratam, procura analisar e determinar o risco a que estão sujeitos, permitindo aplicar medidas e controlos de segurança da informação necessários para o mitigar e garantir que os dados pessoais e titulares dos mesmos estão protegidos de possíveis abusos da informação e ameaças.

O setor financeiro sempre lidou com a matéria dos dados pessoais, pois o cliente particular é um dos seus principais focos e a base da atividade bancária. A atividade bancária pretende ser sempre mais eficiente, mais rentável e tem vindo constantemente a atualizar-se e adaptar-se à nova era das tecnologias, numa banca cada vez mais digital e que potencia o fornecimento de dados pessoais por parte dos clientes. Para Rebelo, Analide e Abreu (2020) a resposta aos novos desafios da era digital pelas instituições bancárias é feita pela implementação de políticas de desmaterialização – segundo um prisma *paperless* – visando a integração de novas aplicações orientadas para o cliente, através do uso de tecnologias que substituem os canais de interação tradicionais, como a inteligência artificial. Os mesmos autores consideram ainda que o cliente é um importante ativo no setor bancário, ao afirmarem que as mais-valias económicas das operações de tratamento de dados em grande escala se revelam sobretudo na consideração da informação pessoal como uma nova categoria de ativo, com o aumento radical da eficiência nos processos.

As instituições bancárias estão autorizadas ao tratamento de dados pessoais através do contrato de abertura de conta, contratação de um cartão de crédito ou outros contratos de produtos bancários que celebrem com os clientes e em que estes têm de dar o seu expresso consentimento ao tratamento dos dados, caso contrário a relação comercial deixará de existir (art.º 6.º alínea b) do RGPD). Também à luz da alínea c) do mesmo artigo o tratamento de dados é admissível quando necessário ao cumprimento de uma relação jurídica, o que se verifica por exemplo nos reportes frequentes ao Banco de Portugal (BdP).

Em caso de violação os bancos são sujeitos a coimas, cujos valores dependem da gravidade da infração. Note-se, como assinala Mendes P. A. (2018, p. 21), que “as coimas categorizadas como baixas não são de todo baixas, apenas significa que têm um valor menor associado às mesmas, sendo esse valor passível de ir até 10 milhões de euros ou até 2% da faturação anual global da organização”.

Conforme refere Morais (2018) a violação dos dados pessoais ocorre quando se verifica por exemplo um lapso na segurança, imprevista ou propositada, e que resulte na transmissão, perda, transformação ou acesso sem consentimento a dados pessoais. Como forma de intensificar e garantir o cumprimento da legislação é criada a figura do encarregado de proteção de dados, sendo, segundo o mesmo autor, uma função de elevada importância, na medida em que garante o cumprimento e aplicação do RGPD, supervisiona a atividade das empresas neste ramo e é um intermediário com os reguladores externos.

Os bancos, no cumprimento do art.º 24.º do RGPD devem ter documentadas as políticas, procedimentos e operações de processamento de dados que comprovem a conformidade com o regulamento, e que possam ser disponibilizados à entidade reguladora, em caso de requisição (Mendes P. A., 2018). Este autor refere ainda a necessidade de implementação de medidas que garantam que apenas os dados necessários são recolhidos, processados, acedidos e, apenas durante o tempo necessário. O art.º 25.º do RGPD especifica assim que as organizações devem incorporar a proteção de dados apropriada por defeito, desde a conceção, o tipo de tratamento, e os riscos a que podem estar sujeitos.

Os artigos 7.º e 8.º do RGPD referem-se ao consentimento, e nesta medida os bancos devem ter capacidade de provar que este foi dado pelos clientes, bem como possibilidade de poderem esclarecer de forma clara e concisa o propósito do processamento de dados. Em relação aos menores o consentimento é dado pelos representantes legais ou tutores.

A notificação de uma violação de dados pessoais à autoridade de controlo está prevista no art.º 33.º do RGPD e prevê um prazo máximo de 72 horas para que as entidades notifiquem a entidade reguladora e informem, nomeadamente a causa da fuga, potenciais consequências, número aproximado de indivíduos afetados e número de registos em causa (Mendes P. A., 2018). O mesmo autor aponta ainda a necessidade de existência de um dicionário de dados (art.º 30.º do RGPD), que registre as atividades de processamento de dados que permita identificar os propósitos e finalidades dos mesmos, os responsáveis pelos tratamentos e os fluxos de dados pessoais.

Refira-se ainda que o tratamento de dados pelos bancos para efeitos comerciais será mantido enquanto forem necessários para relação comercial com os clientes e, finda esta, manter-se-ão pelos prazos legais obrigatórios, ou até que prescrevam, nos termos da lei, os direitos dela emergentes.

Quando consultado o site de um banco existe, por regra, uma secção dedicada à proteção de dados pessoais. Aí podemos consultar por exemplo a forma como são recolhidos os dados, as técnicas utilizadas, os direitos dos clientes e a quem podem os dados ser transmitidos, bem como a forma de contactar o Encarregado de Proteção de Dados ou *Data Protection Officer* (DPO). Esta entidade é, conforme já referido, responsável pela monitorização da conformidade do tratamento dos dados pessoais com o RGPD e assegura a comunicação com os titulares dos dados pessoais.

Nas palavras de Luís Máximo dos Santos (2021), na sua intervenção enquanto Vice-Governador do BdP no encerramento do colóquio CBSF – Três anos de RGPD, “os dados pessoais e o que se pode fazer com eles são centrais na sociedade contemporânea, constituem uma das matérias-primas cruciais do nosso tempo. Trata-se de uma verdade transversal a toda a atividade económica, mas no setor financeiro ganha ainda mais relevo”. Refere ainda que “Há muito caminho para fazer no que diz respeito à proteção de dados no País em geral e no setor financeiro em particular, mas também muito espaço para as instituições financeiras tirarem partido da utilização legítima de dados pessoais, tornando a atividade bancária e financeira mais eficiente e, por isso, mais rentável” (Santos, 2021).

O RGPD apresenta assim uma oportunidade de as empresas acompanharem um cenário de segurança em mudança, obrigando as organizações a adotar medidas técnicas e organizativas adequadas ao tratamento de dados efetuado, assegurando a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento (Teves, 2019).

Francisco e Francisco (2019, p. 69) referem, por sua vez, que esta implementação tem 7 passos:

- “ Planear bem o trabalho;
- Mapear todos os dados pessoais tratados na organização;
- Caracterizar os tratamentos tal como são realizados à data;
- Identificar as atividades que carecem de alteração e quais as que têm maior risco;
- Implementar as alterações, verificar a conformidade e garantir a compatibilidade tecnológica;
- Constituir um dossier com as evidências de implementação;
- Avaliar o impacto do projeto, formar os colaboradores da organização e criar as condições para que a organização integre no seu funcionamento, estruturas e cultura organizacional, a monitorização e a conformidade com o RGPD”.

A recolha, o tratamento e o uso dos dados pessoais implica, segundo Borrvalho (2019) cuidados

adicionais, na medida em que tem de ser conforme ao regulamento, mas alerta para a necessidade da reutilização, mais uma vez em prol da eficiência. O autor sinaliza, em termos gerais, a preocupação em não solicitar sistematicamente os mesmos dados e informação, evitando redundâncias sem valor acrescentado. Naturalmente que esta redundância limita a eficiência. Limitação que pode, ou não, ser justificada pela necessidade de segurança. Aliás, avaliar eventuais trocas entre eficiência e segurança na atividade bancária, constitui um dos fundamentos para a realização da presente investigação.

Verificada que está a origem e evolução, princípios essenciais e forma de tratamento pelos bancos da matéria relativa aos dados pessoais e RGPD, passar-se-á de seguida ao segundo referencial que abordaremos na presente dissertação, o sigilo bancário, instituto que acarreta um direito fundamental dos cidadãos, e em particular do cliente bancário.

2.2 Sigilo bancário

Após a análise anterior dos objetivos do RGPD, nomeadamente a regulação do correto tratamento de dados pessoais no espaço da UE, verificadas as obrigações das entidades que tratam dados pessoais, quer sejam responsáveis pelo tratamento de dados pessoais, quer tratem os dados em nome de outra entidade e definidas as responsabilidades destas entidades perante um evento que comprometa a segurança de dados pessoais, estamos em condições de passar para o instituto seguinte, o sigilo bancário. Este é o instituto basilar do sistema bancário, o mais antigo e sem o qual nenhuma das outras temáticas que aqui elencamos faria sentido, por não estarem reunidas as condições de segurança e confidencialidade essenciais à existência de uma relação cliente/instituição de crédito. O sigilo bancário que estudaremos de seguida consiste assim na discrição que as entidades financeiras, os seus órgãos e seus empregados devem observar sobre todos os dados pessoais, dados económicos, factos dos seus clientes ou da própria instituição e que chegam ao seu conhecimento através do exercício das suas funções.

2.2.1 Enquadramento e evolução do processo legislativo

O sigilo bancário pressupõe o dever de não divulgar determinados conhecimentos e informações, sendo várias as definições encontradas na literatura. “O segredo bancário consiste na discrição que os bancos, os seus órgãos e empregados, devem observar sobre os dados económicos e pessoais dos clientes, que tenham chegado ao seu conhecimento através do exercício das funções bancárias” (Luís, 1981, p. 454). Segundo Gomes (2006) o conceito de sigilo bancário, tem um cunho marcadamente profissional, dando-lhe a qualificação de segredo profissional. Para além de um dever, traduz-se também num direito que tem a particularidade de apresentar uma pluralidade de titulares, o cliente bancário e a própria instituição financeira. Segundo Ribeiro (2011, p. 19) “essa informação, que o indivíduo tem direito a que não seja revelada, consiste, precisamente nos seus dados pessoais que fornece à instituição financeira, quando contrata com ela, e nos registos da movimentação da sua conta, reveladora dos seus

hábitos, crenças e negócios, etc”.

As instituições bancárias têm acesso a um largo número de dados pessoais de natureza sigilosa e que não podem ser revelados a terceiros. Desta forma, há uma proteção que vai além da mera proteção individual do cliente, abrangendo toda a sociedade e a tutela de interesses públicos, como o regular funcionamento da atividade bancária e a manutenção da confiança no sistema bancário, que são essenciais ao sistema financeiro. Marques (2016) refere o aspeto fulcral do sigilo na relação jurídica bancária, que se prende com a questão da confiança e da proteção da intimidade do cliente e da confiança nas próprias instituições bancárias, em termos gerais. Também o bom nome das instituições financeiras é um bem a tutelar como forma inclusive de zelar pelo funcionamento do sistema bancário em geral. Refere assim Gomes (2006, p. 72) tratar-se de uma “relação complexa triangular, formada em cada um dos seus vértices por diferentes interesses”, o interesse privado do cliente, o da instituição financeira e o interesse público.

Segundo Vicente (2014) este dever também abrange as autoridades de supervisão, estando estas sujeitas ao dever de sigilo bancário de supervisão, preservando a confiança das entidades supervisionadas, garantindo nomeadamente que aspetos da sua organização, não destinados ao conhecimento público, são resguardados.

Existem, contudo, situações em que poderá ser permitida a quebra do sigilo, pois como veremos adiante, “não sendo o direito ao sigilo um direito absoluto este, comporta diversas exceções” (Monteiro, 2015, p. 81).

O sigilo bancário relaciona-se com a confiança e é tão essencial como antigo, remontando à origem da própria atividade bancária. Apesar da sua antiguidade, tem vindo a sofrer várias alterações ao longo dos tempos, como forma de se adaptar às novas realidades que vão surgindo.

Não querendo, por desnecessário, desenvolver toda a história do sigilo bancário, cumpre-nos referir que a sua origem é tão antiga quanto a atividade bancária. Ribeiro (2011) remete a sua origem para cerca de quatro mil anos atrás, na Babilónia, e ao Código de Hammurabi, primeira codificação legislativa. No império romano também o segredo bancário está consagrado do *actio injuriarium*, mantendo-se esta tendência durante a Idade Média pelos Templários e banqueiros judeus enquanto costume e alma do comércio (Monteiro, 2015). Refere ainda que é na época do Renascimento que o sigilo bancário começa a ganhar expressão entre os banqueiros protestantes, particularmente após a carta sobre usura de Calvino, no século XVI. O verdadeiro sentido internacional do sigilo bancário surge, como referido por Coelho (2012) na época pós 1.^a Guerra Mundial, com o advento do nacionalismo e o consequente controlo das transações financeiras com o exterior.

A nossa abordagem será referente ao sigilo bancário da era moderna, com a sua primeira consagração já em pleno século XX, na Suíça, onde se decide primeiramente legislar sobre o assunto, punindo criminalmente a sua violação (Vaz, 2017).

Em Portugal é conhecida uma referência ao segredo bancário num Regulamento Administrativo do BdP, que remonta a 1847, que era essencialmente dirigido aos funcionários e que previa sanções disciplinares como a repreensão ou o despedimento, ou mesmo responsabilidade civil dos funcionários e do próprio Banco (Pais, 2016).

Em 1967 foi publicado o Decreto-Lei n.º 47909, de 7 de setembro, que criou o Serviço de Centralização de Riscos de Crédito e que prevê a proteção de dados bancários e a obrigatoriedade de reporte ao BdP, aplicável a todas as instituições de crédito.

Naturalmente, após 1974 tornou-se necessário o reforço da legislação nacional relativa ao sigilo bancário. Segundo Coelho (2012) após a revolução de abril viveu-se um período conturbado, marcado por convulsões sociais e políticas que se repercutiram no sistema económico e financeiro, e o clima de desconfiança geral levou o legislador ao reforço legal da tutela do segredo bancário. Assim, surgiram uma série de decretos-lei, como por exemplo o Decreto-Lei n.º 644/75, de 15 de novembro, que estabelece a Lei Orgânica do BdP, e o Decreto-Lei 2/78, de 9 de janeiro, em que se consagra a proibição de revelação de informação bancária e onde expressamente se prevê a responsabilidade penal em caso de violação. Como refere Pais (2016) este diploma conferiu uma proteção mais coesa ao segredo bancário, definiu o seu âmbito de aplicação e as raras exceções ao seu levantamento, bem como as severas consequências legais em caso de violação.

Após a entrada de Portugal para a Comunidade Económica Europeia também nesta matéria se sentiu a necessidade de harmonização legislativa, como não podia deixar de ser. Assim sendo, surgiu o Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF), aprovado no Decreto-Lei n.º 298/92, de 31 de dezembro, com redação dada pela Lei n.º 54/2021, de 13 de agosto, que é, até aos nossos dias, o principal normativo que regula e protege o sigilo bancário no nosso país. Neste percurso, tal como referido por Ribeiro (2011), a evolução histórica do segredo bancário passou a sua tónica, progressivamente, de costume contratual à defesa da informação privada do indivíduo.

Tem-se contudo assistido à tomada de algumas medidas no âmbito da UE e da comunidade internacional que, segundo Monteiro (2015) se materializam na progressiva diminuição da tutela do sigilo bancário, sendo esta uma realidade suscetível de ser derogada em confronto com outros valores e bens jurídicos a proteger. Gomes (2006, p. 194) conclui mesmo que “a evolução normativa permite asseverar que se está a assistir, a nível do direito comunitário, a uma crescente degradação do segredo bancário”.

2.2.2 Sigilo bancário e direito à reserva da intimidade da vida privada: restrições, violação e derrogação

Assumido que está o papel importante do sigilo bancário, que remonta à origem da atividade bancária, veremos de seguida as situações em que podem ocorrer restrições ou derrogações a este

instituto.

Segundo Ribeiro (2011, p. 14) “os dados bancários integram o âmbito de proteção do direito de reserva sobre a vida privada, na medida em que, dada a importância das movimentações bancárias no nosso tempo, não faria sentido excluir o sigilo bancário da tutela do direito da reserva sobre a vida privada”. Considera assim a existência de um verdadeiro direito ao sigilo bancário.

O sigilo bancário, enquanto segredo profissional, decorre de uma relação contratual entre duas partes e que encontra, por sua vez, fundamento no direito à reserva da intimidade da vida privada. A temática do sigilo bancário está relacionada com atividades públicas e privadas que lidam com conhecimento de factos respeitantes à vida particular de indivíduos e de empresas. Aqui se inclui a atividade bancária e o acesso que têm aos dados de natureza pessoal e económica e que impõe às instituições do setor, aos seus órgãos e funcionários o cumprimento de um dever geral de discrição, proibição de revelação e utilização (Azevedo, 2012).

Pais (2016, p. 18) refere-se também a “interesses privados como são a confidencialidade sobre os dados e informações da esfera patrimonial dos clientes e ainda interesses privados das próprias instituições financeiras relacionados com o direito ao bom-nome, reputação e liberdade de empresa”. Um outro fundamento do sigilo bancário será o direito à reserva da intimidade da vida privada e familiar dos clientes, onde caberá também uma dimensão patrimonial e económica. Contudo esta não é uma matéria que reúna consenso.

O Acórdão do Tribunal Constitucional n.º 672/2006 de 12 /12/2006, processo n.º 298/06 refere o já citado art.º 26.º, n.º 1 da CRP que consagra um direito genérico à reserva, aí se incluindo “a situação económica dos cidadãos espelhada nas respetivas contas bancárias fará parte do âmbito de proteção do direito à reserva da intimidade da vida privada, constituindo o segredo bancário um corolário dessa reserva” (Acórdão n.º 672/2006).

Assim, segundo Vaz (2017), para o Tribunal Constitucional a intimidade da vida privada abarca também a intimidade económica, e o sigilo bancário constitui uma dimensão fundamental do direito à reserva da intimidade da vida privada, com consagração constitucional, acrescentando que qualquer restrição imposta ao sigilo bancário é vista como uma verdadeira restrição a este direito fundamental. Esta posição é fortemente aceite pela doutrina, mas está longe de ser consensual. Não será contudo possível, fazer aqui uma exposição detalhada da controvérsia entre os autores, bastando resumidamente referir que há autores que considerem que o sigilo bancário está acima da proteção do património e do interesse patrimonial do Estado em cobrar impostos e que a proteção de dados bancários só pode ser superada pela autoridade judiciária quando estamos perante crimes de muita gravidade contra pessoas (Campos, 1997). No mesmo sentido Cordeiro, Leitão e Gomes (2002) afirmam que as limitações ao segredo bancário são muito excecionais e que apenas valores claramente superiores e, em princípio, de natureza não patrimonial, poderão consentir, e sempre sob forma de lei com cobertura constitucional,

limitações.

Outros autores como Sanches (2007), que fazem uma clara distinção entre privacidade e intimidade, não consideram que o segredo bancário esteja relacionado com a intimidade da vida privada, e desta forma, terá tutela constitucional, mas de forma menos intensa.

É possível assim afirmar que o direito ao segredo bancário também não é um direito absoluto, podendo em várias circunstâncias sofrer exceções e restrições, sendo a situação mais comum a que se verifica no combate à fraude e evasão fiscais. Estamos novamente perante um conflito de direitos, e onde mais uma vez se deve aplicar o princípio da proporcionalidade. Segundo Canotilho e Moreira (2014) para que tal aconteça a restrição tem de ter consagração constitucional expressa, deve visar a salvaguarda de outro interesse ou direito constitucionalmente protegido, deve ser apta para o efeito, limitar-se à medida necessária para atingir esse objetivo, e não deve aniquilar o direito em causa atingindo o seu conteúdo essencial.

O art.º 79.º do RGICSF prevê as exceções ao segredo bancário, não sendo uma verdadeira exceção o caso em que o cliente autoriza a revelação a terceiros da sua informação bancária sigilosa, e que está prevista no n.º 1 do mesmo artigo. Pais (2016) refere este caso de dispensa do sigilo bancário, que é comunicada pelos clientes à instituição bancária ou financeira, não havendo qualquer violação de segredo e sim o tratamento de um direito disponível.

Já os casos de derrogação, segundo Gomes (2006) consistem em verdadeiras quebras de sigilo, produzindo efeitos independentemente da vontade do titular do segredo, e que por motivos de interesse público prevalecem sobre o dever de sigilo e sobre os interesses por ele protegidos.

O n.º 2 do já citado art.º 79.º do RGICSF prevê as chamadas exceções institucionais nas alíneas a), b) e c), e onde se admitem revelações dos elementos protegidos pelo segredo, e no âmbito das suas atribuições, ao BdP, à Comissão do Mercado de Valores Mobiliários (CMVM), Fundo de Garantia de Depósitos, ao Sistema de Indemnização aos Investidores e ao Fundo de Resolução (Pais, 2016). Para Gomes (2006) estas exceções justificam-se pela tutela do interesse público de bom funcionamento, equilíbrio e estabilidade do sistema financeiro, e salvaguarda da confiança dos que recorrem àquelas entidades.

Relativamente à alínea d) do artigo citado no parágrafo anterior, refere-se à derrogação do segredo bancário para todo e qualquer processo-crime, seja qual for o ilícito típico em apreço, e com competência do Ministério Público. Mendes (2012) enfatiza assim razões de interesse público e punição criminal.

O art.º 79.º, n.º 2 alínea e) refere-se expressamente à revelação de dados bancários protegidos à Administração Tributária, revelando-se uma matéria muito sensível e aquela que mais tem sofrido alterações, mas que aqui não nos interessa, atendendo às questões e objetivos da presente investigação.

A violação do dever de segredo tem previstas, obviamente, várias sanções, nomeadamente penais,

conforme art.º 84.º do RGICSF. Segundo Pais (2016, p. 31) “ a violação do dever de segredo traduz-se pois, num acto ilícito, afrontador de um bem jurídico com dignidade penal no nosso ordenamento jurídico. Contudo, até aí chegar, a violação do segredo bancário é também fonte de responsabilidade contraordenacional, civil e disciplinar.

Também nas palavras de Ribeiro (2011, p. 10) “se o direito de reserva à intimidade da vida privada não for suficientemente densificado pela lei, se não houver um conceito sólido do bem que merece tutela legal e constitucional, se se lhe tolerarem, sucessivamente, restrições e violações, então o direito diluir-se-á, e o cidadão não verá qualquer interesse em invocá-lo”.

2.2.3 A necessidade de ponderação de interesses e o risco de discricionariedade

Estamos, no âmbito da nossa dissertação, constantemente a lidar com matérias em que pode existir colisão de direitos e em que devem ser sempre ponderados os interesse que se opõem, para a partir daqui perceber de que forma podem ou não, uns ceder perante outros.

Para Monteiro (2015) a análise do sigilo bancário não pode ser feita parcialmente, tendo apenas em conta os interesses salvaguardados por este instituto, pois é necessário perspetivar outros valores e interesses que se lhe opõem e que podem justificar o seu sacrifício. O sigilo bancário, a sua proteção e a sua derrogação têm suscitado grandes controvérsias na doutrina, principalmente no que toca à transparência fiscal e cobrança de impostos. Azevedo (2012, p. 232) refere que, “em Portugal, a questão continua a suscitar animados debates, confrontando-se, por um lado, os partidários da prevalência dos poderes do fisco e, por outro, os defensores da manutenção de um segredo bancário forte”.

É certo que é unanimemente aceite que deve haver lugar a uma necessária ponderação de interesses, mas sendo controverso qual o interesse que mais é preponderante proteger. Marques (2016, p. 9) refere que “ao interesse privado... contrapõe-se o interesse público, na sua quebra, estando em causa a determinação do elemento preponderante”. O sigilo bancário tornou-se, para Ribeiro (2011), num dos principais alvos das políticas de combate à criminalidade organizada, económico-financeira e à fraude fiscal. E o acesso à informação bancária dos particulares passou a ser a regra, e não mais a exceção.

Segundo Pires (1998) a proteção de dados bancários visa garantir a atividade que as instituições bancárias desenvolvem, de forma que aí não se violem as regras deontológicas de sigilo, e o art.º 78.º, n.º 1 do RGICSF aponta o revelar informações, o que demonstra o cuidado em delimitar o âmbito material da proteção de dados bancários, não abrindo horizontes à discricionariedade.

O acesso a dados bancários deve ser limitado ao estritamente necessário, referindo inclusive Pais (2016), nas suas conclusões, que deverá haver um regime taxativo e tão claro quanto possível das situações que permitem aceder ao dados bancários, de modo a evitar interpretações discricionárias. Acresce que esta solução será sempre tomada à luz de critérios de necessidade, adequação e

proporcionalidade, não conduzindo ao sacrifício unilateral de um direito, valor ou princípio em face do outro.

Também Marques (2016) se refere à essencial ponderação de valores, de acordo com o princípio da proporcionalidade, e em respeito pelos direitos, liberdades e garantias e sinaliza a necessária observância da legitimidade para aposição de limites ao segredo, nomeadamente nas finalidades fiscais, também previstas constitucionalmente, e onde exista uma situação de conflito. De um lado, identifica o interesse privado na manutenção do segredo bancário, para tutela da privacidade, e do outro, o interesse fiscal e a atempada arrecadação de receitas, no combate à fraude e evasão. Este posicionamento é útil nesta dissertação para explicar a complexidade que envolve a compatibilização de diplomas legais.

Também Monteiro (2015) refere a complexidade que esta questão reveste e sinaliza a necessidade de ser encontrada uma solução para este conflito de valores fundamentais, solução que não implique o sacrifício absoluto de um dos interesses em benefício total do outro.

Segundo Sanches (1995), citado por Pais (2016) existe no ordenamento jurídico português uma clara distinção entre a intimidade da vida pessoal e familiar (núcleo central da esfera pessoal de cada cidadão) e a reserva que pode acompanhar a vida privada, que pode ser objeto de uma disponibilidade implícita, após a realização de uma ponderação de interesses sujeita ao princípio da proporcionalidade. Para o mesmo autor o segredo bancário nem sequer constitui expressão do imperativo constitucional da proteção da intimidade, estando o acesso a essa esfera privada vedado aos próprios bancos, pois trata-se de uma esfera íntima e inviolável da intimidade.

Já para Marques (2016, p.49) o segredo bancário, tendo por base o art.º 101.º da CRP, enquanto direito que tutela a privacidade do cliente, contrapõe-se um interesse público que exige a aposição de certas restrições. O segredo bancário “privilegia não apenas a posição do cliente, no resguardo da sua privacidade, mas tutela também a situação das próprias instituições bancárias. E, sobretudo, o fomento do desenvolvimento económico-social, face à situação de confiança pública, criada em relação à Banca, pelo que se compreende que este é ainda uma instrução ao serviço das finalidades dos sistema financeiro”.

Por outro lado Marques (2016) conclui que o segredo bancário é um direito constitucional fundamental, que constitui dimensão essencial à reserva da intimidade da vida privada e familiar (art. 26.º, n.º 1 da CRP), e que, de acordo com o princípio da proporcionalidade (art. 18.º, n.º 2 da CRP) pode ser derogado na presença de bens jurídicos superiores e da necessária ponderação de interesses realizada. Contudo, ao fazer isto, sem aclarar o entendimento de “bens jurídicos superiores”, acaba por remeter o problema para o casuístico e o discricionário, para o não estruturado, logo de difícil compatibilização com a eficiência que envolve a estruturação, com práticas organizacionais e rotinas padronizadas.

2.2.4 O tratamento do sigilo nos bancos

O sigilo que abordamos é o sigilo enquanto segredo profissional, e em particular o segredo bancário em toda a sua extensão, enquanto instituto que privilegia a total confidencialidade, e que vai muito além dos dados pessoais do cliente bancário.

Segundo refere Marques (2016) os dados de uma conta bancária são o reflexo da vida do cliente, quer a nível pessoal quer económico, e esta relação contratual deve pautar-se por uma garantia de confidencialidade, de modo a assegurar a privacidade. Acrescenta ainda que existe uma relação de discrição e de lealdade das partes envolvidas, que implica a não revelação ou aproveitamento de conhecimentos e informações obtidos no seio dessa relação.

Ainda segundo Semedo (2015), o conteúdo do sigilo bancário refere-se a informações a que só agentes dos bancos e clientes têm acesso, ou seja, terceiros não podem ter acesso a essa informação de forma gratuita, sem fundamento jurídico ou por vontade do cliente, e não pode ser revelado por aqueles que têm o dever de confidencialidade.

A flexibilização do sigilo bancário tem sido mais acentuada no domínio tributário, com o progressivo aumento da possibilidade de derrogação por parte de Autoridade Tributária (AT) sem consentimento do titular. A regra geral para a derrogação do sigilo bancário continua a ser consagrada no artº 63.º, n.º 2 da Lei Geral Tributária, de acordo com o qual o acesso à informação bancária sigilosa depende de autorização judicial. Contudo, e para fins fiscais, existem várias exceções consagradas na lei, que permitem o acesso a essas informações, por parte da AT, que não dependem de autorização judicial (Monteiro, 2015).

Os bancos estão hoje cada vez mais sujeitos às derrogações do sigilo bancário consagradas na lei e ainda à necessidade de os seus colaboradores terem um cuidado extremo para evitar as situações de violação do segredo na sua atuação diária. Ambas as situações são passíveis de melindrar a relação com o cliente que se pretende, e apesar de tudo, de profunda confiança, sob pena de se extinguir.

2.3 Branqueamento de capitais e financiamento ao terrorismo

Apesar de o sigilo bancário constituir a pedra basilar em que assenta toda a atividade bancária, este tem muitas vezes de ser conciliado com outros institutos, como é o caso do BC/FT. Num mundo cada vez mais globalizado existe uma forte exigência de cumprimento da legislação em vigor por forma a evitar ou minimizar o risco de o sistema bancário ser utilizado para efetuar operações relacionadas com BC/FT ou operações ou relações de negócio que violem as sanções internacionais e medidas restritivas. Este capítulo será dedicado ao BC/FT, e far-se-á de seguida, tal como feito para o RGPD o seu enquadramento legal e evolução dos normativos.

2.3.1 Enquadramento e evolução do processo legislativo

Não há dúvida que a globalização e as constantes mudanças de tecnologias de informação são facilitadores para a realização de lavagem de dinheiro. O BC/FT não é realizado exclusivamente através da atividade bancária, contudo, o setor dos serviços financeiros fornece um meio importante através do qual essa lavagem pode ser feita, conforme refere Duarte (2019).

Atualmente o regime do BC/FT está previsto na Lei n.º 83/2017, de 18 de agosto, na Lei n.º 97/2017, de 23 de agosto, na Lei n.º 11/2002, de 16 de fevereiro, Aviso n.º 2/2018 do BdP, de 26 de setembro, e no art.º 368.º do Código Penal (CP). Antes de fazermos uma síntese da evolução legislativa deste instituto, será necessário explicar o seu conceito, recorrendo ao estado da arte.

Brandão (2002) associa o branqueamento de capitais ao lado negro da globalização, informatização e comércio eletrónico. E ainda que esta seja uma, entre várias perspetivas para ajudar a entender a complexidade de práticas que podem ser associadas ao branqueamento de capitais, maior escala pode traduzir maior dificuldade em assegurar a rastreabilidade das transações, particularmente quando estão envolvidos países com diferentes ordenamentos jurídicos.

Já para Pires (2018, p. 18) “o Branqueamento de Capitais constitui um ato ilícito através do qual os perpetradores dissimulam a origem de bens e rendimentos obtidos ilicitamente, convertendo-os em capitais aparentemente lícitos, introduzindo os mesmos no sistema económico”. No mesmo sentido Schott (2004) indica um processo de dissimulação de produtos de uma atividade criminosa, para ocultar a sua origem ilícita.

Trata-se, pois, de um crime económico, segundo Duarte (2019), com impacte a nível mundial e que afeta negativamente o nível de desenvolvimento económico dos países, podendo inclusivamente corromper os sistemas políticos e financeiros e fazer colapsar a economia. Nas palavras de Vicente (2014, p. 18) “os branqueadores desenvolvem técnicas extremamente complexas e infundáveis que estão em constante desenvolvimento, evolução e mutação”. Estes posicionam-se na linha da frente da informação e conhecimento, retirando daí o máximo proveito e sendo os acontecimentos sociais e científicos, a globalização e a tecnologia, os seus instrumentos, possíveis meios de branqueamento.

Em conclusão, Pires (2018) refere que o impacte do branqueamento de capitais assume relevância internacional, sendo que existem aspetos comuns na definição de vários autores, nomeadamente a ocultação de bens, capitais ou produtos, ser um processo dinâmico e lhe ser conferida uma aparência legal. No mesmo sentido Rodrigues (2010) que fala em reciclagem de dinheiro, que transforma capitais obtidos ilegalmente em capitais como se fossem oriundos de atos lícitos.

Segundo Jesus (2016, p. 42) “o esforço internacional tem sido imenso, no sentido de criar medidas preventivas sobre a temática do branqueamento de capitais, mas os esquemas criados pelos criminosos são bastante dinâmicos, por forma a contornar e ludibriar os mecanismos de deteção deste tipo de crime.

Acrescenta ainda que “várias organizações mundiais, em consonância com os Estados, estruturam medidas preventivas ao branqueamento de capitais que, posteriormente, cada estado cooperante implementa em forma de legislação, de acordo com a sua lei base, ou constituição”.

Embora seja possível remeter a sua origem, como refere Jesus (2016) ao século XVII, onde se encontram práticas de branqueamento de capitais na ação criminosa de piratas que pilhavam cargas e embarcações, que voltando às suas terras adquiriam terras e bens, que justificavam como lucros da atividade mercantil, na era moderna o branqueamento de capitais é imediatamente associado a Al Capone, *gangster* de Chicago que utilizava uma cadeia de lavandarias, negócio aparentemente lícito, para encobrir os seus negócios ilícitos de contrabando de álcool, jogo clandestino e prostituição (Rodrigues, 2010).

Já Braga (2020) refere a primeira tipificação legal em 1970, nos Estados Unidos da América, através do Bank Secrecy Act. Contudo, apenas foi tipificado como crime em 1986, primeiro nos Estados Unidos através do Money Laundering Control Act e depois no Reino Unido através do Drug Trafficking Offences Act.

É em 1988 com a Convenção de Viena que se dá o primeiro passo ao nível da consciencialização internacional para esta realidade, embora inicialmente associada somente ao tráfico de droga e integração dos seus lucros no sistema económico-financeiro (Pires, 2018). Segundo a mesma autora só na Convenção de Palermo – Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional, o conceito de branqueamento de capitais é alargado.

Em 1989 foi criado o Grupo de Ação Financeira (GAFI), organismo intergovernamental cujo objetivo principal é controlar, a nível global, todas as atividades que envolvam o BC/FT, pondo em causa a integridade do sistema financeiro internacional. Tem sede na OCDE em Paris e dele fazem parte, atualmente, trinta e sete países, de entre os quais Portugal desde 1990 (Braga, 2020). Segundo a mesma autora os países envolvidos no GAFI são alvos de avaliações periódicas, nas quais são verificadas a conformidade técnica da legislação e da regulamentação dos países envolvidos, a eficácia da aplicação das recomendações e são avaliados os resultados do combate ao BC/FT.

Atualmente o GAFI é, segundo Vicente (2014, p. 93), “um organismo de natureza predominantemente técnica que constrói e promove padrões de comportamento a nível internacional, indicando o “caminho” mais adequado e eficaz, em determinados momentos e circunstâncias, para combater o branqueamento de capitais e terrorismo”. Existem atualmente 40 recomendações emitidas pelo GAFI que têm a finalidade de estabelecer padrões de referência e um guia de boas práticas no âmbito da prevenção de BC/FT.

Em Portugal, o branqueamento é tipificado em 1993, no Decreto-Lei n.º 15/93, de 22 de janeiro, conhecida como a Lei da Droga, sendo apontado por Canas (2004) como a primeira legislação que criminaliza o branqueamento de capitais. Tem como principal orientação os crimes ligados ao tráfico de

estupefacientes, sendo que no mesmo ano foi ainda publicado o Decreto-Lei 313/93, de 15 de setembro, que transpôs a Diretiva 91/308/CEE do Conselho, de 10 de junho, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais (Jesus, 2016). Mas devido à constante evolução desta prática criminosa, foi necessário proceder a diversas alterações a nível legislativo e jurídico (Braga, 2020).

O Decreto-Lei n.º 325/95, de 2 de dezembro, por exemplo, estabelece que as entidades financeiras, e também casinos, casas de apostas, mediadores imobiliários, entre outros, são obrigadas a fornecer informações sobre clientes, a conservar documentos e a comunicar operações suspeitas (Braguês, 2009).

Este decreto-lei sofreu várias alterações e revogações ao longo dos tempos, indo ao encontro de diretivas europeias no sentido de Portugal seguir o normativo legal em harmonia com a lei constitucional, sendo que a Diretiva Europeia de 2001 deu origem à alteração para a Lei n.º 10/2002, de 11 de fevereiro (Jesus, 2016).

A Lei n.º 83/2017, de 18 de agosto prevê nos artigos 11.º e seguintes alguns deveres e obrigações a todas as entidades, financeiras ou não, como o dever de controlo, dever de identificação e diligência, dever de comunicação, dever de abstenção, de recusa, de conservação e de formação (Braga, 2020). Ainda no âmbito nacional a Lei n.º 97/2017, de 23 de agosto, regula a aplicação e a execução de medidas restritivas aprovadas pela ONU ou pela UE e estabelece o regime sancionatório aplicável à violação das referidas medidas. Relativamente aos deveres previstos nesta lei o BdP emitiu o Aviso n.º 2/2018, de 26 de setembro, que regulamenta as condições de exercício, os procedimentos, os instrumentos, os mecanismos, as formalidades de aplicação, as obrigações de prestação de informação e os demais aspetos necessários a assegurar o cumprimento dos deveres preventivos do BC/FT, no âmbito da atividade das entidades financeiras sujeitas à supervisão do BdP, bem como os meios e os mecanismos necessários ao cumprimento por estas instituições.

O branqueamento de capitais é, segundo Rodrigues (2010), uma forma de criminalidade complexa, devido à existência de crimes subjacentes, ou crimes primários, como por exemplo o contrabando de pessoas, tráfico de armas, terrorismo, tráfico de droga, entre outros. O BC/FT será então um crime secundário que utiliza e usurpa o sistema financeiro na dissimulação e ocultação dos capitais obtidos de forma ilícita. No mesmo sentido, Jesus (2016) quando refere que, para além de ser crime por si só, sustenta algo mais preocupante que o crime financeiro, pois a montante e a jusante podem estar outros crimes muito mais graves do ponto de vista humano, sendo o terrorismo apontado como um dos crimes a jusante.

Faremos de seguida, e de forma resumida, a identificação das fases que constituem o branqueamento de capitais, que são três, de acordo com Ferreira (1999):

- Colocação (*placement*) – inserção do dinheiro no sistema económico-financeiro,

utilizando diversos meios, onde se incluem as tradicionais instituições financeiras, mas também outros estabelecimentos comerciais, e compra de diversos bens ou instrumentos monetários.

- Transformação/circulação (*layering*) – conjunto de transações de forma a ocultar a origem dos fundos, com movimentação constante entre bancos e países, de forma a dissimular a fonte dos capitais. Segundo Varela (2006) esta fase pretende tornar o rasto documental irrastrável para as autoridades, não permitindo a reconstrução dos movimentos efetuados.
- Integração (*integration*) – “os capitais já recolocados como se fossem originários de fonte aparentemente lícita, são completamente assumidos pelo sistema financeiro e integrados na economia legal e são investidos ou utilizados na aquisição de bens e serviços que constituem habitualmente sinais exteriores de riqueza” (Rodrigues, 2010, p. 22).

Segundo Duarte (2019) é nesta última fase que existe a integração dos bens e/ou dos valores na esfera patrimonial do criminoso a quem são devidos, e completa-se quando surgem com a aparência de lícitos e são usados livremente pelo criminoso.

Contrariamente ao branqueamento de capitais, “cujo objetivo é ocultar a origem criminosa dos fundos, no financiamento do terrorismo, um dos principais objetivos dos financiadores é ocultar a finalidade a que estes fundos se destina, e por isso toda a investigação é extremamente difícil pois muitas vezes são movimentados fundos monetários muito baixos e até lícitos para que sejam branqueados e misturados para assim não serem detetáveis pelas autoridades” (Braga, 2020, p. 25).

Estes criminosos branqueiam capitais e bens, obtidos de forma ilícita, para serem colocados, circulados e integrados no sistema financeiro, económico e legal e após lhes ser conferida legalidade, serem estes fundos/bens utilizados para pôr em prática atos terroristas ou financiar tais atos que ponham em causa diversos bens jurídicos como a vida, a integridade física, o Estado, a liberdade, entre outros (Banco de Portugal, 2020). E é na Lei n.º 52/2003, de 22 de agosto – Lei de Combate ao Terrorismo – que está previsto o financiamento do terrorismo como crime, com uma moldura penal de 8 a 15 anos.

Braga (2020), referindo-se ao reforço da eficácia no combate ao BC/FT aborda a criação, em 2015, da Comissão de Coordenação das Políticas e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo (Comissão BC/FT), cuja principal missão é acompanhar e coordenar a identificação, avaliação e resposta aos riscos de BC/FT a que Portugal esteja ou possa estar exposto.

Entre outros, fazem parte desta Comissão BC/FT, presidida pelo Secretário de Estado dos Assuntos Fiscais, a Polícia Judiciária, o BdP, a Ordem dos Contabilistas Certificados e o Coordenador da delegação portuguesa ao GAFI.

A Lei n.º 25/2008, de 25 de junho vem reforçar todos os deveres de prevenção do branqueamento

de capitais, prevê o congelamento e perda de bens dos autores de atos de terrorismo, apoiantes ou financiadores de tais grupos ou organizações e prevê ainda o dever de comunicar às autoridades quaisquer suspeitas de transações com ligações ao terrorismo (Braga, 2020).

Refira-se ainda que a Lei n.º 58/2020, de 31 de agosto, veio introduzir, como referido em Garrigues (2020), importantes novidades em relação à prevenção da utilização do sistema financeiro para práticas ilegais de branqueamento de capitais e também importantes novidades no âmbito penal e em matérias de proteção de dados pessoais. Vem nomeadamente estender o âmbito subjetivo da lei de combate ao BC/FT, ao acrescentar entidades obrigadas ao cumprimento deste normativo, como, por exemplo, gestores de fundos de capital de risco qualificados, Sociedades de Investimento e Gestão Imobiliária em Portugal ou entidades que exerçam qualquer atividade com ativos virtuais. Ainda como forma de beneficiar a transparência e o combate ao BC/FT, no âmbito do mundo digital, introduz uma definição de ativo virtual e de atividades com ativos virtuais. Em relação ao Regime Central do Beneficiário Efetivo (RCBE), regime jurídico aprovado pela Lei n.º 89/2017, de 21 de agosto, este passa a prever a necessidade de atualização da informação dele constante e confirmação da sua atualidade aquando da dissolução voluntária da entidade obrigada. O Beneficiário Efetivo (BE) pode ser definido como a pessoa singular que controla direta e ou indiretamente uma percentagem igual ou superior a 25% do capital de uma pessoa coletiva, sendo a sua identificação obrigatória e o tratamento e recolha de dados feito nos mesmos termos que as pessoas singulares. Note-se que apenas se não existirem pessoas singulares nas condições descritas, se devem identificar os BE pelo critério da direção de topo (administração, gerência, ou outro detentor de poder executivo).

De referir ainda que devido à atualidade e importância deste tema, a legislação sobre esta matéria está em constante atualização. As entidades sujeitas, e em particular os bancos, estão em constante alerta de forma a que os seus procedimentos e reportes estejam sempre em sintonia com os normativos e em cumprimento com as obrigações legais. No decorrer desta investigação surgiram novidades a nível nacional e europeu no que toca ao BC/FT. Assim, o BdP emitiu a Instrução n.º 2/2021 que define os fatores de risco reduzido e elevado de BC/FT e medidas específicas de identificação e diligência, simplificadas e reforçadas. Também a Comissão Europeia (CE), em julho de 2021, tornou pública uma ambiciosa e importante proposta de reforma do regime europeu de combate ao BC/FT, sendo que este novo pacote será integrado por quatro propostas de atos legislativos de diferente natureza. Verifica-se assim uma clara intenção de promover um reforço do papel das instituições da UE na prevenção do BC/FT, com a correspondente diminuição da competência dos Estados-Membros. Este reforço assenta no estabelecimento de regras comuns diretamente aplicáveis aos destinatários dos deveres e na criação de uma autoridade de supervisão europeia (Gomes J. G., 2022). A CE considera que existem atualmente sérias deficiências na aplicação da legislação em vigor e divergências entre os Estados-Membros, pelo que apresentou as seguintes propostas (Orrit & Rizzo, 2022, p. 3):

- Um Regulamento que cria a Autoridade para o Combate ao Branqueamento de Capitais

e ao Financiamento ao Terrorismo;

- Um conjunto único de regras em matérias de combate ao branqueamento de capitais e ao financiamento ao terrorismo, que incorpora parte da legislação;
- Uma nova diretiva, a sexta, revendo parte da restante legislação; e
- A reformulação do Regulamento de Transferência de Fundos para abranger os criptoativos”.

As matérias de BC/FT estão, como veremos mais à frente, intimamente relacionadas com a matéria de proteção de dados, exemplo disto é o parecer que a CE solicitou à Autoridade Europeia para a Proteção de Dados (AEPD) para se pronunciar sobre os aspetos mais relevantes do ponto de vista da proteção de dados presentes nesta iniciativa legislativa, preocupada em aumentar a eficácia da luta contra o BC/FT na UE.

2.3.2 O dever de identificação e diligência

Como atrás referido, o sistema bancário está identificado como atividade propensa a facilitar o BC/FT, tanto pelas suas características como pelo volume de capital envolvido em cada transação, permitindo a rápida rotação de capital e algum anonimato no processo de colocação e despistagem (Jesus, 2016). Este autor refere ainda que o branqueador aproveita as falhas do sistema e aproveita-se das vantagens criadas na facilitação do comércio e transações internacionais, dissimulando e reintegrando o capital de origem criminosa. As entidades financeiras estão pois, por força da lei, obrigadas a especiais deveres de identificação e relato de situações potencialmente suspeitas.

O princípio *Know Your Customer* (KYC) é um instrumento que é atualmente imposto às entidades bancárias, apesar de sempre ter havido uma relativa preocupação em conhecer a vida, o património e o perfil do cliente bancário. Desta forma, “o KYC é essencial na luta contra o branqueamento de capitais em instituições financeiras” (Duarte, 2019, p. 24). De acordo com Michugu (2014), citado por Duarte (2019), o KYC ajuda a reduzir os riscos associados ao branqueamento de capitais, à corrupção e à fraude. Este instrumento usa, frequentemente, uma classificação de alto, médio ou baixo nível de risco, e impulsiona a frequência de revisão das informações dos clientes.

Ainda segundo Duarte (2019) é essencial que os bancos comerciais detenham um sistema anti-branqueamento bem desenvolvido e que monitorize as transações das contas dos clientes diariamente e desde o início da relação comercial, dentro das diferentes unidades de negócio.

Independentemente do que se descreveu, o Relatório de Avaliação Mútua do GAFI refere o setor bancário como vulnerável em relação ao BC/FT “devido ao seu papel em relação aos fluxos financeiros que podem ser explorados por criminosos para fins de BC/FT” (Braga, 2020, p. 32).

O BdP impõe medidas preventivas ao BC/FT, previstas essencialmente em Instruções, sendo as

instituições financeiras obrigadas a relatar e a identificar suspeitas. Algumas dessas medidas incluem a comunicação obrigatória de todas as transações feitas por pessoas coletivas que efetuem transações com o exterior em quantias anuais superiores a €100.000, identificação de todas as partes, representantes ou beneficiários efetivos e transações iguais ou superiores a €15.000, numa única transferência ou em várias que perfaçam valor igual ou superior a este montante, que aparentem ter relação entre si (Jesus, 2016).

O mesmo autor refere-se à necessidade de identificação dos intervenientes das transferências, à sinalização e reporte dos depósitos em contas de terceiros, de valor igual ou superior a €10.000, ou sempre que haja suspeitas de BC/FT, também para montantes iguais ou superiores a €5.000.

Segundo Salgado (2015) o enquadramento legal português do combate ao BC/FT reforça a consagração dos deveres de identificação, comunicação, cooperação, diligência e segredo, e define o conceito de Pessoa Politicamente Exposta (PEP). Assim, segundo o art.º 2.º, n.º 6 da Lei n.º 25/2008, de 5 de junho, PEP são pessoas singulares que desempenham, ou desempenharam, até há um ano, altos cargos de natureza política ou pública, bem como membros próximos da sua família e pessoas que, reconhecidamente, tenham com elas estreitas relações de natureza societária ou comercial.

O quadro seguinte resume os deveres de prevenção inerentes ao BC/FT que as instituições financeiras devem cumprir e que passam por conhecer os clientes, as transações e os processos.

Quadro 2: Deveres preventivos

Conhecer o cliente - KYC	Conhecer as transações - KYT	Conhecer os Processos - KYP
Dever de identificação e diligência Aplicação de medidas de diligência reforçada Dever de recusa	Dever de Exame Dever de abstenção	Dever de controlo Dever de comunicação Dever de formação Dever de conservação Dever de não divulgação artigo - 20º Lei 58/2019 de 8 de agosto Dever de colaboração artigo - 8º Lei 58/2019 de 8 de agosto

Fonte: Banco BPI (2021).

Enquadrado, e revisto, o branqueamento de capitais, o ponto seguinte pondera limitações no âmbito da atividade bancária.

2.3.3 As limitações no combate ao branqueamento de capitais nos bancos

Para Duarte (2019) o setor dos serviços financeiros é um meio importante para a lavagem de dinheiro, identificando a globalização e as constantes mudanças das tecnologias de informação como facilitadores, pela velocidade e anonimato que conferem. A mesma autora identifica os bancos como as

instituições financeiras mais vulneráveis face ao BC/FT e posiciona os bancos enquanto meio apetecível para qualquer organização criminosa.

Já Salgado (2015) refere-se também à importância de detetar sinais de alerta, de modo a identificar irregularidades relacionadas com o BC/FT, o que se faz através do conhecimento do cliente e o acompanhamento das suas movimentações financeiras, na instituição.

Uma das forma de classificar esses sinais pode passar por associá-los a tipologias de operações, como faz Braguês (2009). Assim, de uma forma resumida, temos:

1. Transações em numerário:

- Abertura de conta para exclusivo depósito de numerário, nomeadamente em moeda estrangeira;
- Troca de notas de pequeno montante por notas de elevado montante, na mesma divisa ou divisa diferente;
- Aumento substancial de saldos sem causa aparente, de créditos em numerário, num curto prazo e subsequentemente transferidos para uma conta e/ou localização geográfica não associada normalmente à movimentação do cliente;
- Operações de compra e venda de moeda estrangeira, de montante consideravelmente elevado, sem justificação face à atividade declarada do cliente;
- Depósitos em numerário de valor significativo em caixas automáticas e para depósitos noturnos;
- Liquidação em numerário de aplicações em instrumentos financeiros.

2. Depósitos:

- Contas com frequentes depósitos de valores ao portador (cheques e vales de correio), seguidos de transferências;
- Depósitos efetuados em vários locais e em vários momentos sem uma razão lógica;
- Cliente efetua depósitos com alguma regularidade alegando tratar-se de valores provenientes de venda de ativos, que não podem ser comprovados.
- Contas que apresentam saldos aparentemente não compatíveis com a faturação do negócio em causa;
- Contas que apenas são utilizadas para transferência de fundos, nomeadamente de e para o estrangeiro.

3. Transferências:

- Transferências via internet de e para países e zonas geográficas consideradas de elevado risco;
- Transferências eletrónicas com entrada e saída imediata da conta, sem qualquer explicação lógica;
- Transferências efetuadas de e/ou para jurisdições fiscalmente mais favoráveis, sem motivos comerciais consistentes com a atividade conhecida do cliente;

4. Outras transações comerciais:

- A informação financeira da empresa difere significativamente da de outras empresas com a mesma atividade e de dimensão semelhante;
- Conta que foi reativada tornando-se de repente significativamente ativa;
- Recusa do cliente em fornecer informação necessária para formalizar um crédito ou qualquer serviço;
- Utilização acrescida de cofres de aluguer;
- Operações com recurso a crédito;
- Cliente inesperadamente liquida um empréstimo em contencioso;
- Concessão de crédito a cliente com património significativo;
- Não existem preocupações com condições e custos associados ao empréstimo;
- Operações de crédito amortizadas ou liquidadas por comerciantes, em numerário e em nome dos seus clientes (beneficiários).

Relativamente à posição dos bancos comerciais perante o branqueamento de capitais, Duarte (2019) refere-se às instituições financeiras como entidades com cada vez mais risco de lavagem de dinheiro e à necessidade de cumprir os regulamentos contra BC/FT impostos por órgãos reguladores e governos em todo o mundo. Acrescem ainda os riscos de estas entidades serem sancionadas pela participação intencional, ou facilitação involuntária, na lavagem de dinheiro.

A legislação e regulamentos anti-branqueamento de capitais são comumente designadas por ABC, e, segundo Duarte (2019), estes implementam, de uma maneira formal, a necessidade de comprovação da identidade dos clientes, declaração de fonte de rendimentos, a sua autenticidade, e se aquela corresponde totalmente ao valor real remetido para a conta dos clientes. A autora refere ainda que estas operações de monitorização exigem que os bancos obtenham e retirem registos de clientes sobre as suas informações pessoais, como a identificação, endereço do cliente e fonte de rendimento (KYC). Os bancos devem, portanto, melhorar os seus sistemas de informação, por forma a conseguir acompanhar as sofisticadas formas de branquear capitais.

Os bancos são forçados a cuidar a recolha de dados e a geração de informação como forma de mitigar o risco. Segundo Vicente (2014, p. 54) um dos principais riscos para as entidades bancárias é o risco de reputação, que “representa uma grave ameaça para as instituições financeiras (...) devido à natureza da sua atividade, é indispensável as instituições financeiras agirem em conformidade com padrões profissionais e éticos elevados, de modo a manterem a confiança no mercado em geral”. Também Salgado (2015) descreve vários riscos inerentes ao BC/FT, nomeadamente:

- Risco de reputação;
- Risco operacional (inerente ao procedimentos internos, ao *modus operandi* dos funcionários, que podem ser insuficientes e ineficientes);
- Risco legal;
- Risco de concentração;
- Risco de *compliance*.

Relativamente a este último o autor sinaliza a importância de as instituições financeiras criarem um sistema de gestão de riscos de BC/FT, que englobe políticas internas e de procedimentos para toda a organização, de forma a permitir que o sistema seja sólido e eficaz e abranja todos os produtos, atividades e processos, com informação completa, fiável e pertinente. Acrescenta ainda que a responsabilidade da gestão de riscos é de todos os colaboradores, a formação na temática de BC/FT é uma exigência legal, que as instituições financeiras devem ter estruturas internas especializadas nesta matéria, com um controlo interno eficaz que garanta o cumprimento e respetivo reporte das ações preventivas à Administração e que deve ser promovida a monitorização do sistema de gestão de risco implementado.

Apesar de existir um dever de colaboração por parte das entidades bancárias por força da lei, o pedido das autoridades deve-se mostrar individualizado e suficientemente concretizado. E tal como refere Ribeiro (2011), a disposição legal só pode ter como objetivo evitar o acesso a informação que poria em causa o direito à reserva da vida privada, de uma forma desproporcional. O mesmo autor também se refere à existência de tratamento de dados sensíveis, ou potencialmente sensíveis, e à necessidade de o tratamento das informações obtidas pelas entidades de combate ao BC/FT ter necessariamente de cumprir as demais disposições que concernem à proteção de dados pessoais.

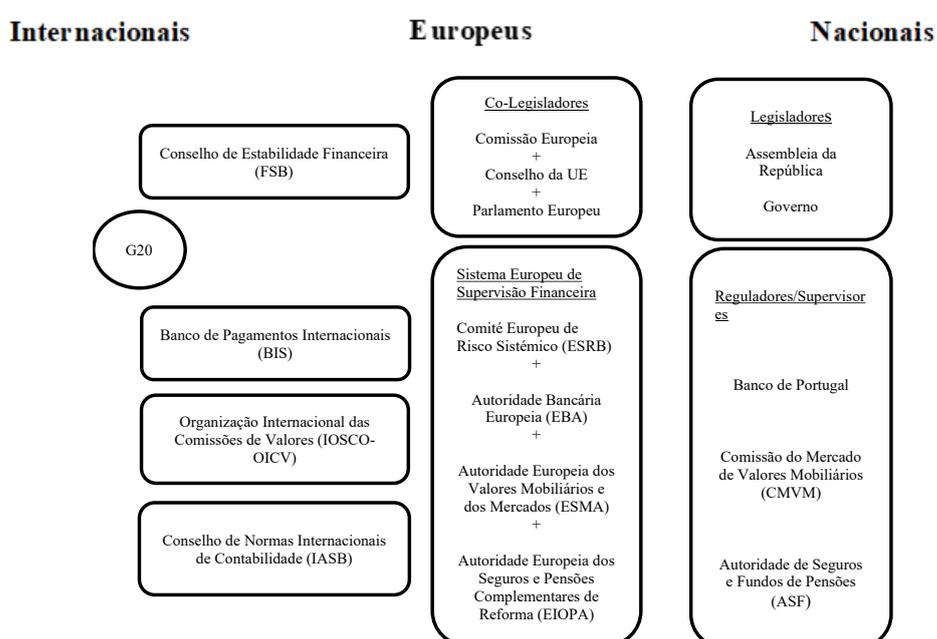
Apesar da existência de algumas limitações das entidades bancárias na prevenção do BC/FT, que não são apenas legais, são mesmo procedimentais e informáticas, como refere Monteiro (2015), perspetiva-se a manutenção da tendência, a nível interno e comunitário, de continuar a flexibilizar o acesso às informações cobertas pelo sigilo bancário.

2.4 O setor bancário português: entidades reguladoras, de supervisão e processo legislativo

Como refere Silva C. P. (2010), o papel das instituições de supervisão é evidente no que toca ao combate ao incumprimento dos normativos legais existentes, papel esse que ganhou relevo na década de 2000 com a introdução de um conjunto adicional de regras.

A imagem seguinte sintetiza as autoridades e instituições que intervêm no processo legislativo e regulamentar do sector bancário português e que atuam a nível internacional, europeu e nacional, através de iniciativas regulamentares que constituem o quadro de referência das regras a aplicar (Associação Portuguesa de Bancos, 2022).

Figura 1: Entidade reguladoras e de supervisão



Fonte: Associação Portuguesa de Bancos (2022).

Constata-se assim a quantidade de intervenientes e a complexidade das distintas perspetivas, factos que se aprofundam no ponto seguinte.

Quanto ao processo legislativo da União Europeia e à sua articulação com o modelo nacional importa sinalizar que são várias as entidades que emitem regras e recomendações, que são posteriormente adotadas no ordenamento jurídico europeu através de Diretivas e Regulamentos (Anexo I). Estes têm origem em propostas apresentadas pela Comissão Europeia e são objeto de negociação e aprovação pelo Conselho Europeu e pelo Parlamento Europeu (medidas de nível 1). Já as medidas de nível 2 resultam de mandatos atribuídos às autoridades europeias de supervisão para regularem sobre as decisões de nível 1. As mesmas autoridades europeias de supervisão podem ainda emitir *guidelines*, recomendações, entre outros suportes, denominadas medidas de nível 3, dirigidas às autoridades de supervisão nacionais competentes ou às entidades supervisionadas, que as adotam ou não, pois não são

vinculativas como as medidas de nível 1 e 2 (Associação Portuguesa de Bancos, 2022).

Quanto ao Anexo II, resume as entidades responsáveis, a nível europeu pelo modelo de supervisão financeira. Assim, o modelo de supervisão financeira em Portugal, nas vertentes comportamental e prudencial é composto por três entidades, o BdP, a CMVM e a Autoridade de Seguros e Fundos de Pensões (ASF), conforme podemos verificar no Anexo III. Destacamos aqui o BdP, a quem está cometida a supervisão prudencial e comportamental das instituições de crédito, segmento de mercado em análise no presente estudo.

O BdP é o banco central da República Portuguesa, e é uma pessoa coletiva de direito público. Faz parte do Eurosistema e do Sistema Europeu de Bancos Centrais, do Mecanismo Único de Supervisão e do Mecanismo Único de Resolução. Tem como missões essenciais a manutenção da estabilidade dos preços e a promoção da estabilidade do sistema financeiro (Banco de Portugal, 2022).

A supervisão bancária tem assim como principais objetivos os sintetizados por Serralheiro (2015, p. 25): “evitar o risco sistémico; proteger os depositantes, através da promoção da estabilidade e saúde financeira das instituições de crédito; proteger os depositantes em caso de falência; proteger os depositantes e os clientes de serviços financeiros, procurando minimizar a sua posição de contraente mais fraco; promover a transparência do sistema financeira; proteger contra o crime financeiro ou contra o crime cuja prática seja facilitada pelo uso do sistema financeiro”, aqui se incluindo o combate ao BC/FT.

O BdP tem competências de supervisão preventiva do BC/FT do setor financeiro e assume-se que deva zelar, em primeira linha, pelo cumprimento dos deveres, já antes elencados, por parte das entidades financeiras e verificar a adoção, por estas, dos meios e mecanismos necessários a assegurar o cumprimento das medidas restritivas. Tem ainda competências de regulação e participa na elaboração do quadro normativo referente à prevenção de BC/FT, com representação em várias instâncias como o GAFI e a Comissão BC/FT.

Analisados os três referenciais que servem de base ao presente estudo, cumpre-nos sistematizar os fatores críticos na sua compatibilização, elemento que consta no ponto seguinte.

2.5 Fatores críticos na compatibilização da proteção de dados pessoais, sigilo bancário e combate ao BC/FT

Os três referenciais abordados são basilares e atuais na atividade bancária. Assim, seguidamente, ponderam-se dimensões de análise e fatores críticos, da sua implementação e compatibilização.

2.5.1 No domínio dos diplomas legais

Da análise individual a cada um dos referenciais anteriormente elaborada, conseguimos aferir que o sigilo bancário e a prevenção do BC/FT dificilmente andam de “mãos dadas”, pelo contrário, são até

contraditórios. Se o primeiro exige segredo, reserva e confidencialidade, já o o segundo exige o acesso a dados e informação bancária. Nas palavras de Rodrigues S. M. (2010) o sigilo bancário levanta problemas à prevenção do BC/FT, na medida em que, se por um lado, protege o cliente honesto, por outro, encobre o cliente fraudulento. O mesmo autor refere que o sigilo bancário é uma matéria encadeada no processo de lavagem de dinheiro, na medida em que favorece o encobrimento dos capitais de origem ilícita, bem como a reciclagem.

Relativamente ao combate à fraude e evasão fiscal, refere Monteiro (2015) que a derrogação do sigilo bancário, será, sem dúvida, uma importante ferramenta na repressão deste tipo de ilícitos, *mutatis mutandis*, também no que toca à prevenção do BC/FT, o acesso a dados bancários, com quebra de sigilo, é um meio importante e eficaz no seu combate.

Um outro ponto contraditório será que, e segundo Semedo (2015), o instituto do sigilo bancário envolve valores e interesses constitucionalmente protegidos, mas circunscritos à esfera individual, ao invés do crime de BC/FT que nos remete para valores e interesses mais altos, supra-individuais, e também constitucionalmente protegidos. Para Vicente (2014) é evidente que o combate ao branqueamento de capitais, ao longo dos tempos, se tem vindo a sobrepor ao sigilo bancário, estando este cada vez mais enfraquecido, quase até ao ponto de ser abolido.

Também segundo Athayde, Athayde e Athayde (2009) o equilíbrio entre transparência e sigilo é difícil de atingir, mas indispensável. Pois a extinção do sigilo não só empobrece o regime jurídico da banca, mas entre outros males, é também um sério recuo ético. Este equilíbrio é muito difícil de alcançar, pois se existe um aumento da eficiência do ponto de vista da atuação penal transnacional, inevitavelmente limita em grande escala a proteção dos interesses individuais (Vicente, 2014).

Tal como já anteriormente foi referido, e também segundo Vicente (2014), o relacionamento entre o branqueamento e o sigilo deve ter em conta o princípio do interesse preponderante. Assim, em caso de conflito de interesses deve ser feita a apreciação da natureza e relevância dos bens jurídicos tutelados, restringindo-os, num caso concreto, segundo um critério de proporcionalidade. Deve prevalecer o dever que tutele o interesse sensivelmente superior, e “desde que seja razoável impor ao lesado o sacrifício do seu direito ao sigilo, tendo em atenção a natureza e os valores do interesse prosseguido com a divulgação” (Vicente, 2014, p. 75). Acrescenta ainda que a quebra de sigilo tem de ser fruto de uma profunda ponderação de interesses e não deve ir além do estritamente necessário.

O mesmo autor, referindo-se à jurisprudência, sinaliza que o sigilo é considerado um direito fundamental inferior, que deve ceder, tendo apenas como limites os critérios da necessidade e proporcionalidade. Justificando-se esta cedência pelo facto da repressão e prevenção do branqueamento visarem a salvaguarda do interesse público, classificado como interesse superior perante o direito à reserva da intimidade da vida privada. No mesmo sentido, nas conclusões da sua dissertação, Semedo (2015, p. 79) refere que “os interesses e valores que representam menores consequências face às

restrições (estritamente necessárias), que devem ser impostas, devem ceder-se perante os interesses e valores de maior relevo social, mediante critérios de ponderação objetivos e credíveis.”

Já Monteiro (2015) refere que o sigilo bancário não é um direito absoluto e que pode sofrer restrições em prol de outros interesses e valores igualmente importantes, fazendo obviamente referência aos interesses públicos que se elevam. Não deixa contudo de afirmar que o sigilo bancário abarca uma parte importante da vida pessoal e patrimonial do cliente bancário e que a revelação de aspetos da sua vida económica, leva também ao desvendamento de aspetos da sua vida privada.

Se o sigilo bancário e a prevenção do BC/FT são, no espírito do legislador contraditórios, também o mesmo se passa com a prevenção do BC/FT e a proteção de dados pessoais. Aqui pretende-se acautelar a privacidade e minimizar os abusos do uso de dados pessoais, pelo contrário na prevenção do BC/FT quanto maior o acesso a dados e informação melhor, pois sem dados não há nada, nem sequer é possível estabelecer uma relação de negócio.

A Lei n.º 58/2020, de 31 de agosto para além de ter introduzido as novidades já referidas no que toca à prevenção da utilização do sistema financeiro para práticas ilegais de branqueamento de capitais, também traz novidades em matérias de proteção de dados pessoais, conforme citadas por Garrigues (2021):

- Os canais (específicos e anónimos) de comunicação de irregularidades relacionadas com eventuais violações da Lei n.º 83/2017 devem garantir a confidencialidade das comunicações recebidas e a proteção dos dados do denunciante e do suspeito da infração, conforme o RGPD;
- As entidades obrigadas, desde logo as instituições de crédito, têm de fornecer aos novos clientes um aviso geral sobre as obrigações legais que lhes são aplicáveis em matéria de dados pessoais e seu tratamento, para efeitos de prevenção do BC/FT;
- Reconhecimento legal de que a proteção de dados aqui tratada é do domínio do interesse público;
- Redução para metade do valor máximo da coima aplicável às contraordenações de proteção de dados, a título de exemplo, à não adoção de medidas de segurança, à efetiva proteção de informação e dos dados pessoais tratados, à ausência de informação aos novos clientes sobre tratamento de dados pessoais e à não eliminação do prazo estabelecido na Lei n.º 83/2017.

Podemos assim verificar que os normativos que regulam ambas as temáticas tendem a caminhar num sentido comum, ou pelo menos não contraditório, e existe a preocupação com a proteção de dados pessoais na prevenção ao BC/FT. Contudo, e como previsto pelo próprio RGPD, o direito à proteção de dados pessoais não é absoluto e, como refere Borralho (2019), deve ter-se em consideração a sua função

na sociedade e equilíbrio com outros direitos fundamentais, sempre na lógica do princípio da proporcionalidade, e remetendo-nos sempre para decisões casuísticas. O autor refere-se à fronteira entre a liberdade de imprensa e a proteção de dados pessoais, sinalizando que a dualidade entre o individual e o coletivo apresenta uma fronteira nebulosa, de difícil definição. O mesmo se poderá dizer relativamente à fronteira entre a prevenção do BC/FT e o direito à proteção de dados pessoais, sem esquecer, como refere o autor, que o cumprimento do RGPD é incontornável e transversal.

Também o CEPD emitiu, em dezembro de 2020, parecer relativo à relação da proteção de dados pessoais e a prevenção do BC/FT. Este parecer surge na sequência de um Plano de Ação da UE relativo às políticas de BC/FT no sistema financeiro que pretende a implementação de um novo pacote de medidas legislativas, com regras únicas e que abranja todos os serviços financeiros europeus e, por sua vez, abranja todas as pessoas que utilizam esse sistema financeiro. A implementação de novas medidas são uma oportunidade de abordar e rever a interação destas duas temáticas, bem como a sua concreta aplicação. O CEPD entende que uma estreita articulação dos normativos beneficiará a proteção de dados pessoais e também a eficácia da legislação de BC/FT e reitera a necessidade de uma base legal clara sobre o tratamento de dados pessoais, definição dos propósitos e limites desse tratamento, de acordo com o art.º 5.º (1) do RGPD. E em particular no que toca à partilha e transferência internacional de dados. Desta forma, esta entidade considera que qualquer pacote legislativo a ser criado deverá ter atenção à perspectiva da proteção dos dados pessoais e o direito à privacidade (Jelinek, 2020).

A Autoridade Europeia para a Proteção de Dados (AEPD) emitiu um parecer em setembro de 2021, onde se congratula com os objetivos do novo pacote legislativo, e que no fundo visam aumentar a eficácia no combate ao BC/FT, em especial pela necessidade de harmonização das regras aplicáveis e de uma supervisão reforçada a nível da UE. A AEPD apesar de concordar com a abordagem baseada no risco de controlo da utilização do sistema financeiro para o BC/FT, considera que o pacote legislativo deverá ter em conta algumas observações e recomendações, a saber, e entre outras, “deverá especificar, em especial, que tipo de categorias de dados pessoais a tratar pelas entidades obrigadas... em vez de deixar sistematicamente esta especificação para as normas técnicas de regulamentação, bem como descrever melhor as condições e os limites aplicáveis ao tratamento de categorias especiais de dados pessoais relativos a condenações penais e infrações... deverá especificar, em especial, que tipos de categorias especiais de dados pessoais deverão ser tratados pelas entidades obrigadas, tendo em conta os princípios da necessidade e da proporcionalidade, considerando as diferentes atividades e medidas a tomar (identificação, diligências adequadas quanto à clientela, comunicação às Unidades de Informação Financeiras, bem como a finalidade específica visada (ou seja, o combate ao BC/FT). Em especial a AEPD considera que não deve ser permitido o tratamento de dados pessoais relacionados com a orientação sexual ou a origem étnica” (Wiewiórowski, 2021, p. 1).

No mesmo parecer a AEPD faz ainda considerações relativamente aos BE, nomeadamente, referindo que a lista de especificação das informações relativas a estes deve ser exaustiva e convidar o

legislador a especificar que o acesso aos registos dos BE se deve limitar à finalidade da luta contra o BC/FT e ser autorizado apenas para esse fim, bem como que o acesso não deve ser público, mas restrito às autoridades competentes responsáveis pela aplicação da lei e às entidades obrigadas.

Os exemplos identificados ilustram a necessidade de harmonização entre os normativos que regulam as matérias de BC/FT e a proteção de dados. Resta-nos aferir se, em termos práticos, essa compatibilização é exequível e de que forma se consegue alcançar.

2.5.2 No domínio da eficiência dos fluxos de trabalho

Se, como vimos anteriormente, a compatibilização dos normativos é desejável mas não é fácil, tal situação pode condicionar fluxos de trabalho. Segundo Borralho (2019, p. 75) “recolher e armazenar dados, processar esses dados em conformidade com padrões e disponibilizar informação tempestivamente, impõe a conjugação de processos, pessoas e tecnologias, numa arquitetura que nem sempre é fácil, e onde o alinhamento é desejado, independentemente das dificuldades operativas em o concretizar”. Ora tal situação pode ainda ser mais complexa quando em presença de normativos legais suscetíveis de interpretações não harmonizáveis, normativos que podem mesmo apontar alternativas contraditórias. Os bancos, como empresas que são, pretendem apresentar os melhores resultados, cumprindo os objetivos comerciais a que se propõem e em cenários altamente competitivos, obviamente sempre sujeitos aos normativos que regulam a sua atividade.

No que toca ao binómio branqueamento e sigilo Vicente (2014) refere-se à importância das instituições bancárias no alcance do ponto ótimo de equilíbrio deste relacionamento, pois a eventual morosidade das respostas oficiais quando decretada a quebra do sigilo bancário, pode ser um impedimento ao sucesso da investigação das práticas de branqueamento. Enfatiza assim o tempo como determinante da eficiência, ou da sua falta.

Também Vicente (2014, p. 55) refere o risco operacional como representativo da “potencial ameaça derivada da deficiência ou falha dos procedimentos internos, como por exemplo, condutas inapropriadas dos funcionários, controle ineficaz dos referidos procedimentos, inadequação ou incumprimento dos programas e das estratégias delineadas pela instituição para combater o branqueamento de capitais”. Ora o problema aqui passa por estabilizar o que se entende por condutas inapropriadas dos funcionários e o que fazer para as tornar apropriadas.

Já no que à proteção de dados diz respeito, e ainda que haja liberdade para a escolha dos procedimentos que as instituições venham a utilizar no tratamento de dados pessoais, o art.º 30.º do RGPD impõe, como refere Teves (2019), que exista um registo das atividades de tratamento, as finalidades, fundamentos da licitude de tratamento, definição de categorias de dados pessoais e prazos de conservação dos mesmos, categorias de titulares de dados, categorias de destinatários de dados pessoais, e definição de medidas técnicas e organizativas de segurança. Estes registos são efetuados por escrito e são facultados à CNPD a seu pedido.

Em relação aos processos que envolvem dados pessoais passíveis de serem acedidos ou manipulados Pinho (2017) refere que mesmo cifrados, ou pseudonimizados, os dados podem continuar a ser pessoais, cabendo a cada organização a identificação desses processos, a avaliação dos riscos e a definição de procedimentos que assegurem o seu tratamento conforme com os normativos legais.

Um processo de tratamento de dados, segundo Mendes (2018), é qualquer processo organizacional em que sejam tratados dados pessoais. Segundo este mesmo autor, com base nos tipos

de dados pessoais e nos processos que tratam esses dados, pretende o RGPD que se faça a análise aos riscos e às atividades para que seja possível a aplicação de medidas e controlos de segurança de informação, necessários à mitigação desses riscos e à garantia de que os dados pessoais estão protegidos de abusos e ameaças. Fonseca, et al., (2018) destacam a importância do profissional da informação na adequação às obrigações impostas pelo novo regulamento, uma vez que é este que detém competências ao nível de serviço de gestão de informação e arquivo, que permitem a integridade e autenticidade dos documentos, mantendo-se assim o equilíbrio entre a proteção dos interesses das pessoas e a proteção da liberdade de informação.

Ora a banca está obrigada ao cumprimento estrito dos normativos relativos aos três referenciais em apreço, o que pode ser feito com diferentes abordagens e importando-nos perceber como podem ser utilizadas tecnologias e fluxos de trabalho de forma a ser alcançada a eficiência. Ou seja, existirão fluxos de trabalho que permitam consumir menor quantidade de recursos e obter os mesmos resultados, ou, com a mesma quantidade de recursos, permitam obter melhores resultados, são questões práticas essenciais para qualquer banco. Como refere Borralho (2019, p. 19) “entender o desenho e a execução de processos de negócio é também entender os meios que podem sustentar a melhoria das organizações, acrescentando adiante que “há, no entanto, princípios e sequências de tarefas que, se consideradas, facilitam resultados. O estudo de caso a desenvolver permitir-nos-á indagar os fluxos de trabalho relativamente às temáticas do RGPD, BC/FT e sigilo bancário, ou o mesmo será dizer processos de negócio do banco, que segundo o ora citado autor não são mais do que a tradução de um conjunto de atividades das organizações, orientadas para a produção de bens e serviços, que implicam entradas, transformação e saída e utilizam múltiplos recursos, físicos, financeiros e informacionais.

2.5.3 No domínio da informação: registos e documentos de suporte

O ponto de partida do nosso estudo obriga-nos a ter sempre presente o conceito de dados, em particular de dados pessoais e os processos de negócio, enquanto fluxos de trabalho, numa perspetiva prática, operativa. O conceito de dados é descrito por Borralho (2019) como elementos atómicos, atributos, características ou ocorrências não tratadas, elementos que podem, ou não, encontrar-se estruturados, mas aos quais ainda não foi adicionado um padrão interpretativo. Já a informação decorre, para o mesmo autor, do processamento de dados, da sua ordenação e classificação, acrescentando ao conceito de dados o elemento padrões que possibilita a formação da matriz interpretativa. A informação é assim uma construção humana, de carácter instrumental na otimização de processos de trabalho, refletindo a atribuição de significado a factos, condicionando naturalmente a utilização de tecnologias. Resulta do que se descreveu que entender quais os dados a registar, os momentos, os suportes a usar nesses registos, são elementos fundamentais para acautelar a eficiência do trabalho, mitigando redundâncias e congestionamentos.

Sousa L. S. (2016) aponta o fenómeno socioeconómico da globalização como fonte de crescentes

mudanças na forma de gestão das empresas, privadas e públicas. Segundo o autor estas devem modernizar e melhorar as suas tarefas e propor a existência de um modelo piloto de gestão de processos como ferramenta integradora, alcance de resultados e padronização de documentos e de rotinas. Desta forma também, segundo Silva (2011), é inevitável que as empresas persigam o objetivo de melhorar os seus processos, ainda que muitas não possuam ainda uma compreensão total de como os processos interagem entre si. Para Antunes (2008) existem atividades que proporcionam melhorias no desempenho das organizações, sendo estas práticas de gestão por processos que englobam o mapeamento, coordenação, melhoria e consequente integração na cultura organizacional. No mesmo sentido Borralho (2018) sinaliza a necessidade de alinhar fluxos de trabalho e de informação, como condição para potenciação da eficiência da gestão.

Partiremos então nesta dissertação dos normativos legais, gerais e abstratos, para chegarmos aos processos de negócio, aqui entendidos como fluxos de trabalho, como sequências de tarefas concretas na atividade bancária. Como refere Silva I. F. (2013) na busca de melhores resultados e face à crescente competitividade do mercado, as organizações têm vindo a repensar os seus processos e a questionar os seus modos de operação, acrescentando ainda que os mercados retalhistas não são exceção, sendo-lhe exigidos parâmetros de excelência em todas as operações e melhorias constantes nos seus processos, de forma a torná-los mais eficazes, eficientes e integrados.

Podemos então definir processo como uma ordenação específica das atividades de trabalho no tempo e no espaço, com um início e um fim claramente identificados (Davenport, 1994). Os processos implicam assim um grupo de tarefas interligadas de um forma lógica, que utilizam os recursos da organização para gerar os resultados definidos de forma a apoiar os seus objetivos (Harrington, 1998). Para Borralho (2019) processos são sequências de atividades e toda a sequência que permita um consumo menor de recursos para obter os mesmo resultados, desde tempo a energia, matéria ou informação, será mais eficiente, comparativamente a alternativas.

Relativamente à abordagem por processos Antunes (2008, p. 31) refere que podem ser utilizadas duas formas fundamentais: “ identificar os fluxos de informação e ao longo dos mesmos determinar qual a informação que é necessária para efeitos de monitorização, medição e gestão; identificar os fluxos dos materiais e ao longo dos mesmos proceder de forma idêntica”, sendo a abordagem por processo, de acordo com a ISO/TC 176/SC 2 – ISO Technical Committee n.º 176, Sub-committee n.º 2, 2008, citada pelo mesmo autor, uma ferramenta que permite às organizações gerir as suas atividades acrescentando valor para os clientes e outras partes interessadas. Silva J. S. (2011) refere que o objetivo da abordagem por processos é atingir os objetivos com eficácia e eficiência, aumentando o nível de satisfação dos clientes, sendo as atividades organizadas e geridas horizontalmente, atravessando barreiras entre as diferentes unidades funcionais e unificando os esforços para as metas da organização.

Numa qualquer atividade comercial, onde a atividade bancária se inclui, a recolha de informação

sobre os seus clientes é uma importante arma na prossecução dos seus objetivos. Weber (2010), citado por Coreni (2018), indica que a garantia de segurança e privacidade de dados é crucial e indissociável da definição de processos fiáveis. Acresce que todo o negócio bancário é centrado em serviços, onde a recolha, o tratamento de dados e geração de informação apresentam um papel nuclear. Tal situação justifica que apresentemos aqui algumas considerações sobre o conceito e a importância da informação, bem como de sistemas de informação.

Rodrigues L. S. (2002) entende que a informação é o resultado da interpretação de dados, sendo que o tratamento destes dados pode ser analisado a partir dos sistemas que a suportam. Os sistemas de informação (SI) são, segundo Borralho (2019, p. 47) “formados por tecnologias de informação e comunicação, por pessoas e por processos. Estes últimos entendidos enquanto acções, modos de relacionar pessoas e tecnologias.” Este entendimento é apresentado em diversas referências na literatura. A título de exemplo, também Alter (1992) define SI como a combinação de procedimentos, informação, pessoas e tecnologias de informação, organizadas para o alcance dos objetivos de uma organização. Adicionalmente, O'Brien (1994) também posiciona os SI como o conjunto de pessoas, procedimentos e recursos envolvidos na recolha, no processamento e disponibilização de informação na organização.

Em suma, e conforme refere Rodrigues J. d. (2010, p. 19), “podemos dizer que um SI tem uma componente técnica, da qual faz parte o seu equipamento, *software* e dados para serem processados e, uma componente social, onde se incluem as pessoas e os procedimentos, com o objetivo de reunir informação”.

Laudon e Laudon (2014) referem que a capacidade de ação de uma empresa está diretamente relacionada com a capacidade dos seus sistemas de informação (SI), ou seja, da forma como se articulam pessoas e tecnologias para produzir e para usar informação.

Face ao que se descreveu, compreender a operacionalização e a compatibilização dos referenciais legais, obriga a considerar as múltiplas partes de um sistema de informação bancário, com destaque para as pessoas e para as tecnologias que essas pessoas usam para realizar trabalho. Neste contexto, descrever processos de negócio significa detalhar fluxos de trabalho e perceber como podem ser melhorados.

Já Kettinger & Groven (1995) definem processos de negócio como um conjunto de tarefas logicamente relacionadas, com utilização de recursos de uma organização, para alcançar um resultado. A simplificação e melhorias dos processos de negócio, e desenvolvimento dos sistemas de informação, destacando, quer as tecnologias usadas, como o envolvimento de pessoas, com culturas e idiossincrasias diferentes, é um requisito fundamental do aumento da eficiência. Também Silva (2011) aponta na mesma direção e indica que é necessário identificar e compreender os fluxos de informação existentes, tanto da informação que flui dentro de um só processo como entre vários.

Indissociável de tudo isto é o RGPD que, segundo Coreni (2018), é uma forma de sensibilizar as organizações para a importância de garantir a segurança de informação, uniformizar o ciclo de vida dos

dados e evitar a sua utilização excessiva, sendo que os processos de negócio e os SI ganham uma outra dimensão, pois têm agora uma função essencial no cumprimento das exigências legais de proteção de dados. Como também referem Fonseca et al (2018) o RGPD trouxe responsabilidades acrescidas às organizações impondo-lhes medidas técnicas e organizacionais na garantia de conservação de dados pelo tempo indispensável, na sua proteção, na utilização apenas para a finalidade para que foram recolhidos, e exigindo a implementação de medidas de segurança de informação que mitiguem os riscos de quebra de segurança. Importa assim acautelar a maturidade dos processos nas organizações (Mendes, 2018). Também neste contexto Vicente (2014, p. 27) refere que “o facto de a maioria das informações bancárias relativas aos clientes estarem arquivados em ficheiros automatizados, de bases e bancos de dados pessoais, o sigilo atualmente também depende em grande medida das leis de proteção de dados face à informática”. Ou seja, além do papel das pessoas reforça o papel das tecnologias.

Consequência de tudo o que se descreveu, nas suas várias recomendações, o GAFI, considera essencial que as instituições financeiras procedam à verificação e identificação de todos os clientes, bem como dos BE das operações, proibindo as contas anónimas ou com nomes fictícios, devendo os deveres de diligência ser intensificados quanto a operações efetuadas por entidades sinalizadas. Acresce ainda que devem guardar os registos e documentos relativos a todas as operações, e caso surjam suspeitas de branqueamento as instituições financeiras devem estar aptas a cumprir o seu dever de as declarar às autoridades competentes e fornecer o necessário à satisfação das necessidades de provas dos processos criminais (Vicente, 2014).

Ainda sobre as recomendações do GAFI, em nenhuma se estabelece qualquer limite mínimo para a proteção da confidencialidade, antes pelo contrário, segundo Vicente (2014, p. 96), pois “são várias as recomendações que colidem com o dever de sigilo bancário e como se não bastasse, ainda estabelece que o sigilo bancário não pode ser um impedimento para a devida aplicação das suas recomendações”.

No seio da UE é de referir ainda a Diretiva 2001/97/CE do Parlamento Europeu e do Conselho, de 4 de dezembro de 2001, transposta para o direito interno português, através da Lei n.º 11/2004, de 27 de março, no reforço de requisitos e medidas específicas, aí entendidas como adequadas, de identificação dos clientes das instituições financeiras, como forma de combate ao BC/FT decorrente das operações à distância (Vicente, 2014).

O quadro seguinte apresenta perspetivas e elementos a considerar para os três referenciais legais.

Quadro 3: Perspetivas e variáveis a considerar na aplicação do RGPD, BC/FT e Sigilo Bancário

Dimensão	RGPD	BC/FT	Sigilo Bancário
Âmbito de Aplicação	<ul style="list-style-type: none"> – Todas as entidades que efetuem o tratamento de dados pessoais, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante, onde se incluem as instituições de crédito 	<ul style="list-style-type: none"> – Instituições de Crédito – art.º 3.º, nº 1 a) Lei n.º 83/2017 de 18 de agosto 	<ul style="list-style-type: none"> – Atividade bancária, na sua amplitude máxima, modelo da banca universal - art.º 4.º RGICSF
Entidades responsáveis ou Autoridade de Controlo	<ul style="list-style-type: none"> – Comissão Nacional de Proteção de Dados (CNPd), art.º 3.º e seguintes Lei n.º 59/2019, de 8 de agosto 	<ul style="list-style-type: none"> – BdP – CMVM, conforme a atividade específica, como entidade de supervisão – São ainda interlocutores privilegiados com as instituições financeiras a Unidade de Informação Financeira da Polícia Judiciária (UIF), a PGR e a Direção-Geral de Política Externa do Ministério dos Negócios Estrangeiros 	<ul style="list-style-type: none"> – BdP
Responsabilidades internas	<ul style="list-style-type: none"> – Responsável pelo tratamento - art.º 24.º RGPD – Encarregado de proteção de dados (DPO) - art.º 9.º Lei n.º 58/2019, de 8 de agosto 	<ul style="list-style-type: none"> – As entidades obrigadas designam um elemento da sua direção de topo ou equiparado para zelar pelo controlo do cumprimento do quadro normativo em matéria de prevenção do BC/FT – O órgão de administração das entidades obrigadas é responsável pela aplicação das políticas e dos procedimentos e controlos em matéria de prevenção de BC/FT – No âmbito da gestão de risco as entidades obrigadas identificam, avaliam e mitigam os concretos riscos de BC/FT existentes no contexto da sua realidade operativa específica, incumbindo-lhe identificar os riscos de BC/FT inerentes à sua realidade operativa específica – art.º 13.º e seguintes Lei n.º 83/2017, de 18 de agosto 	<ul style="list-style-type: none"> – Todos os colaboradores e administradores nas relações com clientes, definido através de códigos internos de ética e de conduta – Dever de confidencialidade, não informando os clientes sobre possíveis investigações ou reportes sobre os mesmo no âmbito do BC/FT

Dimensão	RGPD (exemplo de dados pessoais)	BC/FT	Sigilo Bancário
Dados pessoais a recolher	<ul style="list-style-type: none"> - Dados de identificação e de contacto, bem como dados fiscais e profissionais e as qualificações do respetivo titular, incluído: - Assinatura - Data de nascimento - Endereço completo da residência permanente quando diverso, do domicílio fiscal - Fotografia - Nacionalidade constante do documento de identificação - Naturalidade - Nome completo - Número de identificação fiscal ou, quando não disponha de número de identificação fiscal, o número equivalente emitido por autoridade estrangeira competente - Profissão e entidade patronal, quando existam - Tipo, número, data de validade e entidade emitente do documento de identificação 	<ul style="list-style-type: none"> - Situações Standard: Dados de identificação e de contacto, bem como dados fiscais e profissionais e as qualificações do respetivo titular, incluindo: - Assinatura - Data de nascimento - Endereço completo da residência permanente quando diverso do domicílio fiscal - Fotografia - Nacionalidade constante do documento de identificação - Naturalidade - Natureza da relação de negócio - Nome completo - Número de identificação fiscal ou, quando não disponha de número de identificação fiscal, o número equivalente emitido por autoridade estrangeira competente - Outras nacionalidades não constantes do documento de identificação - Profissão e entidade patronal, quando existam - Tipo, número, data de validade e entidade emitente do documento de identificação 	<ul style="list-style-type: none"> - Todos e quaisquer dados ou informações pessoais, mesmo que não sejam tratados ou recolhidos estão sujeitos ao absoluto sigilo bancário - Só se pode fazer uso da informação recebida para o fim subjacente à sua recolha, sendo totalmente proibido o acesso que não seja estritamente exigido para o desempenho da atividade. - O sigilo é um dever fundamental em matéria de proteção de dados, que obriga os responsáveis pelo tratamento de dados pessoais, mas também quaisquer pessoas, no exercício das funções, mesmo após o termo das funções ou mandatos

Dimensão	RGPD (exemplo de dados pessoais)	BC/FT	Sigilo Bancário
Documentos para comprovação de dados	<ul style="list-style-type: none"> - Assento de nascimento, no caso de menores - Comprovativo de profissão e/ou entidade patronal: particulares e profissionais liberais: recibo de vencimento, declaração da entidade patronal ou cartão profissional emitido por ordem profissional ou entidade patronal - Comprovativo de residência fiscal: quando a morada de residência permanente é diversa da morada de residência fiscal deverá ser obtido certificado de residência fiscal ou documento equivalente emitido pelas autoridades fiscais do país de residência - Comprovativo de residência permanente: cartão de cidadão desde que o cliente digite o código que permite o acesso/ leitura dessa informação, faturas domésticas, declaração de rendimentos ou nota de liquidação de IRS. - Documento de identificação fiscal: cartão de cidadão, cartão de contribuinte ou documento público onde conste o número fiscal de contribuinte - Documento de identificação pessoal: cartão de cidadão, bilhete de identidade ou documento equivalente válido onde conste fotografia e assinatura; - Empresários em Nome Individual: declaração de início de atividade ou mudança de atividade emitida pela Repartição de Finanças (Modelo 1483) ou Anexo B do Modelo 3 do IRS 	<ul style="list-style-type: none"> - Autorização de residência, se cidadão estrangeiro a residir em Portugal - Comprovativo de atividade profissional - Comprovativo da morada fiscal e/ou permanente (se divergente apresentar um comprovativo de cada - Documento de identificação fiscal - Documento de identificação válido (naturalmente, sempre que em presença de cartão de cidadão o documento de identificação fiscal coincide com o de identificação civil) 	<p style="text-align: center;">-</p>

Dimensão	RGPD (exemplo de dados pessoais)	BC/FT	Sigilo Bancário
Momentos de recolha e tratamento de dados	<ul style="list-style-type: none"> - Mediante o preenchimento de formulários, no momento de abertura de conta, contratação de cartão de crédito, adesão a canais digitais, celebração e execução de contratos de aquisição de produtos bancários e de instrumentos financeiros, contratos de gestão de carteira, concessão de crédito, prestação de serviços financeiros, aquisição de produtos financeiros e/ou e seguros de que a entidade bancária seja agente 	<ul style="list-style-type: none"> - Antes do estabelecimento da relação de negócio ou da realização de qualquer transação ocasional: de montante igual ou superior a €10.000, independentemente de a transação ser realizada através de uma única operação ou de várias operações aparentemente relacionadas entre si, ou que constituam uma transferência de fundos monetários superiores a €1.000; se suspeite que as operações, independentemente do seu valor e de qualquer exceção ou limiar, possam estar relacionadas com o B/C ou F/T; existam dúvidas sobre a veracidade ou a adequação dos dados de identificação dos clientes previamente obtidos. - Nas transações ocasionais deve ser verificada a atualidade dos elementos apresentados - Realização de diligências adicionais para comprovação da informação obtida, no âmbito das medidas reforçadas 	-
Conservação de documentos	<ul style="list-style-type: none"> - Período mínimo necessário para cumprir as finalidades da recolha, enquanto forem necessários para a relação comercial e pelos prazos legais obrigatórios: - É permitida a conservação por períodos mais longos se visar fins históricos, estatísticos ou científicos, desde que cumpridas determinadas medidas técnicas e organizativas adequadas (com respeito pelo princípio da minimização dos dados e podendo incluir a pseudonimização) 	<ul style="list-style-type: none"> - Prazos legais obrigatórios, em concreto, os documentos comprovativos de identificação, bem como quaisquer outros documentos de registo das operações, que permitam a sua reconstituição, devem ser conservados por um período de 7 anos a contar da sua execução, ainda que a relação de negócio já tenha terminado 	

Dimensão	RGPD	BC/FT	Sigilo Bancário
Periodicidade de atualização da documentação	<ul style="list-style-type: none"> - Sempre que haja conhecimento do termo do período de validade dos documentos de identificação - Os clausulados contratuais devem prever expressamente a obrigação de o cliente comunicar às entidades financeiras quaisquer alterações verificadas nos elementos de identificação ou noutros elementos de informação disponibilizados no início ou no decurso da relação de negócio 	<ul style="list-style-type: none"> - Cada entidade obrigada define a periodicidade de atualização da informação, tendo em conta o grau de risco, variando os intervalos temporais na ordem inversa do grau de risco identificado, não devendo ser superior a 5 anos a periodicidade de atualização da informação referente a clientes de baixo risco 	-
Portabilidade dos dados	<ul style="list-style-type: none"> - Direito geral à portabilidade dos dados para as situações em que o tratamento de dados pessoais não se baseia no consentimento ou num contrato 	<ul style="list-style-type: none"> - Não existe qualquer obrigação das instituições financeiras de responder a um pedido de portabilidade dos dados 	-
Partilha de dados	<ul style="list-style-type: none"> - BdP: central de responsabilidade de crédito e base de dados de contas do sistema financeiro - Autoridade Tributária e Aduaneira - CMVM - Autoridades judiciais intervenientes em processos judiciais para exercício ou defesa de um direito - Outras instituições de crédito e de serviços financeiros (<i>Swift</i>) e fornecedores de serviços de pagamentos (<i>Mastercard, Visa</i>) 	<ul style="list-style-type: none"> - BdP: central de responsabilidade de crédito e base de dados de contas do sistema financeiro - Autoridade Tributária e Aduaneira, Departamento Central de Investigação e Ação Penal (DCIAP), Unidade de Informação Financeira e demais autoridades judiciais, policiais e setoriais 	<ul style="list-style-type: none"> - O sigilo bancário perdura após o fim da relação comercial ou da cessação de funções - São exceções previstas ao sigilo bancário, a suspeita de BC/FT e as comunicações ao BdP, entre outras prevista na lei penal ou processual penal
Violação de dados	<ul style="list-style-type: none"> - Todo e qualquer forma de tratamento de dados que não esteja previsto no RGPD e na Lei não é considerada lícita, sendo exemplos de violação a divulgação accidental de informação de clientes durante conversa informal, a entrega de cheques de um cliente a um outro cliente ou o envio de correspondência para morada incorreta (não alterada pelo cliente), fazendo menção à falta de atualização da mesma 	<ul style="list-style-type: none"> - Não constitui violação o tratamento de dados pessoais necessários ao cumprimento dos deveres preventivos de BC/FT, sendo esta a sua exclusiva finalidade e não podendo ser posteriormente tratados para quaisquer outros fins 	<ul style="list-style-type: none"> - A comunicação às autoridades competentes é uma obrigação legal e não constitui violação dos limites à divulgação de informação, impostas por via legal ou contratual, e não implica qualquer tipo de responsabilidades para o Banco ou para os colaboradores

Dimensão	RGPD	BC/FT	Sigilo Bancário
O que fazer em caso de impossibilidade de comprovação de dados ou de incidente de violação	<ul style="list-style-type: none"> - Dever de recusa que se concretiza por exemplo na recusa de abertura de conta, inibição de movimentação de fundos ou outras transações ocasionais e termo da relação de negócio 	<ul style="list-style-type: none"> - Dever de recusa e de abstenção, traduzido na não aceitação de relações de negócio ou transações, por insuficiência de elementos identificativos e os respetivos meios comprovativos para identificação da identidade do cliente, do seu representante e do Beneficiário Efetivo - Termo da relação de negócio a definir pela área responsável pelas matérias de prevenção BC/FT 	<ul style="list-style-type: none"> - O motivo de abstenção ou recusa não deve ser transmitido aos clientes no caso de BC/FT
Penalizações	<ul style="list-style-type: none"> - Contraordenações graves (coimas de €2.500 a €10.000 000 ou 2% do volume de negócios anual, a nível mundial, se o valor for mais elevado, se grande empresa) e (coimas de €1.000 a €1.000 000 ou 2% do volume de negócios anual, a nível mundial, se o valor for mais elevado, se PME) - Contraordenações muito graves (coimas de €5.000 a €20.000 000 ou 4% do volume de negócios anual, a nível mundial, se for o valor mais elevado, para grandes empresas) e (coimas de €2.000 a 2. 000 000 ou 4% do volume de negócios anual, a nível mundial, se for o valor mais elevado, tratando-se de PME) - Coimas de €1.000 a €500.000, no caso de pessoas singulares - Repreensão, suspensão do tratamento de dados, direito a indemnização aos titulares dos dados por danos morais 	<ul style="list-style-type: none"> - Praticada no âmbito da atividade de uma instituição de crédito ou instituição financeira, de €50.000 a €5.000.000 se pessoa coletiva, ou entidade equiparada a pessoa coletiva e de €25.000 a €5.000.000 se pessoa singular - Praticada no âmbito da atividade de outra entidade financeira, de €25.000 a €2.500.000 se pessoa coletiva ou entidade equiparada a pessoa coletiva e de €12.500 a €2.500.000 se pessoa singular 	<ul style="list-style-type: none"> - Pena de prisão até 1 ano ou com pena de multa até 240 dias e responsabilidade disciplinar

Fonte: Elaboração própria.

O quadro anterior tem como objetivo permitir uma mais fácil e mais intuitiva comparação das perspectivas de análise, variáveis e dados associados a cada um dos referenciais, para, *a posteriori* e através do nosso estudo empírico, perceber como é que se podem compatibilizar de forma mais eficiente os três normativos. No fundo, e por outras palavras, pretendemos perceber como maximizar a eficiência na operacionalização simultânea dos três referenciais.

2.6 Síntese

Cada uma das dimensões aqui abordadas pode acarretar diferenças nos dados a tratar, fluxos de trabalho, prazos, entre outros. Assim, a geração de informação, que se pretende ágil, na lógica de potenciação da eficiência, pode não ser tarefa fácil.

Neste capítulo de revisão de literatura, destacaram-se três perspectivas fundamentais, concretamente:

- Perspetiva legal, onde se enumeraram os elementos preponderantes de cada um dos três referenciais legais;
- Perspetiva da estrutura de supervisão, onde se enumeraram as diferentes entidades envolvidas e papéis a desempenhar;
- Perspetiva gestionária, onde se sinalizou o papel da informação e dos sistemas de informação, bem como a sua relação com a eficiência de processos de negócio.

A razão para a consideração destas perspetivas aqui, na revisão de literatura, decorre da sua relação intrínseca, resulta do facto de serem indissociáveis e de se poderem comprometer mutuamente. Com isto aclarou-se o facto de, por um lado, ser necessário cumprir os normativos legais, por outro, nem sempre ser fácil a operacionalização do cumprimento, quando em presença de contradições ou perante análises discricionárias.

Após análise dos normativos que as entidades bancárias têm obrigação legal de cumprir, sob pena de lhes serem aplicadas sanções que vão muito além das coimas, e onde se inclui também o risco reputacional, verificou-se que existem informações e documentos de suporte comuns e outros diferenciados. Tentar-se-á perceber no estudo empírico desta investigação se os fluxos de trabalho e sistemas de recolha e armazenamento de dados estão preparados para responder às exigências do regulador, mantendo a ótica da eficiência, e tentaremos igualmente aferir possíveis entraves à interoperabilidade, principalmente organizacional e técnica. Percebe-se que o espírito do legislador é muito diferente em cada um dos referenciais, pois se no RGPD a tónica recai na proteção das pessoas, enquanto detentoras de direitos fundamentais que devem ser protegidos perante entidades que podem atentar contra a sua segurança e privacidade, já a legislação relativa à prevenção do BC/FT o bem a proteger é público e não privado. Aqui o objetivo é a paz pública e a realização da justiça. Em conclusão,

e analisados que estão isoladamente os três referenciais, iremos indagar da importância da especificação dos processos de tratamento de dados, da sua recolha e geração de informação, tempestividade e do reporte às autoridades competentes.

A entrada em vigor do RGPD, tal como afirma Teves (2019, p. 144) “implica, forçosamente, novos deveres para os responsáveis pelo tratamento e subcontratantes. Tal significa que as entidades processadoras de dados pessoais devem dissecar as suas práticas em matéria de proteção de dados pessoais, de modo a garantir *compliance* com o RGPD e adaptação a um quadro legal mais rígido”. Pretende-se, desta forma, resumir a operacionalização necessária ao cumprimento da legislação, não só em termos de RGPD, mas também de BC/FT exclusivamente no âmbito da atividade bancária.

As entidades obrigadas ao cumprimento dos deveres preventivos de BC/FT vão muito além das entidades financeiras, onde se incluem as instituições de crédito. Apenas a título de exemplo, aqui se incluem as entidades pagadoras de prémios de apostas e lotarias, auditores, contabilistas certificados, advogados, solicitadores e notários, entre outros. A Lei n.º 58/2020, de 31 de agosto, impõe assim a um leque de instituições, financeiras, ou não, atividades e profissões, um conjunto de obrigações destinadas a assegurar a prevenção de BC/FT, e elenca nos artigos 11.º e seguintes uma série de deveres preventivos gerais, de onde se destacam os deveres de comunicação, abstenção e colaboração.

No que à proteção de dados diz respeito, a CNPD é a autoridade de controlo, incumbindo-lhe a garantia e fiscalização do cumprimento da lei, sendo o BdP a entidade com competências de supervisão preventiva do BC/FT do setor financeiro e com competência de supervisão das instituições de crédito, de acordo com a sua Lei Orgânica e o RGICSF.

Os três regimes aplicam-se, sem exceção, a todos os colaboradores bancários, mas existem, nos termos da lei responsabilidades internas específicas principalmente relativamente ao RGPD que recomenda a criação da figura do DPO, que assume a responsabilidade na aplicação estratégica da proteção de dados e conformidade com o RGPD.

O DPO deve conciliar em si conhecimentos das áreas tecnológica, gestão e legal e ter idealmente competência de infraestruturas de tecnologias de informação e coordenação de auditorias SI, apoiado por equipa multidisciplinar que reúna igualmente competências nas mais diversas áreas: financeira, recursos humanos, tecnológica, marketing, arquivo, entre outras (Portal do DPO, 2022).

Os bancos procedem à recolha e tratamento de dados dos clientes particulares, necessários ao estabelecimento das relações comerciais, e asseguram o seu tratamento no âmbito do RGPD e demais legislação aplicável, bem como o dever de confidencialidade a que estão sujeitos, de acordo com o RGICSF.

Assim, e entre as finalidades mais comuns para recolha de dados temos:

- Gestão de relações contratuais e pré-contratuais, nomeadamente a abertura de conta ou

- concessão de crédito;
- Avaliação comercial e de risco de operações de crédito;
- Definição de perfis para oferta de produtos e serviços bancários e financeiros;
- Ações de *marketing*;
- Ações de recuperação de crédito ou intervenção em processos de insolvência;
- Adoção de meios e procedimentos de segurança de pessoas e bens que impliquem recolha de imagem;
- Cessão de créditos;
- Utilização de *cookies*;
- Gestão de reclamações;
- Gravação de chamadas com finalidade de prova de transações ou ao cumprimento de obrigações legais;
- Tratamento e prestação de informação obrigatória e resposta a pedido das entidades reguladoras e pedidos de autoridades públicas;
- Cumprimentos de obrigações regulatórias relacionadas com prevenção e controlo de fraude, BC/FT e obrigações em matérias fiscais. (bancobpi.pt/regulamento-geral-protecao-dados, 2022).

Esta revisão de literatura assume particular utilidade face às questões e objetivos de investigação que inicialmente se enumeraram nesta dissertação. A partir dela foi possível descrever os normativos e, principalmente, sinalizar elementos potencialmente críticos na sua operacionalização, com particular destaque para as tarefas bancárias identificadas. Tenha-se em conta que esses elementos críticos focam os dois principais elementos deste trabalho, a saber:

- A eficiência na compatibilização dos três referenciais legais;
- A mitigação, ou não, da discricionariedade, indissociável da eventual verificação empírica da existência de diferenças entre grupos.

Terminada a revisão de literatura o capítulo seguinte apresenta o método e as técnicas que suportaram o estudo empírico.

3. Método

O presente capítulo fará o enquadramento do método de investigação, sendo que o método de investigação expressa o caminho seguido, face aos objetivos e questões de investigação assumidas (Luc Van Campenhoudt & Marquet, 2019). Apresentará também o nosso desenho da investigação baseado no estudo de caso de tipologia mista como estratégia de investigação, as técnicas de recolha e tratamento de dados, e as técnicas de análise desses dados.

Podemos definir método, como o fazem Marconi e Lakatos (2003), como um conjunto de atividades sistemáticas e racionais que visam produzir conhecimentos válidos e verdadeiros com maior segurança e economia, como uma definição clara do caminho a seguir e que permita a deteção de erros. Já Freixo (2011, p. 280) define método como “o processo de aquisição de conhecimentos, recorrendo a procedimentos reconhecidos de colheita, classificação, análise e de interpretação de dados”.

Assim, o método permite que o conhecimento seja considerado científico, e por isso diferente do conhecimento popular, filosófico ou religioso. O conhecimento científico é caracterizado, segundo Assis (2018), em oposição aos outros tipos de conhecimento, como real, contingente, sistemático, verificável, falível e aproximadamente exato. No mesmo sentido, Kerlinger (1979) refere-se ao desenvolvimento da ciência pela necessidade de um método de conhecimento e compreensão mais seguro e digno de confiança do que os métodos relativamente desprovidos de controle. O mesmo autor refere ainda a objetividade e abstração como características indispensáveis e inseparáveis da investigação científica, apelando à evidência empírica e ao corte com as crenças e com a maneira tradicional de olhar o mundo.

É também de referir, conforme Eco (2007), citado por Santos & Lima (2019) que são necessárias algumas condições para que uma investigação tenha carácter científico, a saber: possuir um objeto reconhecível, definido e identificável pelos outros, analisar o objeto segundo uma perspetiva original, ter utilidade para os outros e fornecer elementos para a confirmação ou rejeição das questões de investigação, facultando elementos para que outros possam continuar a investigar, seja para confirmar ou para refutar o argumento. Santos e Lima (2019, p. 12) apontam ainda como vantagens do método científico, e que esperamos ter conseguido alcançar, “a sistematização dos dados, a credibilidade dos resultados e a aceitabilidade pela comunidade científica”.

O método não se dissocia ainda da ontologia e da epistemologia. Assim, a presente investigação assume aqui um posicionamento relativista, no domínio da ontologia, interpretativista no que respeita à epistemologia e, finalmente, recorre a uma metodologia mista, baseada num estudo de caso (Khazanchi & Munkvold, 2002).

O recurso ao estudo de caso como estratégia de investigação, que assumiu uma abordagem mista, é, desde logo, resultado da complexidade dos fenómenos objeto de estudo e da impossibilidade de os isolar. Utilizaram-se, para suportar o estudo de caso, e como técnicas de recolha de dados, a observação, a análise documental, a entrevista e o questionário. Já como técnicas de análise de dados recorreu-se a

análise categorial de conteúdo e a análise estatística.

De seguida apresentaremos algumas características que sustentaram a escolha de uma abordagem de investigação mista, qualitativa e quantitativa, prática usual em mestrados da área onde este se enquadra, com particular destaque para os que apresentem questões no domínio da contabilidade de gestão, da otimização de processos, entre outros.

3.1 O *continuum* da abordagem qualitativa à quantitativa

Uma investigação qualitativa, segundo Dezin e Lincon (2000), citados por Seabra (2010), traduz uma investigação que atravessa disciplinas, campos de estudo e temas, e que tem sofrido inúmeras transformações no âmbito epistemológico e metodológico. Desta feita, implica uma ênfase nas qualidades das entidades, nos processos e nos significados, valorizando a qualidade socialmente construída da realidade. É, por isso, extremamente útil nas ciências humanas, exatamente onde este trabalho se insere.

Já Serapioni (2000) identifica como características dos métodos qualitativos a análise do comportamento humano do ponto de vista do ator, a observação naturalista, a subjetividade, a orientação para a descoberta e para o processo, o carácter exploratório, descritivo e indutivo e a não generalização. Seabra (2010) acrescenta que a metodologia qualitativa pressupõe, mais do que resultados de medida, uma análise em profundidade, de significados e atributos dos fenómenos.

Ainda na defesa da utilização método qualitativo Neves (1996) refere que este método é propício na falta de exploração de um certo tema na literatura, fase ao carácter descritivo da investigação a realizar ou à intenção de compreender um fenómeno complexo na sua totalidade. Ora tentar compreender um fenómeno complexo na sua totalidade foi uma preocupação permanente, e desde o primeiro momento assumida, por esta investigação. Acrescenta ainda o autor que compreender e interpretar fenómenos, a partir dos seus significantes e contexto são tarefas presentes na produção de conhecimento e revela a vantagem de utilização de métodos que auxiliam a ter uma visão mais abrangente dos problemas, que supõem contacto direto com o objeto de análise e fornecem um enfoque diferenciado para a compreensão da realidade. Também Minayo, Deslandes e Gomes (2007) enfatizam que a pesquisa qualitativa procura compreender e interpretar a realidade e trabalha com um conjunto de fenómenos humanos gerados socialmente como os significados, motivos, aspirações, crenças, valores e atitudes.

Quanto a Marques (2005) refere que esta metodologia permite aceder e compreender a complexidade e diversidade da realidade em estudo, no seu contexto e enriquecida pelos significados atribuídos pelos participantes, conferindo-lhe elevada validade interna. Mas, acrescenta também algumas limitações que lhe são atribuídas como a impossibilidade de generalização dos resultados, podendo apenas traçar analogias e procurar padrões e temas comuns. As limitações são também reforçadas por Serapioni (2000), que aponta a imprecisão dos dados que exigem a permanente

referenciação aos dados brutos, a extensão dos estudos que são frequentemente limitados a casos isolados ou pequenas amostras, a dificuldade de legitimação e aceitação nalguns setores de investigação e por fim, o facto de ser questionada por muitos defensores do paradigma quantitativo.

O quadro seguinte resume as principais vantagens e desvantagens da metodologia qualitativa:

Quadro 4: Vantagens e desvantagens da metodologia qualitativa

Vantagens	Desvantagens
– Elevada validade interna	– Imprecisão dos dados
– Acesso à complexidade	– Dificil aceitação por alguns setores da comunidade científica
– Contextualização	– Limitações técnicas: pela sua própria natureza presta-se à compreensão profunda de realidades restritas, não pretende generalizar resultados
– Riqueza de significados	– Lida com pequenas amostras
– Acesso ao mundo experiencial dos participantes	
– Descrição	
– Interpretação	
– Subjetividade – investigador como instrumento da investigação	

Fonte: Seabra (2010).

Já a abordagem quantitativa apresenta igualmente vantagens e desvantagens. Assim, relativamente à investigação quantitativa Freixo (2011) refere-a como um processo sistemático de colheita de dados observáveis e quantificáveis, baseada na observação de factos objetivos, fenómenos e acontecimentos que existem independentemente do investigador. Já para Reis (2010) o método quantitativo considera que todos os dados são quantificáveis e podem ser traduzidos em números, opiniões e informações, que através de métodos estatísticos os classifica e os analisa. Também para Almeida e Freire (2000) a investigação quantitativa visa compreender, explicar, prever e controlar fenómenos, através da quantificação das medidas e objetividade de procedimentos.

As características fundamentais, para Serapioni (2000), são a orientação para a quantificação e a causa dos fenómenos, a ausência de preocupação com a subjetividade, a utilização de métodos controlados, a objetividade através de um distanciamento em relação aos dados, a orientação para a verificação, a natureza hipotético-dedutiva, a orientação para os resultados, a replicabilidade e possibilidade de generalização, e a assunção da realidade como estática, apresentando, portanto, uma forte validade externa. No entanto, a falta de validade interna é precisamente uma das críticas apresentada pelo mesmo autor, na medida em que não atende frequentemente à perspetiva do sujeito, gerando ambiguidade quanto àquilo que é medido. Tenha-se em conta que este ponto é importante para

deixar bem claro que vantagens e inconvenientes todas as abordagens as têm. E também por isso o quadro seguinte resume as principais vantagens e desvantagens da abordagem quantitativa.

Quadro 5: Vantagens e desvantagens da abordagem quantitativa

Vantagens	Desvantagens
<ul style="list-style-type: none"> - Elevada validade externa - Replicabilidade - Possibilidade de generalização - Recorre a procedimentos que facilitam a sua aceitação pelos pares - Capaz de abranger maior número de casos 	<ul style="list-style-type: none"> - Baixa validade interna - Não atende à perspectiva do sujeito - Não tem em linha de conta a subjetividade do investigador

Fonte: Seabra, (2010).

Relativamente à nossa abordagem quantitativa o instrumento de investigação considerado mais adequado foi a investigação por questionário, na medida em que, segundo Fortin M. F. (2009), traduz os objetivos do estudo com variáveis mensuráveis e ajuda a organizar, normalizar e controlar os dados. Ainda para Freixo (2011) o questionário é um instrumento de medida que permite, eventualmente, confirmar ou infirmar as hipóteses de investigação.

Resulta do que se descreveu que nesta dissertação combinaram-se instrumentos de natureza qualitativa com instrumentos de natureza quantitativa, seguindo-se uma abordagem mista. Serapioni (2000) aponta resultados positivos na sua combinação, demonstrados na investigação no terreno e o grau de validade interna e externa que se pode obter das forças e das limitações de cada uma das abordagens. Seguimos então aqui a mesma posição de Seabra (2010, p. 150) para quem “ao longo de um design de investigação, podem intercalar-se momentos de investigação quantitativa, que por sua vez podem levantar questões mais bem respondidas por um estudo qualitativo ou vice-versa: na prática, os dois tipos de estudo podem matizar a compreensão da realidade que obtemos”. Neste mesmo sentido, também Huberman e Miles, (2003) referem que a utilização destas duas abordagens metodológicas não representa uma dicotomia, mas sim uma complementaridade, sugerem mesmo a alternância entre as duas, onde as entrevistas exploratórias conduzem a instrumentos quantitativos e a análise quantitativa é seguida por trabalho qualitativo.

Julgamos assim compreender melhor o fenómeno em estudo, o como e o porquê, inerentes à estratégia de estudo de caso que foi aqui assumida.

Acresce que o método, a estratégia de estudo de caso, bem como as técnicas de recolha e de

tratamento de dados encontram-se aqui integralmente alinhadas indo totalmente ao encontro do argumento de que “para além das questões que se relacionam com as estratégias, as metodologias e as técnicas de recolha e tratamento de dados, em cada trabalho científico, é essencial que o investigador se posicione explicitamente durante a pesquisa em relação às questões ontológicas e epistemológicas” (Santos & Lima, 2019, p. 4). Aqui o posicionamento ontológico relativista e interpretativista admitem uma abordagem mista, ainda que a dimensão qualitativa seja relevada.

Definidos que estão os posicionamentos ontológico, epistemológico e metodológico, faremos de seguida a explicação da escolha do estudo de caso como estratégia de investigação.

3.2 O estudo de caso como estratégia de investigação

Freitas e Jabbour (2017) referem a investigação científica como algo inovador e baseada em estratégias e métodos de pesquisa universalmente aceites. Segundo Neves (1996) são várias as formas de avançar no conhecimento científico de um fenómeno e refere que as diferentes maneiras de conceber e lidar com o mundo geram formas distintas de perceber e interpretar significados e sentidos do objeto investigado, que se complementam.

Strauss e Corbin (2002) alertam para a necessidade de alinhar a escolha do método de investigação com as questões de investigação. E também para Yin (2004) a identificação do tipo de questão de investigação é essencial para a definição da estratégia mais adequada a escolher. Ora uma das questões de investigação desta dissertação aponta imediatamente para uma abordagem de tipo qualitativo, tal como referido por Major e Vieira (2009), por ser aquela que se foca na forma como os fenómenos sociais são interpretados, percebidos, gerados e compostos.

Segundo Yin (2004) as questões de investigação permitem apontar para diferentes tipos de intencionalidade e daí surgindo diferentes estudos de caso que podem ser explicativos, descritivos ou exploratórios. Seguindo a terminologia do autor podemos definir a nossa dissertação como um estudo exploratório por permitir uma maior familiaridade do investigador com o tema, permitir a recolha de informações através da pesquisa bibliográfica, entrevistas e questionários e também na medida em que pretendemos encontrar ideias e soluções na ótica da eficiência das instituições. A nossa investigação assume também carácter descritivo na medida em que como investigadores descrevemos e observámos os fenómenos como um todo. Um estudo de caso traduz “um inquérito empírico que investiga um fenómeno contemporâneo dentro do seu conceito de vida real, especialmente quando as fronteiras entre fenómeno e contexto não são claramente evidentes” (Yin, 1994, p. 24). Assume particular importância nas respostas a questões de investigação iniciadas pelas palavras “como” e “porquê” e se está em presença de um conjunto de eventos contemporâneos. Trata-se de uma investigação empírica que permite o estudo de um fenómeno contemporâneo dentro do seu contexto de vida real. Refere ainda constituir uma estratégia de pesquisa que não pode ser classificada *a priori* como qualitativa nem

quantitativa, por excelência, mas que está interessada no fenómeno.

O estudo de caso requer múltiplas fontes para explorar, descrever e explicar um fenómeno no seu contexto e pode recorrer a técnicas qualitativas e quantitativas, pelo que podemos classificar o nosso estudo como misto. Trata-se, segundo Coutinho (2014), de uma referência metodológica com maiores potencialidades para o cientista social, tendo como principal característica o estudo intensivo de uma entidade concreta.

Já Fortin, Côté e Filion (2009) referem-se a esta estratégia como a realização de um estudo detalhado e integral de um fenómeno ligado a uma pessoa ou grupo e enquadram o estudo de caso nas investigações não experimentais, qualificadas como estudos descritivos realizados no meio natural e sem a utilização de variáveis independentes. Na mesma direção apontam Selltitz, Jahoda e Deutsch (1974) ao dividirem as pesquisas sociais em estudos descritivos, explicativos e exploratórios. A estratégia de recurso a estudo de caso expõe assim “características de determinada população ou de determinado fenómeno... Pode também estabelecer correlações entre variáveis e definir a sua natureza. Não tem compromisso em explicar os fenómenos que descrevem embora sirva de base para tal explicação” (Vergara, 2004, p. 47) citado por Freitas & Jabbour (2017).

Esta dissertação releva a interpretação do fenómeno objeto de estudo, tal como refere Godoy (1995), envolvendo pessoas, lugares e processos interativos, bem como o contacto direto do investigador com a situação estudada, procurando compreender os fenómenos segundo a perspetiva dos participantes, partindo de questões amplas, que se vão definindo à medida do desenvolvimento do estudo, evidenciando o significado que os participantes atribuem. Conforme sinalizado por Liebbscher (1998) a sequência de procedimento é viável, na medida em que o fenómeno é complexo, de natureza social e de difícil quantificação. Resulta do que se indicou que consideramos que o estudo de caso é a estratégia que mais se adequa à finalidade e recursos da nossa investigação, visto que a análise da eficiência só pode ser observada em contexto real, centrado na aplicabilidade, sendo que para Major e Vieira (2009) o estudo de caso é comumente utilizado nos domínios da contabilidade. Também estes autores referem que os estudos de caso podem ser simples ou múltiplos, de natureza quantitativa ou qualitativa, referindo que esta última tenta explicar a forma como os fenómenos sociais são interpretados, percebidos, gerados e compostos. Neste âmbito o investigador observa, descreve, interpreta o meio e o fenómeno tal como se apresenta, sem o procurar controlar (Fortin, 2003).

Quanto a fronteiras, o recurso a estudo de caso incide, em regra, na totalidade e não numa amostra. Assim, ainda que se trate de um estudo de caso único, no Banco BPI, o estudo não considera a totalidade do banco. Na impossibilidade de englobar toda a instituição bancária, que tem milhares de colaboradores e áreas que não lidam diretamente com as temáticas em análise, foi necessário delimitar o nosso estudo de caso a todos os colaboradores da área comercial do Alentejo (SI9 Alentejo), Direção de *Compliance*, Direção de Auditoria Interna, Financeiras, Participadas e *Compliance*, Direção Jurídica, Inovação e

Privacidade e Direção de Marketing, Particulares e Negócio Habitação (DMPN), num universo de 189 colaboradores.

Por último, quanto à aplicação de método e técnicas similares, no domínio da contabilidade e finanças, resta-nos referir aqui o esquema proposto por Lima, Antunes, Mendonça e Peleias (2012). Estes autores identificam algumas temáticas em que o estudo de caso em contabilidade pode ser utilizado, como por exemplo, estudos sobre a realidade das organizações, novos modelos de gestão ou implementação de sistemas. Tendo em conta as várias definições dadas pela literatura, nomeadamente por Yin (2004), extraem daí um conjunto de características, todas aplicadas à vasta área de contabilidade e finanças. Estes autores referem que (Lima, Antunes, Mendonça & Peleias, 2012, p. 133):

- a) É uma estratégia de investigação apropriada para ciências sociais e, particularmente, para as ciências sociais aplicadas;
- b) É uma estratégia utilizada para as pesquisas de acontecimentos contemporâneos em condições contextuais;
- c) Deve ser precedido pela elaboração de um protocolo que defina os procedimentos e as regras gerais, possibilitando ao pesquisador conduzir o seu trabalho com êxito;
- d) Está embasado em uma lógica de planeamento, evitando a sua condução por comprometimentos ideológicos;
- e) Há convergência de informação e troca de experiências sobre o fenómeno;
- f) As inferências são sempre feitas tendo por base um teste empírico;
- g) O estudo sobre o fenómeno deve ser profundo e deve exaurir as possibilidades do que foi delimitado;
- h) Abrange a lógica do planeamento, as técnicas de coleta de dados e as abordagens específicas para a análise dos achados.

Fundamentado o recurso ao estudo de caso como estratégia de investigação, seguidamente apresenta-se o desenho de investigação e aclaram-se as técnicas utilizadas.

3.3 Desenho de investigação

Um desenho de investigação é um plano, um guia de trabalho. Nas palavras de Yin (1994) é a lógica que liga os dados a serem recolhidos e as conclusões a serem retiradas, atendendo às questões iniciais da investigação.

A figura seguinte representa as fases seguidas no desenvolvimento do estudo de caso como estratégia de investigação. Note-se, conforme apontado por Gil (2009), que não há consenso entre os autores quantos às etapas a serem seguidas ao longo de um estudo de caso, contudo, e tendo por base as

referências de Yin (2004) e Stake (2006), construímos, com adaptações, o esquema a seguinte.

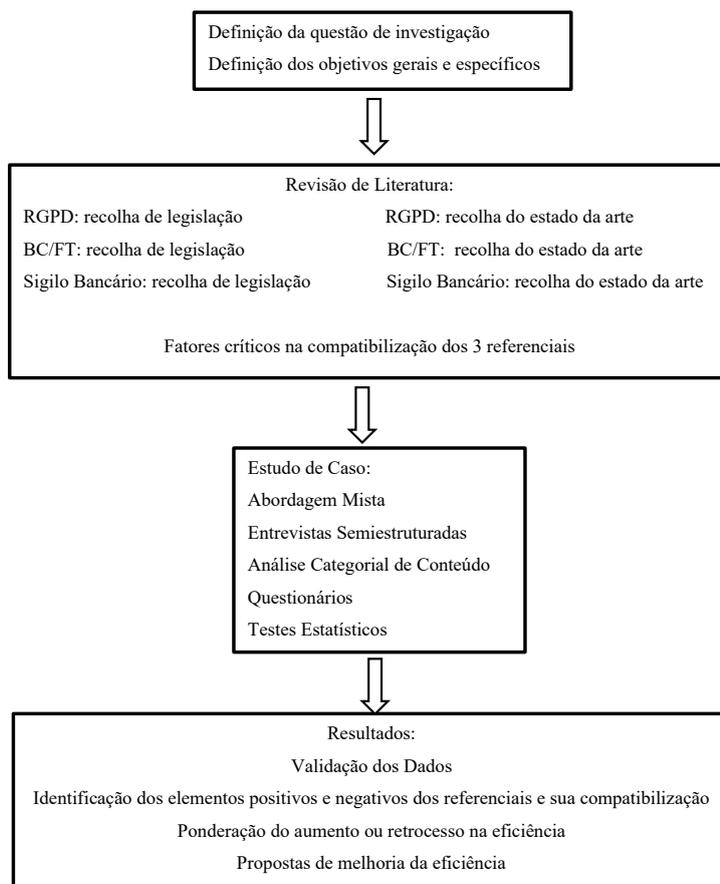
Figura 2: Fases do estudo de caso



Fonte: Adaptado de Lima e Pacheco (2006), Yin (2004) e Stake (2006).

Um desenho de investigação apresenta assim uma combinação de elementos orientados para tornar possível a resposta às questões de investigação.

Figura 3: Desenho de investigação



Fonte: Elaboração própria.

Apresentado o desenho de investigação assumido, os pontos seguintes apresentam e ponderam as técnicas utilizadas.

3.4 Técnicas de recolha de dados

Como sugerido por Yin (2004), para a realização de um estudo de caso devem ser utilizados vários procedimentos e o maior número de fontes. São indicadas pelo autor, como principais, a documentação, os registos de arquivos, as entrevistas, a observação direta, a observação participativa e os artefactos físicos, referindo ainda que a obtenção de um estudo de caso robusto requer a utilização de múltiplas fontes de prova, criação de uma base de dados e manutenção de registos.

No âmbito da investigação documental importa referir que “o uso da informação disponível, qualquer que seja o seu carácter documental (numérico ou não numérico, elaborado ou em bruto) é praticamente indispensável em investigação social” (Moreira, 2007, p. 153). O mesmo autor define documento como o material informativo sobre determinado fenómeno que existe com independência da ação do investigador, aqui se incluindo livros, legislação e documentos institucionais, entre outros. Erlandson (1993) citado por Moreira (2007) refere ainda que os documentos incluem praticamente

qualquer material e dados disponíveis antes e durante a investigação e podem ser utilizados da mesma forma que os dados resultantes de observações ou entrevistas.

O estudo do estado da arte foi assim o ponto de partida para a nossa dissertação, e tal como referido por Martins (2008), utilizámos um referencial teórico de base às questões, sendo reunidas diversas informações. Como também sugerido por Yin (1994) a revisão de literatura é essencial à posterior definição dos dados a recolher. Foi assim elaborada uma pesquisa bibliográfica com o levantamento do estado da arte publicado, nomeadamente em relação aos conceitos, enquadramento legal atual e evolução histórica dos diferentes referenciais em análise. É certo que os autores desenvolvem exaustivamente qualquer uma destas matérias – RGPD, sigilo bancário e BC/FT, contudo não se encontrou nenhuma bibliografia publicada que relacionasse os três institutos de forma a encontrar os seus pontos comuns, ou contraditórios. Aliás, esse é um atributo distintivo e inovador do presente trabalho.

Realizámos pesquisa documental, em que foram analisados documentos de âmbito interno e a também de âmbito público, no site da instituição bancária, pesquisa bibliográfica, como já referido, realizámos entrevistas e, por fim, formulámos questionários, na vertente empírica da investigação. Como refere Fortin (2009) a característica fundamental da investigação qualitativa é a flexibilidade dos métodos de colheita de dados e análise, permitindo o desvendar de novos fenómenos ou o seu aprofundamento. A consulta de textos e documentos é uma das formas de recolha de dados utilizada na investigação qualitativa, que se utiliza frequentemente para confirmar ou clarificar informação obtida de outras fontes, como as entrevistas ou observação (Major & Vieira, 2009). Consultámos essencialmente legislação, bem como o site do banco BPI, e de outros bancos portugueses, onde consta informação pública, e analisámos documentos internos, muito deles sigilosos, e a estrutura organizacional da instituição, através da colaboração da entidade bancária, e tendo em conta os objetivos da investigação. Independentemente disso, o sigilo dos documentos internos foi cuidado.

Quanto à observação consideramos que foi realizada uma observação participante (Yin, 2004) e (Quaresma, 2005), pois a investigadora trabalha na instituição bancária e, para além das tarefas que a própria desempenha e que se relacionam com a temáticas em causa, teve a oportunidade de observar o desempenho de outros colegas. Ainda assim, e apesar de conseguir ter noção de algumas das atividades desenvolvidas na entidade, fluxos de trabalho, recursos e dificuldades existentes, trata-se de uma noção que se restringe apenas a um dos setores do banco, a banca de retalho e a uma única função.

Desta forma, tornou-se essencial o recurso à técnica de entrevista. Mayer (1974), citado por Vicente, Reis e Ferrão (2001), define a entrevista pessoal como uma conversação face a face entre duas pessoas, iniciada e dirigida pelo entrevistador com o propósito particular de obter informação relevante, e no sentido de concretizar os objetivos do estudo. Já Coutinho (2014) considera que a entrevista é uma poderosa técnica de recolha de dados na medida em a interação entre entrevistador e entrevistado

permite obter informação que não seria possível obter através de questionário e esclarecimentos adicionais sempre que a resposta não é elucidativa. Adicionalmente, Guazi (2021), citando Gil (2008) assinala que a entrevista é uma técnica particularmente útil para investigar o comportamento e a subjetividade humana, e permite a coleta de dados a respeito do que as pessoas fazem, como o fazem e os motivos pelos quais o fazem.

Major e Vieira (2009) referem ainda a frequente utilização de entrevistas, normalmente semiestruturadas e de resposta aberta, na investigação em contabilidade de gestão, tendo sido esta a nossa escolha que, somada à consulta de documentos e à observação direta, permitiu a triangulação. A triangulação de dados, fruto da utilização de várias técnicas de recolha de dados, é apontada por Nunes M. G. (2020) como forma de afastamento de algumas críticas à insuficiência de dados, quando usada esta estratégia de investigação.

As instituições bancárias são organizações complexas, com muitos colaboradores alocados a diferentes áreas e por isso com tarefas e objetivos múltiplos. Na impossibilidade de entrevistar todos os colaboradores e todos os diferentes setores, foi necessário proceder à escolha de uma amostra. A ideia de amostra surge quando os recursos disponíveis não são suficientes para analisar todas as unidades da população, no nosso caso, todos os colaboradores (Sampaio & Lycarião, 2021). Neste mesmo sentido Fortin (2009), acrescentando, que a amostragem é feita por escolha racional e os participantes comungam das suas características, para desta forma representarem bem o fenómeno e auxiliarem na sua compreensão. Já o término das entrevistas resulta da saturação, ou seja, sempre que novas entrevistas não acrescentam elementos adicionais, comparativamente àqueles que antes foram recolhidos.

Para essa amostragem foram indicados pelo banco, a nosso pedido, colaboradores com conhecimentos e competências práticas em RGPD e BC/FT, de forma a obter um grupo o mais qualificado possível, tal como referido por Neves (1996), para os estudos qualitativos.

Vicente, Reis, & Ferrão (2001) apontam a presença física do entrevistador como o principal fator diferenciador da entrevista pessoal relativamente a outros métodos de obtenção de dados. A presença física não deixou de existir nas nossas entrevistas, apesar de todas terem sido feitas à distância, através do programa informático *Teams*. Esta opção foi tomada não só pela situação pandémica que se vivia, mas também por tão bem permitir colmatar a distância física entre os locais de trabalho da investigadora e da maior parte dos entrevistados. Cada entrevista tinha uma previsão de duração de 30 minutos cada, sendo que a mais longa teve a duração de 57 minutos. Considerámos assim ter atingido a saturação após a realização de 11 entrevistas. A entrevista semiestruturada foi suportada em guião (Anexo IV). No entanto, tendo ciente a necessidade de ter presente os conceitos de amostragem e de saturação, foi necessária a seleção de outros colaboradores para além daqueles que foram inicialmente indicados. Sobre esta matéria, refere Minayo (2017) que há necessidade de saber até que ponto uma quantidade pequena de entrevistas, a um grupo delimitado e restrito, assim como a forma intersubjetiva de atuação

do pesquisador em campo, podem ser considerados científicos. Glaser e Strauss (1967) definem saturação como o momento no trabalho de campo a partir do qual a coleta de novos dados não traria mais esclarecimentos para o objeto estudado. Não existem na literatura conclusões decisivas sobre este ponto de saturação “diferentemente dos que dizem investigações quantitativas em que refinados cálculos estatísticos estabelecem o tamanho ideal da amostra e as possibilidades de expansão dos resultados” (Minayo, 2017, p. 5).

Para a realização das entrevistas foi necessária a prévia autorização do banco, a escolha dos entrevistados, verificação da sua disponibilidade e a obtenção do seu consentimento. A autorização para recolha de gravação de áudio e imagem, ainda que esta não seja utilizada *a posteriori*, foi também essencial à transcrição, revisão e análise pela investigadora, reforçando também a fiabilidade dos dados recolhidos (Nunes M. G., 2020).

Ao serem realizadas entrevistas semiestruturadas, conforme Denzin (1970), citado por Moreira (2007), foi usada uma lista de perguntas ordenadas (para se conseguir um contexto equivalente) e redigidas (para terem o mesmo significado) por igual, para todos os entrevistados, mas de resposta livre ou aberta. Todas as perguntas foram efetuadas da mesma forma, de modo a que quando surgissem diferenças entre entrevistados estas se pudessem atribuir a variações reais de resposta e não ao instrumento.

Tentou-se assim no decorrer das nossas entrevistas explorar não só as experiências vivenciadas, mas também as interpretações e sugestões relativamente aos fenómenos em estudo. Quivy e Campenhoudt (2008) salientam a importância das entrevistas abertas para a troca de informações, em que o participante pode ser mais profundo e autêntico, não se distanciando dos objetivos da entrevista. Os mesmos autores referem ainda a entrevista semiestruturada como aquela que é dotada de maior flexibilidade, em que existem questões pré-definidas, colocadas ou não pela ordem prevista, no sentido de encaminhar a entrevista de uma forma natural para os objetivos do estudo. No mesmo sentido também Fortin (2009) se refere à entrevista semiestruturada como a que permite uma compreensão genuína, natural e autêntica do fenómeno em estudo, através da utilização de um guião que facilita a condução da entrevista.

Segundo Coutinho (2014) a ciência que se produz está intimamente relacionada com o universo social em que é construída, sendo o contexto sociocultural indissociável do investigador. Tivemos sempre em consideração aspetos éticos e a disponibilidade dos envolvidos, conforme sugerem Fortin, Côté e Fillion (2009), bem como as características pessoais capacidade e integridade referidas por Weiers (1988), citado por Vicente, Reis e Ferrão (2001), como atributos essenciais do entrevistador.

Nas nossas entrevistas seguimos os passos sugeridos por Guazi (2021), que vão desde o agradecimento pela participação até à autorização para gravação. Após a realização das mesmas procedeu-se à sua transcrição.

Considerámos assim ter conseguido entrevistar todos os setores de uma instituição bancária com relevância para a matéria em estudo, apesar de considerarmos que são matérias transversais a todos os sectores e a todos os colaboradores de um banco.

Tendo em conta as nossas questões de investigação, os objetivos definidos e a matéria apurada da análise dos dados recolhidos através das entrevistas, considerámos que o nosso estudo de caso deveria ser complementado, pelo que considerámos importante a realização de um inquérito por questionário (Anexo V), na medida em que pretendemos testar a solidez dos resultados obtidos. Esse questionário teve como preocupação poder captar as respostas de colaboradores que, podendo apresentar contributos válidos, não realizaram entrevista.

No entanto, como referido por Seabra (2010, p. 150) “questionários e entrevistas são instrumentos que os investigadores recorrem para transformar em dados a informação comunicada diretamente por uma pessoa (o sujeito). Quaresma (2005) aponta como principais vantagens do questionário a não exigência da presença do pesquisador, o facto de se atingir várias pessoas ao mesmo tempo, podendo obter um grande número de dados, permitir maior liberdade de resposta em razão do anonimato e permitir ainda obter respostas rápidas e precisas.

Para Fortin M. F. (2009), a mais-valia do questionário é permitir organizar, normalizar e controlar os dados, por forma a que as informações sejam recolhidas com rigor. Já Freixo (2011) categoriza os tipos de medidas de um questionário em objetivas e subjetivas. As objetivas relacionam-se com factos, conhecimentos, comportamentos e características dos indivíduos. Por sua vez as subjetivas relacionam-se com opiniões, atitudes, preferências, crenças, entre outros. Ainda segundo o mesmo autor e também Hill e Hill (2012) as perguntas podem ser fechadas ou abertas, sendo que naquelas os inquiridos escolhem as suas respostas consoante duas ou mais opções oferecidas e nas abertas é lhes permitido formular opiniões e comentários e fornecer pormenores, utilizando o seu próprio vocabulário.

Atendendo aos fundamentos expostos, optou-se também pela aplicação de um questionário semiestruturado, composto por questões fechadas e uma última aberta. O questionário foi previamente autorizado pela entidade e foi remetido para a área do banco que é responsável pela elaboração e difusão de questionários ao cliente interno e externo. Antes disso o questionário foi ainda sujeito a pré teste com o intuito de perceber se a linguagem era clara, se o instrumento era efetivamente percebido, sem apresentar questões dúbias.

Podemos, por esta via, aceder ao programa informático utilizado pelo Banco BPI, que remeteu o nosso questionário através de um link enviado para o *e-mail* profissional dos 189 colaboradores por nós indicados e em conformidade com a delimitação do caso de estudo, assegurando o anonimato dos respondentes. Seguidamente realizou-se o tratamento estatístico dos dados, no sentido de se encontrar resposta à questão de investigação que tentava avaliar a existência, ou não, de diferenças entre grupos.

A metodologia quantitativa seguiu assim as seguintes etapas:

- Preparação e desenho do questionário;
- Pré-teste;
- Envio e acompanhamento do questionário;
- Recolha e tratamento de dados;
- Análise dos resultados;
- Conclusões.

Para reforçar a justificação da escolha entre entrevista ou questionário Tuckman (2000) refere, em relação a este último, que requer menos custos, permite abranger um número vasto de sujeitos, as fontes de erro limitam-se ao questionário e à amostra e tem uma razoável fidelidade total. Por outro lado, acrescenta que não oferece grande possibilidade de personalizar, questionar ou aprofundar as questões com cada sujeito, tem baixa taxa de resposta, e prende-se muito com a capacidade de expressão escrita, podendo ser inadequado para algumas populações. Já Seabra (2010) argumenta, no entanto, que as vantagens referidas pelos autores são simultaneamente a sua força e a sua maior fraqueza ao não permitir a adequação das questões ao sujeito e ao contexto no decorrer do discurso. E, no mesmo sentido, Hill e Hill (2000) afirmam que a riqueza dos dados é comprometida para privilegiar a possibilidade de analisar os dados mediante análises estatísticas sofisticadas. Ora aqui, ao se combinarem instrumentos, aproveitou-se o potencial de cada um deles (Fortin M. F, 2003).

O Banco BPI tem mais de quatro mil trabalhadores, pelo que seria praticamente impossível interagir com todos os colaboradores da instituição. Tal facto suportou a decisão de redução das fronteiras do caso de estudo, tal como antes se indicou. Assim, ainda que a construção de uma amostra do universo permita a substituição do universo em análise e se assuma ser um meio de o conhecer, com razoável segurança, aqui não se procura a generalização de resultados (Pardal & Lopes, 2011).

A primeira secção do questionário pretende caracterizar os respondentes. A segunda secção visa recolher a perceção dos respondentes sobre a compatibilização operativa do RGPD com a Lei de combate ao BC/FT e com o sigilo bancário, sendo composta por quatro questões, de escala tipo *Likert*. A última secção apresentou uma questão aberta, com espaço para o respondente, livremente, explicar o porquê da sua concordância, ou não, com afirmações apresentadas.

Por forma a responder à questão de investigação “Existem diferenças entre grupos quanto à forma como percecionam a compatibilização, esforço requerido e a eficiência de aplicação do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário?” considerámos as seguintes hipóteses para esta investigação:

1. Quanto ao grau de perceção de compatibilização dos três referenciais:
 - H1.0: existe igualdade na distribuição dos grupos quanto à perceção de

compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário;

- H1.1: existem diferenças na distribuição dos grupos quanto à percepção de compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário.

2. Quanto ao reconhecimento da dificuldade de compatibilização dos três referenciais:

- H2.0: existe igualdade na distribuição dos grupos quanto ao reconhecimento da dificuldade na compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário;
- H2.1: existem diferenças na distribuição dos grupos quanto ao reconhecimento da dificuldade na compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário.

3. Já para a eficiência enunciaram-se as seguintes hipóteses:

- H3.0: existe igualdade na distribuição dos grupos quanto à eficiência na compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário;
- H3.1: existem diferenças na distribuição dos grupos quanto à eficiência na compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário.

Enquadradas as técnicas de recolha de dados, torna-se possível enunciar as diferentes técnicas de análise desses dados (Yin, 2004). O capítulo seguinte considera essa necessidade.

3.5 Técnicas de análise de dados

Após a recolha dos nossos dados necessário será proceder à sua análise para tentarmos alcançar as nossas conclusões. Como observado por Cardoso, Oliveira e Ghelli (2021) a escolha do melhor método sempre dependerá, entre outras, da natureza do objeto da pesquisa e dos objetivos da investigação. Iniciámos a análise dos nossos dados pela análise de conteúdo das entrevistas realizadas.

Para Yin (2004) a análise de dados é não só um dos aspetos menos explorados em estudos de caso, mas também o mais complicado, essencialmente porque não existem fórmulas fixas para orientação, como acontece na análise estatística. Para este autor aquela tem como objetivo a produção

de conclusões analíticas irrefutáveis através do tratamento dos dados recolhidos de uma forma justa e imparcial, sem interpretações alternativas.

Já Oliveira (2008) refere, na sua proposta de sistematização sobre a análise de conteúdo temático-categorial, que existe na literatura uma variedade de conceitos e de finalidades identificadas e coloca-a como instrumento de pesquisa com múltiplas aplicações. Chama-nos ainda a atenção para a variação dos instrumentos utilizados em função dos objetivos da pesquisa e para a necessidade de a análise de conteúdo se submeter a regras específicas sob pena de não se diferenciar de análises meramente intuitivas.

Relativamente à nossa abordagem qualitativa, não faremos, por desnecessidade, referência a outras as técnicas de análise de dados, que não a análise de conteúdo. Esta foi a opção tomada, considerando, como o fazem Cardoso, Oliveira e Ghelli (2021) que é uma excelente opção quando o objetivo é analisar dados provenientes das comunicações, na busca de compreensão dos significados e dos sentidos das mensagens, que vão além da leitura comum. Cumpre-nos assim dar nota de algumas definições da própria análise de conteúdo, que mais não é do que o tratamento da informação recolhida empiricamente.

Assim, podemos definir a análise de conteúdo como “um recurso determinante na sistematização da informação recolhida, tratando de forma metódica as informações e testemunhos que apresentam um certo grau de profundidade e de complexidade” (Quivy & Campenhoudt, 2008, p. 227).

Berelson (1952) apresentou a análise de conteúdo como uma técnica de investigação para a descrição objetiva, sistemática e quantitativa do conteúdo, definindo na sua obra, nomeadamente as suas regras e princípios de análise.

Já Campos C. J. (2004, p. 611) refere-se à análise de conteúdo como uma técnica muito utilizada na análise de dados qualitativos, “compreendida como um conjunto de técnicas de pesquisa cujo objetivo é a busca do sentido ou dos sentidos de um documento”. Quanto a Bardin (2016, p. 44), define a análise de conteúdo “como um conjunto de técnicas de análise das comunicações, que utiliza procedimentos sistemáticos e objetivos de descrição do conteúdo de mensagens”. Mas acrescenta que estes segmentos da definição são insuficientes para definir a sua especificidade e é necessário acrescentar a finalidade (implícita ou explícita). A esta intenção a autora chama “de inferência de conhecimentos relativos às condições de produção (ou, eventualmente, de receção), “que recorre a indicadores (quantitativos ou não)”. A obra de Bardin é amplamente considerada pela literatura como “um verdadeiro manual sobre a operacionalização da análise de conteúdo” (Cardoso, Oliveira, & Ghelli, 2021, p. 99). Desta forma, compreendemos que os dados nos chegam em estado bruto e é a partir daí que se inicia a análise, com os dados a serem trabalhados de forma sistemática pelo analista. Tais argumentos sustentam aqui o recurso à análise de conteúdo. Lima (2013) refere a existência, na literatura, de muitas modalidades de análise de conteúdo. Também Bardin (1977), citada por Cardoso, Oliveira e Ghelli (2021), sinaliza que

existem várias maneiras de analisar conteúdos, sendo as principais técnicas a análise categorial, análise do discurso, análise de avaliação, análise de enunciação, análise de expressão, análise das relações (co-ocorrências e estrutural). Mas é a análise categorial a que servirá de base para a análise de conteúdo aqui realizada, pois a “análise por categorias é de citar em primeiro lugar: cronologicamente é a mais antiga; na prática é a mais utilizada”, acresce o facto de ser “eficaz na condição de se aplicar a discursos diretos”, usada em significações manifestas (Bardin, 1977, p. 153).

Desta forma, a “categorização é a operação através da qual os dados (invocados ou suscitados) são classificados e reduzidos, após terem sido identificados como pertinentes” (Lima & Pacheco, 2006, p. 109), ou seja, é um procedimento que reconfigura o material ao serviço da investigação.

Bardin (2016) identifica a categorização de forma dedutiva (procedimentos fechados), com categorias criadas a partir da revisão de literatura e objetivos do trabalho e categorização de forma indutiva (procedimentos abertos), emergindo as categorias do material em análise. No nosso estudo optou-se pela criação de categorias *a priori*, como forma de facilitar a classificação do texto em função dos objetivos específicos da investigação.

A mesma autora identifica três fases da técnica de análise de conteúdo: pré-análise, análise e interpretação. A fase de pré-análise tem como intento a leitura dos documentos a serem submetidos a análise, a formulação de hipóteses e dos objetivos e a elaboração de indicadores que fundamentem a interpretação final; a fase da análise do material é o momento de exploração e tratamento do material coletado e consiste no estabelecimento de uma codificação e enumeração que possibilite a identificação rápida de cada elemento da amostra.

Bardin (2016), citada por Ferreira M. N. (2017), sinaliza que a organização da codificação compreende a definição de unidades de recorte, segmento mínimo com significado completo e como unidade de contexto a parte do documento necessária para compreender o sentido global do discurso e precisar o significado da unidade de registo. Esta segunda fase permite a produção de um texto síntese para cada categoria, de modo a expressar o conjunto de significados presentes nas diversas unidades de análise.

A terceira e última fase é a do tratamento dos resultados obtidos, requerendo o estabelecimento de inferências e interpretação, “consiste em descobrir por detrás do discurso aparente, geralmente simbólico e polissémico, um sentido não explícito. E isso exige grande esforço de interpretação” (Cardoso, Oliveira, & Ghelli, 2021, p. 110). Em suma, seguindo as conclusões dos mesmos autores, é possível inferir que a análise de conteúdo é uma técnica de análise de comunicações, que visa, por procedimentos sistemáticos de descrição de conteúdo de mensagens, a obtenção de conhecimentos relativos ao emissor, ao recetor e ao meio.

O processo de categorização também encerra regras e elementos fundamentais, como resumido por Carlomagno e Rocha (2016, p. 184):

- a) “É preciso existir regras claras sobre os limites e definição de cada categoria;
- b) As categorias devem ser mutuamente exclusivas (o que está numa categoria, não pode estar noutra);
- c) As categorias devem ser homogêneas (não ter coisas muito diferentes entre si, no mesmo grupo);
- d) É preciso que as categorias esgotem o conteúdo possível (conteúdos que não encaixem em categoria alguma);
- e) É preciso que a classificação seja objetiva, possibilitando a replicação do estudo”.

Outros autores, nomeadamente Freitas, Júnior e Mascarola (1997) sinalizam a importância do estabelecimento e cumprimento de regras predefinidas, claras e precisas, pois só assim a análise de conteúdos pode ser objetiva e sistemática e pode permitir que diferentes investigadores, ao analisarem os mesmos conteúdos, cheguem aos mesmos resultados.

Sampaio e Lycarião (2021) sugerem que uma das maiores lacunas no manual de Bardin (2016) é a excessiva simplificação do desenho da análise de conteúdo e dão o exemplo de Bauer & Gaskellm (2007), que subdividem as fases da autora em oito fases diferentes. Sampaio e Lycarião (2021), baseados em Riffe, Lacy, Watson e Fico (2019), apresentam a análise de conteúdo em três grandes etapas, conforme o esquema apresentado no Anexo VI. Contudo, independentemente disso, na nossa pesquisa seguimos as fases recomendadas por Bardin (2016), por ser a mais antiga e difundida na literatura.

Quanto ao uso desta técnica no domínio das ciências empresariais e em concreto da contabilidade, o artigo de Alves (2011) identifica a aplicação da análise de conteúdos a diferentes temas e tópicos na investigação em contabilidade. Neste âmbito a autora observou 53 artigos publicados em 23 revistas, incluídas na base de dados ProQuest, entre 2001 e 2010. Verificou como tema mais investigado o relato financeiro, com destaque para o tópico designado de capital intelectual e que o objetivo mais comum era explicar, explorar e/ou descrever as diferenças nas práticas de divulgação de informação. Venceu ainda que a “potencialidade da análise de conteúdo como método de investigação no estudo de uma gama de temas e tópicos..., sobretudo para permitir a verificação de tendências e padrões em documentos (na maioria dos estudos, nos Relatórios de Contas)” (Alves, 2011, p. 156). Ainda no domínio da contabilidade, também Moura e Filho (2010) alertam para a necessidade de se procurarem melhorias constantes para o desenvolvimento e solidificação da investigação, sendo que o principal objetivo do seu estudo foi evidenciar desenvolvimentos teórico-metodológicos que as técnicas de análise de conteúdos podem trazer para a pesquisa em contabilidade, realizada com o auxílio da teoria institucional. Estes autores focaram-se assim nas contribuições que a análise de conteúdo traz para o desenvolvimento de investigação sobre estratégia e estudos organizacionais, nomeadamente no que se refere às práticas, rotinas e procedimentos de contabilidade. Concluem os autores pela importância do uso da análise de conteúdo, nomeadamente pela sua capacidade de retirar informação de dados textuais,

como as divulgações financeiras. Também Steenkamp e Northcott (2007) são um outro exemplo do uso de análise de conteúdo em contabilidade, sustentados nos relatórios anuais (sobre propriedade intelectual) de empresas da Nova Zelândia. Aliás, neste artigo os autores são bastante acutilantes e referem que a análise de conteúdo não é um simples exercício de contagem de palavras, mas antes uma técnica de produzir e recolher dados, através da produção de inferências sobre as mensagens transmitidas pelos textos escritos e imagens visuais presentes nas demonstrações contabilísticas.

Assim, no nosso estudo de caso, e após a realização das entrevistas, foi feita a sua transcrição para um documento *Word*, foi criada também uma grelha (Anexo VII) onde definimos *a priori* 4 categorias, o que nos permitiu individualizar as unidades de contexto, as unidades de registo e a frequência.

Para auxiliar o processo de compreensão do conteúdo e só em relação à análise qualitativa, recorreu-se também ao *software* Nvivo. Nvivo é “um *software* de análise de dados qualitativos desenvolvido para fornecer um espaço de trabalho e reflexão para organizar, visualizar e analisar os seus dados não estruturados e qualitativos... faz a gestão de várias fontes e formatos de dados, como entrevistas” (Gades Solutions, 2022, p. 1).

A propósito do Nvivo, Miranda (2016) enumera algumas vantagens, entre o *software* de análise qualitativa mais popular, nomeadamente:

- Permite visualizar hierarquicamente o esquema de codificação;
- Facilita a organização dos dados em grupos de códigos pelo uso de nós de ligação entre códigos e subcódigos;
- É útil em estudos que usem amostras pequenas e entrevistas semiestruturadas;
- É simples de usar;
- Permite apresentar vários temas e as suas relações num diagrama;
- Oferece uma variedade ampla de desenhos de pesquisa e métodos de análise de dados;
- Alivia o investigador da codificação manual.

Todas as transcrições das entrevistas foram importadas para o Nvivo como “fontes”, mas não optámos pela autocodificação, facto que reforçamos, uma vez que as codificações foram pré-estabelecidas por nós com a criação das categorias e depois de fixada a questão de investigação. Pretendeu-se, com a utilização deste programa unicamente verificar quais as 40 palavras mais frequentes e estabelecer uma hierarquia de palavras usadas, tendo sido necessário excluir algumas palavras que não têm qualquer significado na análise de conteúdo, tais como “acho”, “não”, “aqui”, “etc.” ou “para”, entre outras.

Para finalizar este subcapítulo resta-nos abordar a análise quantitativa de dados. Esta é, para Freixo (2011), um processo sistemático de recolha de dados observáveis e quantificáveis com base na

observação de factos, acontecimentos e fenómenos que existem independentemente do investigador. Já, segundo Vilelas (2020), o objetivo é a generalização dos resultados obtidos, o que se faz através do conhecimento e controlo das variáveis de modo a eliminar os fatores de incerteza. Ainda para Creswell (2013), citado por Santos e Lima (2019), a estratégia de investigação quantitativa procura explicações para os fenómenos estudados através da formulação de hipóteses prévias e da utilização de técnicas de verificação sistemática, procurando testar teorias através da verificação da relação entre variáveis. O investigador tem assim ao seu dispor dois tipos de estatística, a descritiva e a indutiva ou inferencial (Santos & Lima, 2019).

Começámos por sinalizar diferenças entre técnicas paramétricas e técnicas não paramétricas. As primeiras são, segundo Hill e Hill (2012) estatísticas que lidam com parâmetros, e um parâmetro é uma característica de um universo. As estatísticas paramétricas assumem um pressuposto forte, nomeadamente que, no universo (e numa amostra retirada do universo), os valores de uma variável têm uma distribuição normal. Os autores identificam também como um dos pressupostos mais importantes o que diz que os valores de uma variável são medidos numa escala de intervalo ou rácio. São tidos como mais poderosos e com maior capacidade de detetar diferenças entre as medidas comparadas (Sá, Costa, & Moreira, 2021). Por sua vez, os testes paramétricos exigem que os dados “tenham uma distribuição normal, especialmente se tiverem uma dimensão inferior a 30. Em caso de dimensão superior, a distribuição tem de ser aproximar à distribuição normal” (Firmino, 2015, p. 8). Já as técnicas não-paramétricas não lidam com parâmetros, não assumem que os valores de uma variável têm uma distribuição normal e permitem, desta forma, analisar variáveis com valores numa escala ordinal ou numa escala nominal. E ainda que nas escalas ordinais de maior dimensão seja admissível o uso de técnicas paramétricas. Em qualquer caso o uso de técnicas não paramétricas é recomendado quando o número de observações é pequeno, particularmente, quando estamos em presença de um $N < 30$ e, quando o N é maior, mas os pressupostos paramétricos não se verificarem (Sá, Costa, & Moreira, 2021). Como última nota, os mesmos autores referem que os testes não paramétricos não se devem utilizar em situações em que se observem as condições de utilização dos testes paramétricos, por serem ligeiramente menos eficientes. Assim, sem pretendermos ser exaustivos, faremos referência principalmente aos testes estatísticos utilizados, ainda que por necessidade de contraposição ou explicação da escolha se faça referência a outros.

Nascimento, Venturine, Demba, e Neves (2021) citam alguns autores como Graybill et al (1998), Guimarães (2008) e Samohyl (2009), para definir os testes estatísticos, sendo estes entendidos como procedimentos que permitem tomar uma decisão (aceitar ou rejeitar a hipótese nula, usualmente representada por H_0), por oposição a uma hipótese alternativa, utilizando os dados observados de uma determinada experiência e inferir determinadas características da população através de amostras que a representem. São usados modelos diferentes para fazer comparações, mas os testes partem sempre da mesma premissa que é testar se uma hipótese inicial, hipótese nula (H_0) não pode ser rejeitada,

(considerando um determinado nível de significância), ao mesmo tempo que se testa se hipótese alternativa (H1) não pode ser rejeitada, sendo esta contrária à primeira.

Seguidamente procurou-se entender a eventual existência de diferenças na percepção de compatibilização do RGPD com a Lei de combate ao BC/FT e com o sigilo bancário, por ser essa uma das questões de investigação do presente estudo. Para tal foram, sistematizadas as variáveis ordinais, nominais e métricas, constantes no quadro seguinte.

Quadro 6: Ficheiro de Dados

Escala de Medida	Ordinais: respostas alternativas, estabelecendo uma ordem de relação entre elas	Nominais: categorias de resposta qualitativamente diferentes e mutuamente exclusivas	Métricas: dados quantitativos
	V6_Perc_compatib com uma escala entre 1 e 9, em que 1 Totalmente incompatível e 10 Totalmente compatível Ausência de resposta (99)	V1_Genero: Masculino (1) ou Feminino (2)	V2_Idade
	V_8.1 a V_8.9 (fatores críticos) com uma escala entre 1 e 6, em que 1 Discordo totalmente e 6 Concordo totalmente Ausência de resposta (99)	V4_Habilita: Ensino Básico (1) Ensino Secundário (2) Bacharelato (3) Licenciatura (4) Pós-Graduação (5) Ausência de resposta (99)	V3_Anos_Banca
	V_9.1 a V_9.10 (eficiência) com uma escala entre 1 e 6, em que 1 Discordo totalmente e 6 Concordo totalmente Ausência de resposta (99)	V5_Funcoes: Área Comercial (1) Direção de Compliance (2) Direção de Auditoria (3) DMPN (4) Direção Jurídica (5) Ausência de resposta (99)	
		V7_Compatibilizacao: Fácil (1) Difícil (2) Ausência de resposta (99)	
		V_10_Dificuldade: Sim (1) Não (2) Ausência de resposta (99)	

Fonte: Elaboração Própria, baseado em Hill e Hill (2012).

Tenha-se em conta que, em regra a análise estatística é iniciada pela análise descritiva. Situação também efetuada nesta dissertação, tendo-se começado pela caracterização dos respondentes. A análise descritiva resume os dados e permite ao investigador obter as primeiras interpretações dos dados recolhidos (Coutinho, 2014), citado por Sá, Costa e Moreira, 2021).

Foi necessário ainda aferir as condições de aplicação dos testes paramétricos. Neste âmbito os testes de Kolmogorov-Smirnov e Shapiro-Wilk são utilizados para testar a normalidade da distribuição. O teste de Kolmogorov-Smirnov é usado para decidir se a distribuição da variável sob estudo provém de uma população com uma distribuição específica (Maroco, 2003). O autor indica ainda que a alternativa ao teste Kolmogorov-Smirnov que o SPSS produz, surge o teste de Shapiro-Wilk, tendo em atenção que este último é mais exato quando o N é maior do que 100. No nosso caso importava entender se os pressupostos de normalidade se verificavam, ou não.

Como já referido, no âmbito da inferência estatística surgem primeiramente os testes paramétricos “que visam analisar a viabilidade dos resultados da variável dependente, em função da manipulação das variáveis independentes, de forma a que se possa refutar ou aceitar a hipótese nula, a qual postula que os resultados da investigação são devidos, não aos efeitos previsto pela hipótese experimental, mas a diferenças aleatórias nos resultados, devidas a outras variáveis irrelevantes ou ao acaso” (Firmino, 2015, p. 8). Desta forma, os testes paramétricos não foram usados pois estes exigem que a amostra tenha uma distribuição normal. O pressuposto da normalidade não foi comprovado na maioria das variáveis deste estudo. Logo o teste t ficou injustificado. O teste paramétrico t testa se a média de dois grupos é significativamente diferente, mas pressupõe a existência de uma distribuição normal. Assim, como alternativa ao teste t foi utilizado o teste de U Mann-Whiney que é alternativa não paramétrica para amostras independentes e que permite detetar diferenças significativas entre os valores, quando se consideram sujeitos diferentes (Martinez & Ferreira, 2008). Pestana e Gageiro (2000) referem que o teste t compara as médias de duas amostras independentes, enquanto teste de Mann-Whiney compara o centro de localização das duas amostras, como forma de detetar diferenças entre as duas populações correspondentes. O último é assim preferível ao teste t, no presente estudo, pois “trata-se de um teste não paramétrico potente, e constitui uma alternativa bastante útil quando se deseja evitar suposições exigidas pelo teste paramétrico t” (Firmino, 2015, p. 97).

O teste de Mann-Whiney pode ser, por sua vez, generalizado para mais de dois grupos através do teste de Kruskal-Wallis (Pestana & Gageiro, 2005). Este teste foi também utilizado e é considerado a alternativa não paramétrica ao teste Anova para amostras independentes, sempre que não se encontram reunidas as condições de aplicação de um teste paramétrico, no caso quando não se encontram reunidos os pressupostos da normalidade (Maroco, 2003; Martinez & Ferreira, 2008).

Relativamente à análise da consistência interna Maroco e Garcia-Marques (2006) salientam o Alfa de Cronbach como aquele sobre o qual assenta a confiança da maioria dos investigadores e uma das medidas mais utilizadas para avaliar a fiabilidade de uma variável latente. Os mesmos autores qualificam-no como um “instrumento útil para a investigação da fiabilidade de uma medida” (Maroco & Garcia-Marques, 2006, p. 80).

Segundo Churchill (1979) e Kline (2011), citados por Miranda (2016), devemos considerar como

valor mínimo satisfatório 0,3, sendo apontados como adequados valores acima de 0,7. Consequência do que se descreveu, no sentido de avaliar a consistência das várias dimensões em análise pode recorrer-se ao cálculo do valor de Alfa de Cronbach, que segundo Pestana e Gageiro (2005) estima em que medida a uniformidade dos vários itens contribuem para a soma não ponderada do instrumento. Para estes autores um instrumento tem fiabilidade apropriada quando assume também um valor maior que 0,7.

Por fim é de referir que, os testes não paramétricos são, como referem Nascimento, Venturine, Demba e Neves (2021), particularmente adaptáveis aos dados das ciências do comportamento e interessantes para análise de dados qualitativos. No nosso caso, acresce que os teste escolhidos foram aqueles que melhor se alinharam com as variáveis e escalas que se pretenderam analisar, factos que serão detalhados no capítulo *Resultados*.

3.6 Síntese

Neste capítulo especificou-se a investigação quanto à ontologia, epistemologia, estratégia de investigação, técnicas de recolha e de análise de dados.

Assim, esta investigação é relativista, interpretativista, baseada no recurso ao estudo de caso, usa as técnicas de análise documental, entrevistas semiestruturadas e questionários semiestruturados como instrumentos de recolha de dados. Já a análise de dados considera a análise categorial de conteúdo, bem como análise estatística para procurar as respostas às questões de investigação.

No que respeita à análise estatística, além da análise descritiva recorre a testes não paramétricos.

4. Resultados

O presente capítulo apresenta e discute os resultados do estudo empírico. Adicionalmente, começa por enquadrar o estudo de caso, ou seja, serviços específicos do Banco BPI.

Pretende ainda demonstrar os resultados obtidos no nosso estudo de caso realizado nas áreas funcionais do Banco BPI que adiante se especificam e tem como propósito responder às questões de partida, aos objetivos gerais e objetivos específicos, a que nos propusemos.

É nossa intenção apresentar os dados recolhidos, discuti-los e fazer a sua interpretação à luz do enquadramento teórico, complementado com o estudo empírico e tendo em conta os objetivos definidos *a priori*. A análise dos dados será feita através da informação recolhida em entrevistas e questionários realizados, da observação direta realizada em contexto de trabalho da investigadora e da análise de documentação, quer disponível nos sites públicos, quer informação interna.

4.1 O Banco BPI SA

A origem do BPI remonta a 1981 com a criação da SPI – Sociedade Portuguesa de Investimentos. Em 1985, a SPI deu origem ao BPI, primeiro banco privado criado após a reabertura do setor à iniciativa privada no seguimento das nacionalizações em 1975. Em 1986 tona-se o primeiro banco cotado na bolsa portuguesa. Durante vários anos continuou o seu crescimento através de algumas aquisições e fusões com outros bancos.

Segundo informação oficial do site do banco, atualmente o Banco BPI faz parte do Grupo *CaixaBank*, e é, desde 27 de dezembro de 2018, integralmente detido pelo *CaixaBank*, S.A., tem cerca de 1,93 milhões de clientes no mercado doméstico (Banco BPI, 2021). A rede física inclui 421 balcões de retalho, 1 balcão móvel, 39 centros *premier*, 31 centros de empresa e institucionais e 3 centros de *Corporate and Investment Banking*.

Estando nesta data já disponíveis os resultados de 2021, consultados em Informação Financeira (2022), verifica-se que o BPI apresentou um total de balanço consolidado de 41.378.311 milhares de euros, um total de capital próprio de 3.667.51 milhares de euros e um resultado líquido consolidado de 306.823 milhares de euros. Apresentou ainda um volume de negócios de cerca de 59 mil milhões de euros e tinha no final do ano 4.484 funcionários.

4.2 Análise qualitativa

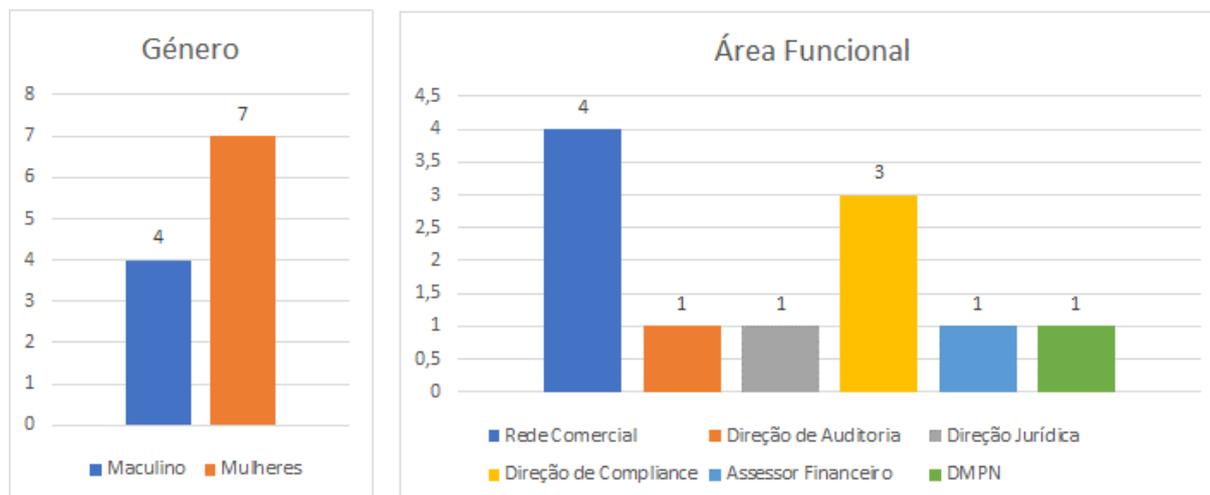
A análise dos resultados será aqui apresentada com recurso a quatro dimensões distintas, segundo as categorias que foram previamente definidas (Anexo VII):

1. Importância da compatibilização harmoniosa dos diplomas;
2. Fatores críticos na implementação (RGPD, LBC/FT e SB);

3. Aumento da eficiência associada a dados a recolher, momentos e fluxos;
4. Redução da eficiência associada a dados a recolher, momentos e fluxos.

Far-se-á de seguida uma caracterização geral do grupo de entrevistados, tendo em conta o género, anos de experiência, habilitações literárias e área funcional. Tendo em conta as características de cada um dos entrevistados, a sua área de atuação e procedimentos que desempenham no dia a dia, foi necessário e possível, pela escolha de entrevistas semiestruturadas, capturar diferentes perspetivas.

Figura 4: Caracterização dos entrevistados



Fonte: Elaboração própria.

Quanto aos anos de experiência dos entrevistados encontravam-se compreendidos entre o valor mínimo de 12 anos e máximo de 30. A média situou-se nos 18,55 anos, com um desvio padrão de 6,23.

Da análise gráfica verifica-se que o nosso grupo é constituído por 7 mulheres e 4 homens, todos com vários anos de experiência. Todos os entrevistados são licenciados, em áreas diversas que vão desde a Sociologia (1), Ciências da Comunicação (1), Direito (3), Gestão (3), Economia (2) e Marketing (1). Para além da licenciatura base dois dos entrevistados referem ter formação adicional noutras áreas (Gestão Bancária, Pós-graduação em mercados e instrumentos financeiros e especialização em *compliance*, pelo Instituto de Formação Bancária).

Relativamente às áreas funcionais são mais representativas a Rede Comercial e a Direção de *Compliance*, com 37% e 27% dos entrevistados, respetivamente.

Todos autorizaram a gravação das entrevistas e responderam positivamente à pergunta sobre a familiaridade com as temáticas de RGPD, BC/FT e sigilo bancário.

Depois de caracterizado o grupo de entrevistados faremos de seguida a análise de conteúdo das 11 entrevistas realizadas.

Desta forma, e pela análise de conteúdo dos discursos que a integram, verifica-se que o tema mais

desenvolvido está relacionado com a categoria 1 (Importância da compatibilização harmoniosa dos diplomas), com 66 unidades de registo, seguindo-se as categorias 3 (Aumento da eficiência associada a dados a recolher, momentos e fluxos) e a categoria 2 (Fatores críticos na implementação (RGPD, LBC e SB), com 53 e 39 unidades de registos, respetivamente. O tema menos desenvolvido foi o da categoria 4 (Redução da eficiência associada a dados a recolher, momentos e fluxos), com apenas 29 unidade de registo.

Antes de passarmos à análise de conteúdo em profundidade apresentamos o resumo dos dados efetuado com recurso ao *software Nvivo*. Com a utilização deste programa pretendemos apenas verificar quais foram as palavras mais usadas, tendo limitado este número a 40, eliminando palavras com menos de três caracteres e retirando dos ficheiros de transcrição das entrevistas palavras que em nada acrescentam significado ao discurso (“termos indesejados”) como por exemplo “pois”, “porém”, a identificação dos entrevistados “E1”, “E2”, “não”, “acho”, entre outros.

Figura 5: Nuvem de palavras



Fonte: Elaboração própria com recurso ao NVivo.

Destacamos assim as palavras “dados”, “RGPD” e “informação”, como as mais usadas, mas também, e entre outras, clientes, importância, sigilo bancário, eficiência, processos, documentos e recolher. A palavra “dados” foi referida 200 vezes, “RGPD” 122, “informação” 118, “cliente” 102 e “sigilo” 99 vezes.

O *Nvivo*, e mantendo-nos exclusivamente na hierarquia de palavras, construiu também um mapa de árvore que é uma outra forma de apresentar a frequência, com figuras proporcionais ao número de citações (Anexo VIII) e uma análise de *cluster* (Anexo IX), que é também útil e interessante pois permite a visualização dos termos mais frequentes (círculos maiores) e também a sua proximidade de outros termos frequentes.

A palavra mais citada (dados) está assim relacionada com o primeiro referencial em estudo, o RGPD (segunda palavra mais citada) que visa precisamente a proteção de dados (pessoais). As palavras “dados” e “informação” estão obviamente relacionadas com o RGPD, mas estão igual e intimamente relacionadas com o regime de BC/FT, pois como temos verificado ao longo do nosso estudo a única forma de gerir o BC/FT é a recolha e atualização constante de dados e informação dos clientes, pois,

sem dados não há possibilidade de construir o *KYC* e gerir o risco de *compliance*.

4.2.1 Importância da compatibilização dos diplomas

A nossa análise categorial de conteúdo das entrevistas realizadas estruturou-se tendo por base as quatro categorias por nós definidas, estando a primeira relacionada com a compatibilização dos diplomas legais. Esta temática assume uma enorme relevância e foi a que obteve mais unidades de registo (66). Ao longo do guião de entrevistas várias foram as questões orientadas no sentido de perceber qual a sensibilidade dos entrevistados quanto às fronteiras existentes entre os 3 regimes e a forma como se compatibilizam.

Em relação ao RGPD, legislação mais recente, é de notar que para os entrevistados este regime apenas veio trazer alterações no tratamento de dados para fins de *marketing* e publicidade, contactos comerciais e para a definição de perfis:

- “...a nível dos contactos, as restrições isso é definido pelo cliente: como é que prefere ser contactado, em que horário, o telemarketing... o cliente veio definir o que é mais conveniente para si e que o banco neste caso é obrigado a respeitar de acordo com a vontade do cliente...” E4.

De referir também a importância que reconhecem ao novo regulamento ao colocar no consentimento do cliente a principal tónica. O consentimento do cliente foi referido por 4 dos entrevistados, a título de exemplo a seguinte unidade de registo:

- “...temos que ter mais um consentimento dos clientes, estes têm uma palavra a dizer sobre o tratamento dos dados que eles nos facultam e estejam alertados para essa situação...” E3;

O consentimento é assim o principal princípio do RGPD que é apontado pelos entrevistados e vai no sentido do que já foi sinalizado na nossa revisão de literatura, ou seja, é o princípio basilar do regime, que legitima o tratamento dos dados pessoais e sem o qual todos os outros perderiam o seu sentido.

O princípio da limitação das finalidades (como apontado na revisão de literatura está previsto no art.º 5.º, n.º 1, al, b) do RGPD e no art.º 35.º, in fine da CRP) permite o controlo pelo cidadão dos fins para os quais são recolhidos os seus dados pessoais e foi também referido por vários entrevistados. Assim, a finalidade da recolha de dados pessoais deve ser determinada, explícita e legítima, não podendo ter um fim diferente daquele que foi acordado. Vejamos as seguintes unidades de registo que o referem:

- “...o que se preconiza é só utilizar os dados para as finalidades específicas para as quais são recolhidas ou então de acordo com a lei pois a lei também possibilita, sem consentimento, fazer a gestão dos dados...” E7
- “... o RGPD, de uma forma genérica, visa proteger a informação relativa às pessoas

e para que ela seja utilizada para o propósito a que se destina...” E11

Esta última citação permite-nos verificar que para além do consentimento e da limitação do tratamento de dados para o fim para o qual foram recolhidos, também existem tratamentos de dados sem o consentimento do titular. Entramos aqui especificamente na necessidade da compatibilização dos diplomas legais.

A importância do RGPD é referida também como uma proteção adicional ao titular dos dados pessoais, e em particular ao cliente bancário, na medida em que visa evitar o tráfico de informações entre as empresas e mesmo até a circulação abusiva de dados, nomeadamente com parceiros, sem o consentimento dos titulares, a título de exemplo as seguintes citações:

- “...RGPD permite evitar o tráfico de informação de clientes entre grandes empresas...” E10
- “... o RGPD vem em complemento, vem reforçar de facto essas medidas e fazer com que o banco não utilize essa informação dos clientes ou potenciais de forma abusiva...” E10

A citação anterior remete-nos para a temática do sigilo bancário, tendo sido pedido aos entrevistados que se pronunciassem sobre este regime individualmente, mas também que ponderassem a fronteiras do sigilo bancário à luz do RGP e à luz da lei de BC/FT.

A maioria dos entrevistados tem consciência da importância do sigilo bancário e do RGPD nas tarefas do dia a dia e da sua presença em todas as atividades, tendo sido verificadas 9 unidades de registo neste sentido, a título de exemplo a seguinte:

- “...o sigilo bancário sim é uma preocupação que nós temos que ter, é algo que temos que respeitar bastante no nosso trabalho... tem que haver sempre esse cuidado de nós quando falamos com o cliente não falar em alto para outros clientes não ouvirem... nas perguntas de outro cliente nós não podemos partilhar dados, temos que ter sempre cuidado às vezes mesmo em termos informais...” E1

De uma forma geral todos os entrevistados consideram que RGPD e sigilo bancário são dois regimes perfeitamente compatíveis. Referem que o RGPD vem até reforçar e complementar o sigilo bancário, tendo esta compatibilização sido expressamente referida em 4 unidades de registo, a título de exemplo:

- “...o sigilo bancário faz parte da proteção de dados, é um aspeto que engloba a proteção de dados. Esta depois tem outras dimensões... mas a confidencialidade e o sigilo bancário é precisamente uma delas, portanto, é completamente conciliável. A partilha de dados quando é feita tem de ser fundamentada e com as regras de segurança possíveis, mas digamos que há um casamento perfeito aqui...” E6

- “...acho que é perfeitamente possível, aliás uma coisa até reforça e complementa a outra... o RGPD veio reforçar, em primeira instância aquilo que é o sigilo bancário, para não andar nenhum documento descuidado, para não andar informação descuidada fora do circuito, para não se partilhar dados sem necessidade e sem autorização prévia dos clientes...” E10

Para alguns dos entrevistados estes dois regimes até se confundem, de tão inerentemente ligados que estão, e neste sentido encontramos 2 unidade de registo:

- “... a proteção de dados aparece aqui também como um reforço ao sigilo bancário ...” E5
- “...o sigilo bancário é algo que está inerentemente ligado ao RGPD ainda que eventualmente não o mencione expressamente...” E11

E se para um dos entrevistados o consentimento à partilha derroga de imediato o sigilo, para outro nem se pode falar em quebra de sigilo se a partilha de dados for feita dentro do próprio banco:

- “...se o cliente autorizar que a partilha de dados seja efetuada julgo que o sigilo bancário já está um pouco, ultrapassado...” E1
- “... se a partilha de dados não vai sair do âmbito do que é nossa instituição do que é o nosso banco, não vai mais além... porque se foi mais além já está interferindo no sigilo bancário...” E4

Em relação ao binómio sigilo bancário e RGPD conclui-se que é uma temática muito importante e que todos os entrevistados têm noção dessa importância e que são perfeitamente compatíveis, veja-se a unidade de registo seguinte:

- “...sim tenho esse cuidado de não partilhar os dados dos clientes que não o autorizaram até porque o banco faz diversas formações a esse nível e todos estamos alertados para essas situações e para as multas a que o banco está sujeito...” E1

Não referem assim qualquer incompatibilidade a nível dos normativos que se traduza por sua vez em incompatibilidades nas suas tarefas do dia a dia. Aliás, é inclusivamente referido em 5 unidades de registo que para haver uma quebra de sigilo tem de existir uma autorização expressa de entidades judiciais, estando, portanto, estas situações bem definidas:

- “...existem as exceções, nomeadamente o sigilo pode ser quebrado se houver alguma suspeita, nomeadamente a nível das autoridades. Nessas situações deve estar tudo definido e nessas situações o banco terá que ser obrigado a fazê-lo, dentro dessas exceções...” E4
- “... nós não podemos partilhar oficialmente informação fora do banco sem termos

a necessária autorização para a derrogação do sigilo bancário...” E11

Contudo, quando se referem às exceções e à derrogação dos regimes previstos na lei não estabelecem diferenças entre o RGPD e sigilo bancário, reforçando o sentido de que são regimes compatíveis e que até se confundem.

Desta forma, ambos visam a discricção e a confidencialidade, tal como antes referido no nosso estado da arte e têm subjacente a proteção de direitos, liberdades e garantias individuais dos cidadãos. Contudo existem exceções também reconhecidas pelos entrevistados, que permitem, na ótica da proporcionalidade e na ponderação dos direitos a proteger do caso concreto, a sua derrogação. Apesar de não haver referências em concreto em nenhuma unidade de registo a uma exceção em particular, fazem-se sim referências às exceções previstas na lei de um modo geral. Estas foram elencadas na revisão do estado da arte e são resumidamente questões de interesse público, como a segurança e defesa do Estado, interesses económicos, financeiros ou fiscais, defesa da independência judiciária, entre outros.

A necessidade de ponderação de valores e interesses em causa também foi uma matéria abordada no que toca ao BC/FT. E se no binómio RGPD e sigilo bancário se conseguiu chegar à conclusão da sua complementaridade, já relativamente ao BC/FT o consenso não foi tão fácil, como veremos:

- “... sigilo e a proteção de dados é o casamento perfeito... o sigilo é uma componente da proteção de dados... No BC/FT quanto menos sigilo tiver que cumprir, quanto mais souber melhor... aliás esta é uma temática que é muito discutida a nível europeu também e das instituições e como é que estas duas realidades se conjugam...” E6;
- “...não é muito fácil... há áreas que se tocam e há áreas que se repelem... por vezes para dar seguimento a uma proteção de dados não poderíamos revelar certas coisas que serão do âmbito do BC. Há que ter um certo bom senso para saber qual delas é mais urgente tratar e dar prioridade...” E3
- “...já com o branqueamento de capitais não é bem a mesma coisa...” E6

Todas estas matérias que abordamos se relacionam porque todas elas tratam com dados, e estes são informação. E se o RGPD não trata dados por si só, a prevenção do BC/FT não tem outra forma de gerir o risco, que não o tratamento de dados, exemplo são as 3 unidades de registo seguintes:

- “... o RGPD protege os dados que são recolhidos dentro do banco com as várias finalidades que deles existem... dados, estamos a falar de informação das pessoas e, portanto temos informações financeiras, patrimoniais tudo o que é recolhido no banco nós olhamos para isso... mas eu não tenho dados específicos para o RGPD, isso não existe...Eu trato com os dados que o banco trata... portanto com dados do branqueamento de capitais, com os dados do risco, com dados comerciais que são

oferecidos, com tudo isto não é, não tenho dados específicos de RGPD...” E6

- “...nós quando abrimos uma conta... vamos usufruir daqueles dados que estamos a recolher para a restante relação contratual...no fim da relação contratual temos de os conservar pelo prazo legal de 7 anos, por via da prevenção BC/FT... findo desse prazo temos que eliminar os dados...” E7
- “... toda a informação com que trabalhamos está relacionada com a proteção de dados...” E9

Para melhor perceber por que motivo a prevenção do BC/FT foi identificada como podendo colidir com alguns princípios do RGPD e sigilo bancário (a partir daqui assumiremos que o tratamento destes regimes é feito de igual forma), necessário é relembrar o estado da arte em relação à sua própria definição e fundamentos e o que os entrevistados afirmam sobre esta matéria:

- “... e depois a questão da luta contra o BC/FT aquilo que está em causa é a própria transparência do setor, o reconhecer o cliente, o definir regras de atuação com clareza e evitar o tráfico de estupefacientes, pessoas, etc. ...garantir que no sistema bancário estão atividades lícitas, que ajudam a economia a crescer, com transparência e rigor e com tudo aquilo que é o contributo positivo de cada empresa ou particular para aquilo que são os impostos de cada país...se toda a gente tiver essa consciência é tudo mais fácil para todos...” E10
- “... dos 3 sem dúvida que para mim é o branqueamento de capitais, sigilo bancário e proteção de dados também não temos dúvida, mas sem dúvida que a prevenção do branqueamento de capitais deve prevalecer porque quem faz isso está a prejudicar outras pessoas e acho que aí não se deve colocar a questão do sigilo bancário, ou a proteção de dados...” E1
- “... ok estava a falar dos direitos liberdades e garantias do sigilo, mas o BC/FT é um crime e provavelmente aqueles deixam de ter tanta importância senão seria um encobrimento desse crime...” E3
- ... “tem sido entendido como uma premissa até agora que as matérias sobre prevenção de BC sobrepõem-se às matérias de proteção de dados... obviamente que eu tendo a concordar com isto...” E11

Assim, e como já referido antes, para o BC/FT o setor dos serviços financeiros é um meio importante através do qual essa lavagem pode ser feita, conforme refere Duarte (2019). Outros autores antes referidos como Rodrigues (2010) e Jesus (2016) referem-se ao BC/FT como uma forma de criminalidade complexa devido à existência de crimes subjacentes ou crimes primários, como por exemplo o contrabando de pessoas ou tráfico de droga. O BC/FT não é um crime por si só, utiliza o

sistema financeiro na dissimulação e ocultação dos capitais obtidos de forma ilícita e sustenta algo mais preocupante que o crime financeiro.

São estas as principais preocupações igualmente reconhecidas pela maioria dos entrevistados e estando presentes em pelo menos 5 unidades de registo, ao colocar a prevenção do BC/FT como primordial e mais importante face aos outros dois regimes:

- “... mas sem dúvida que a prevenção e branqueamento de capitais deve prevalecer porque quem faz isso está a prejudicar outras pessoas e acho que aí não se deve colocar a questão do sigilo bancário, ou a proteção de dados...” E1
- “... coloco no topo o BC/FT porque tem implícito o RGPD e o sigilo, abarca os dois: os dados sensíveis têm de ser tratados com cuidado...” E9

Um dos entrevistados afirma expressamente que a lei exceciona as questões de proteção de dados, face a um interesse específico que é mais importante e que se deve proteger, e um outro, considera até que se complementam na perspectiva de que, havendo suspeitas, pode haver quebra de sigilo:

- “... se a lei não for alterada, existe um interesse específico mais importante que exceciona o RGPD...” E11
- “... ou seja, respeitando na mesma o sigilo bancário, mas depois só o quebrar quando efetivamente há alguma suspeita e nós temos que fazer a comunicação das operações suspeitas a quem de direito... eu acho que eles na prática se ajudam uns aos outros...por isso acho que eles se complementam e que são indispensáveis, apesar de parecerem conceitos um bocadinho opostos...” E2

Assumido que está que os direitos que se visam proteger no RGPD e na prevenção de BC/FT são opostos e também os deveres de RGPD/sigilo bancário e de BC/FT conflituam, nem sempre é fácil afirmar quais devem prevalecer, nem para os entrevistados, nem para algumas entidades, como a CNPD, conforme refere o E7:

- “... nem sempre a CNPD tem abertura suficiente para entender que os deveres que nós temos no âmbito da prevenção do BC/FT se devem sobrepor aos deveres que resultam diretamente da lei da proteção de dados...” E7

Também os autores se pronunciam sobre estes binómios e sinalizam a sua contrariedade. A título de exemplo e revisitando uma vez mais o estado da arte, temos Semedo (2015) que afirma que o instituto do sigilo bancário envolve valores e interesses constitucionalmente protegidos, mas circunscritos à esfera individual, ao invés o crime de branqueamento de capitais remete-nos para valores e interesses mais altos, supraindividuais e também constitucionalmente protegidos. No mesmo sentido, Vicente (2014) que considera evidente que o combate ao BC/FT se tem vindo a sobrepor ao sigilo, ao longo dos tempos e que o equilíbrio é muito difícil de alcançar, pois se existe um aumento da eficiência do ponto

de vista da atuação penal transnacional, inevitavelmente limita em grande escala a proteção dos interesses individuais.

Ainda segundo Athayde, Athayde e Athayde (2009) o equilíbrio entre transparência e sigilo é difícil de atingir, mas indispensável, pois a extinção do sigilo não só empobrece o regime jurídico da banca, mas entre outros males, é também um sério recuo ético.

Neste sentido verifica-se uma unidade de registo:

- “... acho que o sigilo bancário é primordial e também já existe há muito tempo... quer dizer, o BC também, mas o sigilo bancário é daquelas coisas que é transversal a todos os clientes e o branqueamento de capital não. Não toca a todos os clientes, nem sequer à maioria dos clientes...” E4

Mas, se por um lado identificámos 5 unidades de registo que vão no sentido de colocar os direitos e os deveres da prevenção do BC/FT em primeiro lugar, também são identificadas outras 5 unidades de registos que não consideram que haja colisão entre os 3 regimes, antes os equiparam em termos de importância e até afirmam que são complementares:

- “... acho que não punha de lado nenhum... são importantes os 3, apesar de parecerem conceitos que colidem, acho que se complementam acho que é difícil dispensar um...” E2
- “... eu acho que são possíveis de compatibilizar. A questão da transparência da banca que queremos dar para com o mercado, do rigor e salvaguardar os interesses quer do consumidor, quer de todos, neste caso até da própria nação, acho que tudo isto são complementos necessários para a nossa atividade. O sigilo bancário por aquilo que é o reconhecimento da nossa discrição e da nossa reserva sobre a partilha de informações dos clientes, que é o primeiro fator de confiança...” E10
- “... não consigo dizer porque, honestamente, eu vejo os dois com igualdade de importância porque no fim do dia, havendo alguma falha grande da parte do banco em algum dos dois o impacto...para o banco, a nível de risco reputacional será igualmente grande. À data de hoje se calhar uma reportagem na TVI e na SIC etc., sobre temas de BC/FT é mais prejudicial para o banco do que uma reportagem equivalente a nível de RGPD, de sigilo bancário...” E5

Em conclusão podemos afirmar que existem reservas quanto à perfeita compatibilização quanto aos regimes de proteção de dados e da prevenção do BC/FT uma vez que não estão harmonizados em termos de princípios estruturantes: enquanto que os primeiros visam a confidencialidade, a discrição, a menor intrusão possível e pretendem a limitação da reutilização de dados em nome da segurança e proteção da reserva da vida das pessoas, o outro pretende ser intrusivo, ter acesso ao maior número de

dados pessoais, numa ótica de KYC, e em nome de uma segurança que se pode dizer que é de interesse público, e que visa o bem comum, e também o risco reputacional das instituições. Desta forma, os fundamentos das leis de BC/FT são compreendidos por todos e por isso aceites como exceção à proteção de dados. A unidade de registo seguinte é exemplificativa:

- “... tens que por um lado a prevenção do BC/FT que visa basicamente combater a prática de crimes que são muito danosos para a sociedade como um todo, mas em particular para o sistema financeiro... obviamente que isto mina completamente a sociedade. Estamos a fomentar aqui a incidência de crimes que estão na origem, na base de crimes de BC... a lei do branqueamento de capitais existe com um racional bastante compreensível para o comum dos cidadãos...” E7

Mas esta exceção é referida, essencialmente, como sendo uma exceção legal e daí a sua aceitação:

- “... e quando há exceções são exceções concretas e determinadas e conseguimos comprovar o porquê da exceção...” E7
- “... são dois regimes que não estão harmonizados, que são algo conflitantes... há um cuidado acrescido no que toca ao tratamento de informação... mas no que toca à parte de termos informação necessária para analisar o risco fazemo-lo em respeito daquilo que é a lei do BC... que nos dá margem para pedir determinado tipo de informação...” E11

Ainda relativamente às exceções previstas na lei é referida numa unidade de registo a importância de as documentar, numa ótica de comprovação e justificação perante as entidades de supervisão, assim:

- “... as exceções são documentadas e temos um fundamento específico para excecionar o sigilo ou para excecionar a confidencialidade dos dados... no fundo, mas são basicamente, eu diria que em termos práticos que se confundem... porque o objetivo é o mesmo: salvaguardar os dados...” E7

Em suma, os entrevistados compreendem e aceitam as derrogações que possam existir ao sigilo bancário e ao próprio RGPD, não só pela necessária ponderação de interesses e direitos a proteger, na ótica de primazia do bem mais importante, que neste caso será o bem comum e a paz pública, mas também porque a lei prevê as situações de exceção e por isso devem ser aceites.

No sentido de reforçar as conclusões retiradas da análise categorial de conteúdo relativamente à primeira categoria - Importância da compatibilização harmoniosa dos diplomas - recorde-se a necessidade de ponderação de interesses, numa ótica de proporcionalidade e de ponderação de bens e direitos a proteger no caso concreto, referida por alguns autores. Ribeiro (2011) refere que apesar de existir um dever de colaboração por parte das entidades bancárias, por força da lei, o pedido das autoridades deve-se mostrar individualizado e suficientemente concretizado, ou de outra forma poria em

causa o direito à reserva da vida privada, de uma forma desproporcional. O mesmo autor também se refere à existência de tratamento de dados sensíveis ou potencialmente sensíveis e à necessidade de o tratamento das informações obtidas pelas entidades de combate ao BC/FT ter necessariamente de cumprir as demais disposições que concernem à proteção de dados pessoais.

Braga (2020) refere também, citando a Comissão BC/FT que “as instituições e entidades deverão entender que o fornecimento de qualquer informação pedida por autoridades competentes não constitui qualquer violação de segredo ou quebra de sigilo que seja imposto por via contratual, legislativo ou regulamentar”.

Para além dos autores também os normativos legais demonstram esta preocupação. De seguida apenas alguns exemplos já antes citados.

O Decreto-Lei n.º 15/93, de 22 de janeiro – Lei da Droga acaba por ser uma lei que quebra o sigilo bancário, pois obriga as entidades financeiras a conceder informações sempre que forem solicitadas por uma entidade jurídica competente.

A Lei n.º 58/2020, de 31 de agosto também nos dá alguns exemplos sobre a preocupação com as matérias de proteção de dados pessoais, conforme citadas por Garrigues (2021):

- Os canais (específicos e anónimos) de comunicação de irregularidades relacionadas com eventuais violações da Lei n.º 83/2017 devem garantir a confidencialidade das comunicações recebidas e a proteção dos dados do denunciante e do suspeito da infração, conforme o RGPD;
- As entidades obrigadas, desde logo as instituições de crédito, têm de fornecer aos novos clientes um aviso geral sobre as obrigações legais que lhes são aplicáveis em matéria de dados pessoais e seu tratamento, para efeitos de prevenção do BC/FT;
- Reconhecimento legal de que a proteção de dados aqui tratada é do domínio do interesse público.

De seguida será analisada a segunda categoria que se relaciona com os fatores críticos na implementação dos regimes jurídicos.

4.2.2 Fatores críticos na implementação (RGPD, LBC e Sigilo Bancário)

Averiguadas que estão as razões de ser de cada um dos diplomas legais (que no caso do RGPD e sigilo bancário são acautelar a privacidade e minimizar os abusos no uso dos dados pessoais e no caso da prevenção de BC/FT é precisamente o contrário, sem dados não há segurança e quanto maior for o acesso a mais informação menor será o risco a gerir, para a entidade e para a sociedade de uma forma geral), de seguida faremos a análise dos fatores críticos na implementação dos diplomas legais, identificados pelos entrevistados em 39 unidades de registo.

O regime do RGPD e a sua importância para os clientes é referido em 4 unidades de registo, principalmente no que toca em colocar do lado do cliente a decisão de como e para quê querem que os seus dados sejam utilizados, e a sua aplicação essencialmente para efeitos de *marketing* e publicidade:

- “... claro que os clientes acabam por ficar mais salvaguardados nesse sentido porque têm a certeza de que os dados deles não vão ser utilizados para além daquilo que eles nos autorizaram... mas em termos do nosso dia a dia, do nosso trabalho foi muito complicado e depois também em termos da prática comercial...” E1

A entrada em vigor do RGPD, que trouxe essa proteção adicional aos clientes, teve de facto impacto nas práticas do banco e houve uma necessária obrigação de adaptação dos sistemas e processos do banco. Os entrevistados sinalizam, em 8 unidades de registo, que foi necessária a recolha do consentimento quanto a esta matéria, atualizando desta forma os dados dos clientes e recolhendo a devida assinatura, conforme podemos verificar nas seguintes unidades de registo:

- “... nós todos os dias para podermos contactar os clientes, temos que ter em consideração se eles têm o RGPD no sistema ou não...se já foi recolhido... para respeitarmos as respostas do cliente...” E1
- “... depois da entrada do RGPD na nossa atividade tivemos que ir atualizando a ficha de cliente... dá-lhes uma proteção maior e desde essa altura passaram a ter mais confiança...” E4

Acrescentam ainda que todos os processos do banco, desde a sua conceção foram desenhados ou redesenhados numa lógica de recolher o consentimento dos clientes:

- “... mudou de facto porque todos os processos têm de ser desenhados numa lógica de recolher o consentimento, portanto no desenho, na conceção dos processos temos de ter em mente a proteção de dados...” E9

Podemos afirmar que a exigência legal de recolha do consentimento foi o ponto que, na prática, mais constrangimentos acarretou na medida em existem muitos clientes e todos os processos devem então estar em conformidade com o RGPD. Para além deste acréscimo de trabalho associado à recolha do consentimento e assinatura foi ainda necessária a criação do DPO, conforme também a imposição legal:

- “... temos que recolher a ficha de informação, o cliente tem que assinar, tem de dizer o que é que quer em termos de proteção de dados, aceitar ou não aceitar e aí depois temos todo o processo de digitalizar, assinar, enviar, ou seja, toda a parte documental que não é assim às vezes tão rápido... e depois há sempre situações em que um documento se extraviou, temos que recolher novos documentos, ou seja um

acrécimo de trabalho...” E1

- “... o RGPD foi bastante disruptivo porque veio criar obrigações muito superiores às que existiam e com um impacto muito grande para as instituições que não estavam adaptadas às obrigações do RGPD... também muito impacto em sistemas sobretudo, no desenvolvimento de sistemas de execução das tarefas porque tivemos que criar um gabinete específico de proteção de dados... veio criar obrigatoriedade de termos um DPO...” E7

O impacto operacional da constante recolha da assinatura dos clientes é ainda maior no caso de idosos e emigrantes, existindo uma unidade de registo neste sentido e referindo-se quer ao RGPD, quer ao BC/FT:

- “... esta parte muito burocrática da assinatura, da constante recolha da ficha de cliente e como disse muitas vezes até de clientes que estão longe e que não têm acesso aos canais automáticos, até pela idade dos clientes, acho que deveriam pensar numa forma de otimizar isto...” E1

Um dos entrevistados refere também como fator crítico o texto das questões RGPD que poderá ter de ser adaptado para melhor ser perceptível para alguns clientes:

- “... há clientes para quem provavelmente o que está prescrito é suficiente, mas há outros que obrigariam a existir situações mais específicas e numa linguagem mais abrangente...” E3

É também apontado em duas unidades de registo como fator crítico da sua implementação a necessidade de atuação em 72 horas em caso de incidente de violação de dados pessoais. É também apontado por um dos entrevistados que esta matéria não deve ser uma situação puramente administrativa e que deve haver uma sensibilização de todos os colaboradores.

- “... esse normativo aliás prevê todas estas situações que possam existir e obriga a que estes incidentes sejam tratados dentro de 72 horas que deles tomamos conhecimento, que é outra coisa que também não casa muito bem com as violações de sigilo não é, porque nestes casos o banco vai gerindo, aqui não, eu tenho 72 horas ...” E6
- “... o banco tem que dinamizar um pouquinho mais também a parte de sensibilização das pessoas... isto é um tema que está mais administrativo...” E5

Ainda em relação ao RGPD, isoladamente, é sinalizado como fator crítico a pouca disseminação da utilização da chave móvel digital, que como veremos mais à frente, é apontada como uma importante ferramenta para o aumento da eficiência:

- “... mas a lei portuguesa já consagra que no âmbito da recolha da informação sempre que o cliente der nota que o pretende fazer através da chave móvel digital deve ser disponibilizado... mais uma vez há um problema de operacionalidade disto, porque a chave móvel digital ainda não é uma ferramenta largamente disseminada...” E11

Uma outra situação apontada como fator crítico na implementação do RGPD foi a validação e correção do documento para recolha do consentimento para tratamento de dados que chega ao banco através de parceiros:

- “... e essa adaptação foi feita, também foi feito o reconhecimento, nomeadamente em grandes parceiros do seu próprio RGPD dando nota daquilo que eram correções necessárias para o banco...e por isso posso-lhe dizer que teve impacto na minha atividade, nomeadamente no canal de intermediação de crédito que são os parceiros imobiliários...” E10

Passando agora em particular, e ainda no âmbito da segunda categoria, para os fatores críticos na implementação da LBC/FT, é igualmente referido que houve efetivamente um acréscimo de tarefas e preocupações. Foi sinalizada, nomeadamente nas unidades de registo seguintes, a efetiva necessidade de reajustamentos internos de pessoas e de processos.

- “... quer dizer, há uma série de preocupações que nós temos hoje que não tínhamos há algum tempo atrás... acresce tarefas? claro, porque tem que haver aqui um controlo diário das contas dos nossos clientes...” E2
- “... houve de facto um reajustamento interno, quer em processos quer em pessoas... há uma dinâmica e uma evolução constante que faz com que nos tenhamos que constantemente a adaptar, muitas vezes até mais a reagir...” E11

Tal como no RGPD, foi indicado por um dos entrevistados a dificuldade acrescida nestas matérias no que toca a clientes emigrantes:

- “... vai depender muito da capacidade e da vontade do interlocutor de nos dar essa informação... por exemplo com emigrantes... é difícil a recolha de algum tipo de informações, ou porque não dominam os meios informáticos ou porque nem entendem algumas das expressões...” E3

E se na categoria anterior concluímos pela difícil harmonização entre os diplomas e aferimos o porquê dessa incompatibilidade, nesta categoria - Fatores críticos na implementação (RGPD, LBC e Sigilo bancário) - tentaremos aferir como é que essa (in)compatibilidade se manifesta na prática. Verifica-se em 4 unidades de registo referência à difícil compatibilização, nomeadamente por terem objetivos, princípios e prazos de conservação opostos:

- “... para cumprirmos com a legislação de prevenção de branqueamento de capitais

temos de recolher um mundo sobre o cliente... acaba por, se calhar, ser um bocadinho contra o princípio do RGPD em si, portanto eu vejo-os como incompatíveis nesta perspetiva, ou seja, um caminha para um lado e outro caminha para o lado completamente oposto, mas acho que há formas de compatibilizar q.b....” E5

- “... as questões de BC/FT vivem costas voltadas para as questões da proteção de dados, elas não casam bem... no BC/FT quero saber mais, uma maior informação possível sobre os clientes e não clientes...quero saber de tudo, guardar tudo e durante o maior tempo possível. Na proteção de dados o que é que nos diz? Que só devo recolher aquilo que eu preciso, pelo tempo que eu preciso e só devo usar para isso mesmo. Portanto vivem de costas voltadas umas para as outras e esta conciliação às vezes é difícil sem dúvida nenhuma...” E7
- “... há um risco a gerir que é o risco de BC e esse risco gere-se com informação... portanto eu acho que eles conflituam os dois e não sei como se vão harmonizar...” E11

No sentido da sua compatibilização identificámos 3 unidades de registo que se referem à recolha e tratamento de dados e documentação associada. No âmbito do BC/FT a recolha e tratamento está justificada, independentemente da aceitação ou não do tratamento:

- “... no fundo acho que já está compatibilizado e tens justificação para a recolha por isso acredito que está sempre compatibilizado...” E7
- “... mas acho que havendo conflito aqui deve prevalecer o que mais protege não só as instituições e as pessoas de forma individual, mas a própria sociedade... aqui teremos sempre legitimidade e a CNPD tem dificuldade em refutar que não temos uma lógica muito válida subjacente à recolha desses elementos e da documentação relacionada...” E7

Note-se que a forma de recolha e procedimentos de tratamento de dados no âmbito da LBC/FT não é dada pela lei, sendo este aspeto apontado como um fator crítico da sua implementação, podendo ser mais ou menos invasivo. Acresce que, como sinalizado em mais do que uma unidade de registo, as informações e dados nunca são demais, no que à prevenção de BC/FT diz respeito, senão vejamos:

- “... muitas vezes também criamos processos que não são exatamente aqueles que a lei diz... a lei dá-nos um objetivo que é o combate ao BC/FT, mas não nos diz como é que fazemos e a forma como fazemos, que pode ser mais ou menos invasiva...” E6

Em resumo e sistematicamente os fatores críticos na implementação do RGPD, sigilo bancário e

BC/FT enunciados são:

- ✓ Necessidade de colocar do lado do cliente a decisão sobre a utilização dos seus dados;
- ✓ Adaptação dos sistemas e processos do banco ao RGPD;
- ✓ Necessária atualização dos dados pessoais quanto a esta matéria;
- ✓ Consentimento ou recusa dado através de assinatura do cliente;
- ✓ Existência de acréscimo de trabalho e constrangimentos na recolha do consentimento, na medida em existem muitos clientes, e em especial nos clientes emigrantes;
- ✓ Necessária criação do DPO, conforme imposição legal;
- ✓ Dificuldades na compreensão das perguntas RGPD para alguns clientes;
- ✓ Necessidade de atuação em 72 horas em caso de incidente de violação de dados pessoais;
- ✓ Necessidade de haver uma sensibilização de todos os colaboradores para esta temática;
- ✓ Pouca disseminação da utilização da chave móvel digital para comprovação de dados e consentimento;
- ✓ Necessidade de validação e correção do documento para recolha do consentimento para tratamento de dados que chegam ao banco através de parceiros;
- ✓ Acréscimo de tarefas e preocupações para cumprimento da LBC/FT, em particular em clientes emigrantes;
- ✓ Necessidade de reajustamentos internos de pessoas e de processos;
- ✓ Dificuldades na compatibilização dos regimes, nomeadamente por terem objetivos, princípios e prazos de conservação opostos;
- ✓ Necessidade de recolha e tratamento de dados e documentação associada, no âmbito do BC/FT, que está justificada, independentemente da aceitação ou não do cliente;
- ✓ A forma de recolha e procedimentos de tratamento de dados no âmbito da LBC/FT não é dada pela lei, podendo ser mais ou menos invasiva;
- ✓ Muitos dados e informação a recolher, pois estes nunca são demais, no que à prevenção de BC/FT diz respeito.

Sistematizado este ponto, o seguinte é focado no aumento da eficiência.

4.2.3 Aumento da eficiência associada a dados a recolher, momentos e fluxos

Identificados que estão os principais fatores críticos na implementação dos diplomas, passamos agora para a terceira categoria definida - Aumento da eficiência associada a dados a recolher, momentos

e fluxos. Nesta categoria foram registadas 53 unidades de registo, sendo apenas referidas as que melhor resumem as ações de melhoria propostas no sentido do aumento de eficiência:

- ✓ Criação de alertas por SMS, com avisos para RGPD e atualização de dados a realizar nos canais digitais;

Esta proposta foi sugerida em 4 unidades de registo, veja-se o seguinte exemplo:

- “... eu acho que poderia ser feito uma SMS com um alerta para o cliente fazer nos canais digitais e não ter que se estar à espera do cliente vir ao banco para tratar disso... alguma coisa que fosse mais intuitiva e que alertasse o cliente para essa necessidade...” E1
- ✓ Gravação de chamadas que possam ser usadas como consentimento para RGPD;
 - “... se não passar pelo balcão era muito mais rápido porque uma gravação de 5, 10 minutos e ficava feito já não era preciso da outra parte todo do tratamento processual...” E1
- ✓ Aposta nas chaves móveis digitais e leitura do cartão de cidadão para recolha, tratamento e comprovação de dados;

A proposta anterior contou com pelo menos 5 unidades de registo:

- “... para já aquilo que me ocorre é mesmo a chave móvel digital...” E1
- “... A partir do cartão de cidadão hoje já se conseguem comprovar várias coisas, identificação pessoal, o contribuinte, a morada está tudo já muito facilitado a esse nível...” E4
- “... eu acho que o que podia ser mais simples e que estamos a implementar já é a comprovação de dados através das chaves móveis digitais, que é um passo bastante bom...” E9
- “... a única coisa que eu acho, e já temos essa possibilidade, mas que é pouco utilizada é a chave móvel digital e o cartão de cidadão por PIN e a assinatura... mas os clientes particulares usam pouco...” E10
- “... há pequenas iniciativas que vão com certeza ajudar, como é a questão da chave móvel digital, para evitar que se andem a tirar cópias de documentos...isso também traz benefícios para a própria questão do BC pois a informação por via digital e eletrónica e vir de entidade oficiais, partimos do princípio que é fidedigna e não manipulada, portanto aí há uma melhoria...” E11
- ✓ Assinatura digital para prova do consentimento;

- “... como posso tornar isto mais digital? só mesmo através dos dois fatores, assinatura digital certificado ou PIN do CC, só assim sabemos que foi a pessoa... Portanto só mesmo com uma assinatura, não consigo simplificar mais este processo para garantir que cumpro...” E10
- ✓ Aposta na utilização de fotografias enviadas pela aplicação para comprovação de dados;
 - “... nas aplicações, as fotografias servirem também como comprovativo e a pessoa não ter de se deslocar é uma boa pratica e a informação chega logo, o que torna o processo muito mais célere...” E9
- ✓ Massificação da assinatura digitalizada e fim da assinatura em papel;

Proposta referida por dois dos entrevistados:

- “... poderia ser mais uma situação para se fazer uma assinatura digital, que nós já temos, após preenchimento no sistema, ... e já não nos obrigar a fazer a digitalização, a imprimir, o cliente assinar a ficha de informação individual, que nós digitalizamos e enviarmos para arquivo... já não obrigando a que nós fôssemos fazer digitalizações...” E1
- “... eu acho que se calhar o que podemos fazer é apostar nos canais digitais, na recolha digital, usar tablet, em vez de nos focarmos tanto no papel... acredito que a digitalização possa ser um caminho útil para as primeiras linhas...” E7
- ✓ Necessidade de todos os dados estarem informatizado e ao acesso de todos;
 - “... eu peço os documentos comprovativos de rendimentos, nacionalidades, várias moradas, que me tragam pessoalmente, em papel ou digital, através de *e-mail*...o que acontece é que após introduzirmos a informação informaticamente, porque quanto mais informatizada estiver a informação mais facilmente chegamos a coerências ou incoerências...” E8
- ✓ Evolução operacional na recolha e tratamento de documentos com a criação de nova plataforma que permita a comunicação dos sistemas dos parceiros com o sistema do banco;

Esta proposta e a seguinte relacionam-se com o aumento de eficiência intimamente relacionada com a troca de documentos e dados com parceiros comerciais externos ao banco:

- “... é por *e-mail* ...nós estamos a preparar uma plataforma de comunicação às grandes redes para o fluxo poder ser integrado diretamente...” E10
- “... e depois aquilo que queremos fazer ao longo deste ano é fazer uma evolução para integrar também os documentos ou de uma forma manual ou de uma forma,

enfim com um robô por trás, a fazer a integração dos documentos nas pastas respectivas ...” E10

- ✓ Dados apagados ao fim de 30 dias sem evolução;
- ✓ Aposta na automatização;
 - “... podemos sempre automatizar e é isso que estamos a fazer... há reportes que têm de ser feitos, obrigatoriamente de informação e estamos a automatizá-los, para não haver erros, quebras de sigilo...” E8
- ✓ Parametrização dos sistemas informáticos na identificação de quebras de sigilo e de RGPD;
 - “... e a sistematização de procedimentos internos do banco que irão ajudar a que o próprio sistema tenha menos quebras do sigilo bancário... ou seja se os sistemas do Banco já estiverem pré parametrizados para evitar determinado tipo de situações, de fugas...” E5
- ✓ Criação de plataforma para descarregar documentos enviados pelos clientes, sem intervenção do balcão e do gestor;
 - “... eventualmente só mesmo tendo o cliente alguma plataforma onde pudesse descarregar a informação e que alguém pudesse controlar, confirmar a fiabilidade da documentação e da informação e eventualmente não houvesse intervenção do balcão..., mas acho que é sempre importante passar pelo gestor...” E2
- ✓ Executar a fiabilização dos *e-mails* dos clientes para evitar perdas de informação;
 - “... estamos a tentar desenvolver também a fiabilização dos *e-mails*, quando os recolhemos não é, porque os clientes às vezes enganam-se, escreveu mal ou colaborador engana-se a ouvir..., portanto sim existem coisas que podem ser melhoradas neste nível, estamos num processo de mudança...” E6
- ✓ Assegurar a encriptação de *e-mails* para troca de informação com dados pessoais para entidades externas;
 - “... ter por exemplo os *e-mails* encriptados em vez de *e-mails* simples quando se remete a informação... da parte da informática e sempre a encriptação para proteção desses dados...” E9
- ✓ Necessidade de existência de canais expeditos para todos os colaboradores comunicarem a identificação de melhorias ou deficiências;

No sentido da proposta anterior, a seguinte unidade de registo:

- “... portanto eu diria que... se cada um dos colaboradores, atuar no âmbito do modelo de controlo interno acho que conseguimos sempre corrigir as eventuais fragilidades que existam no sistema...” E7
- ✓ Colocar o tema do RGPD e do consentimento no fluxo de todos os processos;
 - “... eu diria que para assegurar o cumprimento do RGPD é continuar o que estamos a fazer, que é em todos os processos de negócio, ou de crédito, o que seja, a temática do RGPD tem de estar lá. Em todos os produtos, para além da informação contratual tem uma parte para o cliente assinar o RGPD, mesmos nos canais digitais...estar no fluxo...” E9
- ✓ Descentralizar a monitorização dos movimentos de conta;
 - “... o ideal era que não fosse a rede a tratar disso, acho que se conseguíssemos ter alguém no banco a tratar disso era excelente, mas claro que o contacto com cliente tem que ser sempre nosso, nós é que somos os gestores de conta é natural que o contacto e os pedidos sejam nossos...” E2
- ✓ Agilização de processos, mas sem perda de qualidade de informação;
 - “... eu acho que podia ser melhor, que podemos sempre melhorar aqui algumas coisas do ponto de vista processual: uma coisa que depois não implique perda de qualidade da informação que recolhemos... eu acho que é mais nesse sentido, ou seja, em prol de poupar algum tempo, não descurar uma parte que depois é importante para nós e para o banco...” E2
- ✓ Reforço da informação e conhecimento sobre estas matérias para melhor as executar;
- ✓ Incentivar os colaboradores a dar opinião sobre os processos e tarefas em que estão envolvidos;
 - “... acesso a mais informação para quem trata destes assuntos e até dar opiniões sobre melhorias a efetuar... passa tudo pelo acesso ao conhecimento...” E3
 - “... eu acho que era muito importante nós percebermos exatamente aquilo que os colegas precisam e nós tínhamos de ter canais mais diretos com eles...” E8
- ✓ Criação de uma *check-list* para orientar o processo de recolha e uniformização da parte de quem trata, para tornar os processos mais rápidos;
 - “... acho que devia haver uma listagem com aquilo que eles realmente pretendem, e eu acho que também depende um bocadinho de quem trata...que me tenha percebido uns pedem a inscrição no SEF, há outros que não pedem...devia haver um parâmetro para todos e para ser mais fácil chegarmos à aceitação mais rápido possível...” E4

- ✓ Sensibilizar todos os colaboradores para esta temática;
 - “... mas no limite acho que podem desconhecer as consequências das suas ações e se isto não for amplamente divulgado primeiro numa ótica de sensibilização, do que não deve ser feito e avançando depois... do que acontece se for feito, acho que em tudo o que diz respeito a sigilo bancário, RGPD e outros tantos temas acho que é uma coisa que o banco tem imenso para melhorar...” E5
- ✓ Reforço do princípio do *privacy by default*;
 - “... outras é os tipos de dados que nós recolhemos... não vale a pena recolher dados desnecessários ou dados que se desatualizam muito... nesse aspeto o banco tem feito um esforço de só recolher efetivamente aquilo que é necessário, é o princípio do *privacy by default*... os processos do banco estão a ir nesse sentido... a ter essa evolução e portanto nos momentos em que eu recolho os dados, tenho de informar os meus clientes e só devo recolher aquilo que necessito mesmo...” E6
- ✓ Otimização dos processos na fase inicial, a de contacto com o cliente, vai otimizar os processos com os reguladores;
 - “... no fundo se as primeiras linhas tivessem se calhar o trabalho mais eficiente se calhar os resultados que nós temos com os reguladores, os processos não tinham tanto impacto no nosso dia a dia, mas isso é uma questão de otimizar sempre as tarefas de primeira linha e não tanto de segunda...” E7
- ✓ Padronização de tarefas para se seguir para a fase de eliminação de algumas;
- ✓ Definição de todas as tarefas, documentos e fluxos nos processos de KYC e explicar o porquê da sua necessidade;
 - “... no BC/FT, pensando mais na admissão e sendo um tema novo a remediação penso que a partir de agora que já temos definido o que se pretende e que a rede já o conhece a necessidade de conhecer o cliente e perceber o que está em causa e não meramente executar, sabe que cuidados se devem ter...” E9
- ✓ Criação de *task forces* de apoio para explicar os processos e procedimentos necessários à prevenção de BC/FT;
 - “... criámos uma *task force* de apoio à rede comercial para saberem exatamente quais são os documentos que tinham de enviar e como é que se processava basicamente...” E9
 - “... ou até haver um *helpdesk* direto para nós... pessoas formadas e familiarizadas que despachem entre colegas, sem superioridade, tem de haver um espírito comum

de entreajuda...” E8

A unidade de registo anterior é reforçada e complementada por mais 2 unidades de registo que se referem à importância da formação dos colaboradores:

- ✓ Reforço da formação dos colaboradores e explicar o porquê dos processos de BC/FT para melhor serem compreendidos por quem os executa;
 - “... a proposta de melhoria seria a própria formação...” E3
 - “... apostámos fortemente em formação, tínhamos uma colega quase 100% dedicada à formação, um bocadinho mais de topo, mas também à rede comercial...” E9
 - “... explicar o processo, o que tem de se fazer, o que temos de pedir, de enviar... também falar o que é que é isto do BC ... porquê temos de o fazer e o porquê dos procedimentos...” E9
- ✓ Criação de canal para dúvidas com elementos formados e informação na intranet, com alertas para os erros frequentes;
 - “... apostámos também em ter um canal para *compliance* no *helpdesk*, que não havia... agora há uma linha própria com formação aos elementos..., portanto mais canais, formações e informações na intranet cada vez que verificávamos erros frequentes...” E9
- ✓ Reforço dos colaboradores dedicados à análise de processos de prevenção de BC/FT;
 - “... claro habilitar as equipas com mais pessoas para o tratamento, que não estava minimamente dimensionado, mas agora estamos a fazer esse trabalho e também acho que será melhor porque a rede já conhece o processo...” E9
- ✓ Criação de um canal próprio para comunicações com entidades externas;
 - “... as autoridades estão a trabalhar na criação de um canal para estas comunicações, mas ao dia de hoje ainda não existe. Portanto o canal que é disponibilizado para os bancos e outras instituições é o *e-mail*...” E11

A ótica de reforço da confidencialidade dos processos é proposta na unidade de registo seguinte:

- ✓ Evolução do processo de troca de informação e disponível só para quem a trata;
 - “... no sentido que o “GP” possa ser segregado apenas pelo órgão de onde vem a informação, ou seja, a informação só fica disponível para o órgão que a enviou... o processo começou de uma forma muito básica, muito arcaica, mas tem tido várias evoluções... ao dia de hoje é uma das melhorias que podia ser feita...” E11
- ✓ Criação de um canal dedicado à comunicação de operações suspeitas;

- “... sugestões de melhoria seria ter um canal dedicado para as comunicações suspeitas...” E1
- “... questão de construir canais privilegiados para troca de informação é sempre um bom princípio até para a própria gestão de informação, para garantir que existe um repositório dedicado...” E11

E por fim o tempo despendido com os processos que os tornam mais ou menos eficientes, contribuindo mais uma vez a sua automatização para o aumento da eficiência.

- ✓ Maior rapidez no processo de recolha de informação interna e externa através da criação de *robôs*;
 - “... o que estamos a fazer é sobretudo na rapidez de processo, estamos a desenvolver *robôs* para obtermos a informação mais depressa, informação que já está dentro do banco para ela ser recolhida...e informação externa ao banco, ou que está em fonte aberta, no google e por aí, ou que está em determinados sites que nós pagamos... que têm bases de dados...” E11
- ✓ Necessidade de reportes instantâneos às autoridades de controlo;
 - “... no caso de BC/FT eu diria que sim, porque o dever de comunicação é instantâneo..., no RGPD, digamos que nunca acontece instantaneamente...” E5
- ✓ Necessidade de comunicação entre os vários sistemas que guardam dados de clientes;
 - “... existiam aplicações, por exemplo, que recolhiam os mesmos dados e ficavam lá umas e depois outras, elas depois não conversavam... isso era gerador de muitos erros no envio das comunicações...” E6

4.2.4 Redução da eficiência associada a dados a recolher, momentos e fluxos

Identificadas que estão as propostas de melhoria no sentido do aumento da eficiência associada a dados a recolher, momentos e fluxos, faremos de seguida a análise categorial de conteúdo relativamente à quarta e última categoria definida - Redução da eficiência associada a dados a recolher, momentos e fluxos, onde tentámos identificar as tarefas e procedimentos que, por sua vez, reduzem a eficiência.

Foram registadas 29 unidades de registo, que serão apresentadas de forma individual, com recurso a exemplos das unidades de contexto observadas.

A unidade de registo que foi mencionada mais vezes (4) está, precisamente, relacionada com o tempo que é despendido no processo de aceitação de clientes de risco elevado:

- ✓ Morosidade na validação dos processos de aceitação de clientes de risco elevado torna os processos pouco eficientes;

- “... eu perco muito tempo, muito... por exemplo, a minha carteira é basicamente de não residentes estrangeiros... pessoas que têm muitos negócios e várias empresas... existe aqui alguma atenção e capacidade até de compreensão... estar a pedir rendimentos, encaixar isto nos *templates*, naquilo que são os nossos formulários, estar a explicar isto a um colega que analisa depois a informação, que tem de bater toda exatamente com a que está na ficha de informação, com o que está no relatório e bater tudo certo com os documentos de suporte que o cliente nos dá...” E8
- “... única questão que eu sinto é que quando há um cliente novo há demoras significativas na aprovação ou não do cliente... acho que isso é que se poderia efetivamente melhorar, os timings de resposta na análise...” E10
- ✓ Recolha obrigatória da assinatura, com acréscimo de dificuldade em clientes emigrantes e idosos;
 - “... fez com que nós tivéssemos que recolher todos os documentos novamente, com que os clientes tivessem que assinar a ficha de informação porque muitos dos clientes que estão lá fora não vêm cá, não têm a APP nem acesso aos canais digitais foi muito complicado conseguir gerir isso e foi um acréscimo de trabalho muito grave...” E1
- ✓ Relatórios de risco muito extensos;
 - “... termos do relatório de risco que nós temos que preencher... só para imprimir preencher e digitalizar todo esse esse documento acho que é uma burocracia e um acréscimo de trabalho tremendo para os balcões o que nos tira muitas vezes o nosso tempo para outras tarefas que são muito importantes...” E1
- ✓ Recolha de documentos e assinatura presencial, digitalização, envio para tratamento e repetição do procedimento sempre há alterações ou correções;
 - “... é o cliente que nos traz em papel, os originais dos documentos, nós fotocopiamos, a nova ficha de informação individual assinada pelo cliente onde nós preenchemos os dados da relação do negócio... onde o cliente nos diz se vai fazer ou vai receber transferências do estrangeiro, ou não, quais os montantes, de que países é que também vai receber ou fazer... porque motivo... essa informação colocamos também no relatório de risco e depois digitalizamos tudo e é criado um processo e se for risco elevado será enviado para a outra área, que irá analisar e depois se necessário mais algum documento ou esclarecimento é-nos solicitado... e nós temos que responder e sempre que alteramos uma informação qualquer dos dados pessoais do cliente temos que recolher nova ficha de informação individual e digitalizá-la para acompanharem...” E1

- ✓ Problema do extravio dos documentos assinados;
 - “... se tudo correr bem e a ficha não for extraviada no correio... se por acaso a ficha for extraviada isso duplica porque temos que estar a recolher novamente...” E1
- ✓ Utilização de papel e digitalização para os mesmos documentos por medo da perda de informação digital;
 - “... no momento da abertura de conta tudo o que sejam documentos originais normalmente eu tiro sempre fotocópia porque tenho sempre medo da digitalização não funcionar então depois digitalizo, coloco nas pastas para tratamento e coloco na trituradora...” E2
- ✓ Aplicação que gere processos digitais muito morosa, com constantes devoluções por falta de páginas ou de associações erradas às pastas respetivas;
 - “... se calhar podia ser poupado algum tempo depois na parte da digitalização, do arquivo... se não tivesse a nossa intervenção, mas na prática estava ali alguém para analisar com mais calma e guardava e punha nas pastas e depois se se esquece de pôr uma página e tens que fazer outra vez o processo e pronto isso leva tempo quando tens 1500 coisas...” E2
 - “... depois são os processos que são devolvidos várias vezes..., porque não bate, porque falta...” E8
- ✓ A eficiência nos processos está muito dependente da resposta e disponibilidade dos clientes;
 - “... depende de cliente para cliente... há situações que podem ser tratadas em meia hora e outras que levarão duas horas... isto é uma questão até da própria disponibilidade do cliente e da informação que nos presta... porque muitas vezes o que acontece é que o cliente não está nada familiarizado com isto e até nós próprios não fomos suficientemente formados e que vamos ter que questionar mais do que uma vez, quando bastaria uma...” E3
- ✓ Em Portugal o reporte de BC/FT é feita para duas entidades distintas;
 - “... acho que se calhar às vezes poderiam ser ligeiramente mais ágeis, ou seja, digo isto porque em Portugal em concreto cada vez que é preciso fazer uma comunicação de BC/FT ela tem que ser feita a duas instituições, coisa que não acontece noutros países..., portanto se fosse feita a uma instituição só todo o processo seria mais ágil...” E5

Relativamente a esta unidade de registo podemos considerar que é uma constatação que acaba por

ser transversal a todos os bancos em Portugal e que não é apenas uma questão de eficiência, mas da própria eficácia no cumprimento da lei de BC/FT.

- ✓ Regulador por vezes pede informação mais do que uma vez porque os diferentes setores não comunicam entre si;
 - “... eventualmente as dificuldades que sentimos enquanto trabalhamos com mais de um departamento dos órgãos de controlo, que são muito grandes e que eles próprios não comunicam entre si... informação que envias para departamentos diferentes... podia tornar-se mais eficaz se houvesse comunicação interna dos reguladores e a partilha de informação entre os vários departamentos dos reguladores facilitariam a vida às instituições...” E7
 - “... acho que os reguladores/supervisores apesar de terem os canais instituídos quando recebem a informação devia haver uma compatibilização da informação recebida e que fosse acessível aos vários departamentos para tornar o processo com contacto com as instituições mais eficientes...” E7
- ✓ RGPD não é consultado frequentemente porque não é de visualização automática e instantânea;
- ✓ A importância da documentação arquivada não é consensual;
 - “... os colegas que validam a informação em termos de arquivo digital recusam muitas vezes informação que, apesar de não cumprir o que eles têm de aceitar, precisam de perceber que ainda que não cumpra exatamente aquele requisito, é importante para ficar associado ao cliente e isso facilitaria muita coisa em termos de tempo...” E8
- ✓ A dificuldade de comunicação entre as áreas e inexistência de canais diretos;
 - “... com comunicações que só podem acontecer através daquele canal próprio...” E8
 - “... compreendo que não seja possível o envio direto para os colegas, mas facilitaria muito... há um canal intermédio e perde-se muita coisa... há muita coisa que se perde e que não funciona da forma mais eficiente...” E8
- ✓ Mobilidade como inimiga do *KYC*;
 - “... questão de mobilidade que há de estar estudada a nível estratégico, e faz com que não exista conhecimento de cliente absolutamente nenhum...” E8
- ✓ Consulta do BE é feita com os dados pessoais do colaborador e devia ser mais institucionalizado;

- “... nas empresas, a questão do BE, na recolha do RCBE acho que podíamos fazer uma melhoria porque é o balcão que o faz, é um acesso nominativo... acho que é uma situação que podia ser melhorado, que devia ser algo institucional...” E9
- ✓ Dificuldade na padronização dos processos de BC/FT;
 - “... o problema das leis que vão saindo, das inspeções, do regulador e exigências que alteram muito rapidamente e que não dá margem para que se padronize um bocadinho mais os processos... enquanto no RGPD já sabemos o que temos de fazer, e no fundo é desenvolver, no outro é um bocadinho mais complexo...” E9
 - “... em BC/FT obviamente que se podem melhorar os processos, e estamos a fazer por isso, mas não é um caminho fácil porque saem sempre novas leis, novas exigências e depois dependente do que é o cliente, do que ele nos vai enviando pode surgir maior ou menor complexidade...” E9
- ✓ Repetição dos pedidos de elementos de identificação;
 - “... os vários elementos de identificação naquilo que a lei chama o momento do estabelecimento da relação de negócio... pensando bem até repetitiva...” E11
- ✓ Utilização de *e-mails* encriptados como forma de comunicação com as autoridades;
 - “... feito por *e-mail* ... os portugueses estão muito atrasados... a informação vai encriptada e com password... com a encriptação a informação julgamos que ela vai de forma minimamente segura...” E11
- ✓ Informação trocada por *e-mail* leva à sua dispersão e falta de concentração;
 - “... inicialmente fazia-se por *e-mail*, onde a informação se dispersa e a informação não fica concentrada...” E11
- ✓ O software que já existe noutros países será difícil de aplicar porque não está adaptado à comunicação para duas entidades;
 - “... este software que já existe e que está implementado numa série de países só está dedicado para receber para uma entidade e adaptá-lo para receber para duas entidades é complicado...” E11

A análise de conteúdo das entrevistas ora realizada já nos permitiria retirar algumas conclusões no que toca à identificação dos principais elementos geradores de maior ou menor eficiência, mas antes de avançarmos para estas conclusões necessário será realizar a análise de conteúdo da pergunta aberta realizada através dos questionários: “10.1. Existem dificuldades práticas na implementação dos diplomas (RGPD, Lei de combate ao Branqueamento de Capitais e Sigilo Bancário)? Sim/Não 10.2.; Porquê?”. Responderam positivamente 47 dos inquiridos, mas apenas 25 responderam ao “Porquê?”.

Da análise das 25 respostas verifica-se que todas vão no mesmo sentido das obtidas nas entrevistas.

Vejam os:

- ✓ Morosidade no tratamento dos processos
 - “Processos complexos e burocráticos, deveriam ser mais ágeis”.
 - “Processo muito complexo e burocrático. Deveria ser automatizado de forma que as respostas fossem feitas online pelo cliente numa base de dados alterável...”.
 - “Matéria complexa”.
 - “Muitas situações difusas e de elevada complexidade”.
 - “... por vezes os clientes não estão na posse de toda a documentação (nomeadamente os emigrantes) o que dificulta muito os processos tornando-os muito morosos, levando a uma grande perda de tempo e sinergias para a nossa atividade principal”.
 - “... nem sempre os clientes entendem o grau de importância... exigem que facilitemos e agilizemos as questões operativas”.

- ✓ Alterações legislativas que conduzem a reajustamentos e alterações dos processos para que estejam em conformidade
 - “Constantes atualizações”.
 - “Porque são diplomas muitos complexos, muito técnicos, com muitas obrigações para as partes envolvidas e com muita legislação avulsa que tem de ser tida em consideração”.
 - “Nem sempre é fácil para as organizações acompanharem as muitas alterações legislativas e em algumas situações... na prática é complicado executar”.
 - “Principalmente para o cliente, muita alteração foi implementada e a ideia que fica é a falta de confiança... não é a ideia de segurança e conforto, mas a desconfiança que alastra”.

- ✓ Sistemas de informação que, apesar de existirem, nem sempre correspondem às necessidades dos colaboradores
 - “Informação por vezes difusa”.
 - “Muitas dificuldades prendem-se com os sistemas ineficientes”.

- “Sistemas informáticos e comunicações com os clientes”.
- “RGPD: a implementação de determinadas medidas técnicas acaba por se tornar difícil do ponto de vista operacional”.
- ✓ Necessidade de reajustamentos internos de pessoas e de processos
 - “Qualquer diploma deste género requer a disponibilização de recursos (tempo/pessoas), definição/implementação de circuitos, por forma a garantir a conformidade com a legislação na estrutura da organização”.
- ✓ Necessidade de colocar do lado do cliente a decisão sobre a utilização dos seus dados
 - “Clientes pouco informados não querem partilhar informação sobre rendimentos e património para efeitos de prevenção de BC/FT, que é confundida com a informação para efeitos de base de dados para obtenção de informação com vista a uma oferta específica/vendas direcionadas”.
 - “Mas há muitos clientes/pessoas que não têm noção destes aspetos e por vezes recusam-nos sem ter a consciência dessa decisão”.

Em resumo, conclui-se que existem 5 pontos em comum nas entrevistas e questionários que são geradores de ineficiência ou pelo menos redutores da eficiência:

- ✓ Morosidade no tratamento dos processos;
- ✓ Alterações legislativas que conduzem a reajustamentos e alterações dos processos para que estejam em conformidade;
- ✓ Sistemas de informação que, apesar de existirem, nem sempre correspondem às necessidades dos colaboradores;
- ✓ Necessidade de reajustamentos internos de pessoas e de processos;
- ✓ Necessidade de colocar do lado do cliente a decisão sobre a utilização dos seus dados.

Os respondentes também se pronunciaram relativamente ao “como” aumentar a eficiência da compatibilização operativa, prática, dos diplomas, destacando-se a necessidade de mais formação aos colaboradores, conforme já tinha sido indicado pelos inquiridos nas entrevistas. Adicionalmente foram ainda sinalizados:

- ✓ Conjugação das obrigações decorrentes do RGPD com o tratamento de dados

decorrentes da função de *compliance* ao abrigo dos artigos 54.º, 57.º, 58.º e 59.º da Lei de BC/FT;

- ✓ Vedar a consulta e tratamento de dados resultantes de procedimentos relacionados com a prevenção de BC/FT;
- ✓ Melhorar a explicação aos clientes acerca dos fundamentos das questões que lhes são colocadas;
- ✓ Maior conhecimento da legislação (que está relacionado com a formação já referida);
- ✓ Mudança das leis de prevenção de BC/FT.

De forma a perceber se as principais conclusões retiradas da análise de conteúdo têm ou não consistência recorreu-se também à análise quantitativa, desta feita tendo por base apenas os inquéritos realizados.

4.3 Análise quantitativa

A análise quantitativa de dados começou pela caracterização dos respondentes. Para a análise de dados existiu recurso às aplicações SPSS, versão 27 e JAMOVI, versão 2.2.5. A opção de recurso a estas duas aplicações foi confirmatória e centrada no facto do JAMOVI ser um *software* livre e que possui um *layout* mais intuitivo, comparativamente ao apresentado pelo SPSS. O uso do JAMOVI foi confirmatório.

Responderam ao questionário 77 pessoas, 46,8% do género masculino e 53,2% do género feminino. Quanto à idade, prevaleceu a faixa etária compreendida entre os 40 e os 49 anos, inclusive, com 55,8%, seguida da faixa etária compreendida entre os 50 e os 59 anos de idade, inclusive, com 23,4% e, finalmente, em terceiro lugar, a faixa etária compreendida entre os 30 e os 39 anos, inclusive, com 18,2%. Dessa forma, apenas 2,6% dos respondentes tinham menos de 30 anos. Aqui a média de idade situou-se nos 44,58 anos, com um desvio padrão de 6,317. Já no que respeita à antiguidade na banca é de salientar o facto de 44,2% dos questionados exercer atividade na banca num período compreendido entre os 20 e os 29 anos, inclusive, seguindo-se o intervalo de antiguidade compreendido entre os 10 e os 19 anos, inclusive, com 36,4%. Aqui a média da antiguidade situou-se nos 19,25 anos, com um desvio padrão de 7,004. No âmbito das habilitações detidas, a maioria dos respondentes apresentava bacharelato ou o ensino secundário, 59,7% e 16,9%, respetivamente. A maioria dos questionados, concretamente 61%, enquadraram-se na área comercial, seguindo-se os respondentes enquadrados na área de *compliance*, com 23,4%.

Efetuada a caracterização sumária dos respondentes, seguidamente, procurou-se entender se os fatores género, idade, antiguidade na banca, habilitações e área funcional, apresentavam diferenças na perceção de compatibilização do RGPD com a Lei de combate ao BC/FT e com o sigilo bancário.

Para procurar aferir a existência de diferenças significativas entre grupos, começou por se entender se poderiam ser aplicados aqui testes paramétricos, ou não. É que para se aplicarem testes paramétricos, nomeadamente o teste t (para dois grupos) ou o teste anova de uma via (para três ou mais grupos), importa começar por confirmar a existência de normalidade das distribuições. E ainda que, no caso, a variável dependente seja uma variável categórica ordinal e não uma variável quantitativa. Inicialmente considerou-se, dada a amplitude da variável categórica ordinal, que, caso fosse verificada a normalidade, poderia fazer sentido aplicar também testes paramétricos, ainda que completando sempre essa análise com pelo menos uma alternativa não paramétrica.

Acresce que, para avaliar a normalidade com recurso ao SPSS é usual recorrer aos testes Kolmogorov-Smirnov e Shapiro-Wilk. O teste Kolmogorov-Smirnov, ainda que possa apresentar menor eficiência comparativamente ao teste Shapiro-Wilk, pode ser mais ajustado porque o N é menor que 100, neste caso de estudo o N é de 77. Assim, recorreu-se ao SPSS por apresentar os dois testes lado a lado, comparativamente ao JAMOVI que destaca o teste Shapiro-Wilk.

O teste de normalidade Kolmogorov-Smirnov assume as duas hipóteses seguintes:

- H0: a distribuição é normal;
- H1: a distribuição não é normal.

O mesmo é dizer que quando *sig* (*p-value*) for maior que 0,05 a distribuição é normal e quando *sig* (*p-value*) for menor que 0,05 a distribuição não segue uma distribuição normal. Dessa forma, testada a normalidade da variável dependente “V6_Perc_compatib” com os primeiros cinco fatores, concretamente, “V1_Genero”, “V2_Idade”, “V3_Anos_Banca”, “V4_Habilita” e “V5_Funcoes”, foi verificado que o pressuposto de normalidade não era observado para a grande maioria dos grupos, pois foram obtidos valores de *sig* menores que 0,05 para a maioria das situações. Adicionalmente o procedimento foi repetido, após agrupamento em classes e recodificação das variáveis “V2_Idade” e “V3_Anos_Banca” para “V2_Idade_recod” e “V3_Anos_Banca_recod”. Com recurso a essa recodificação foram criados quatro grupos por variável. Contudo, embora este procedimento tenha aumentado o número de grupos onde se comprovou a normalidade, a análise de dados continuou sem permitir assegurar a normalidade na esmagadora maioria das situações. Adianta-se igualmente que, neste caso, também os resultados do teste Shapiro-Wilk conduziram às mesmas conclusões, onde os valores de significância sempre se mantiveram abaixo de 0,05, na maioria das ocorrências.

Consequência do exposto, o procedimento seguinte consistiu na aplicação de testes não paramétricos. A alternativa não paramétrica ao teste t, usada para comparar dois grupos independentes, como forma de detetar diferenças estatisticamente significativas, foi o teste U de Mann-Whitney, na medida em que se trata de um teste de “utilização preferível ao teste t quando há violação da normalidade, ou quando os N são pequenos, ou ainda quando as variáveis são de nível pelo menos ordinal” (Pestana & Gageiro, *Análise de Dados para Ciências Sociais*, 2005, p. 444).

O teste U de Mann-Whitney foi usado para avaliar as hipóteses H1.0 e H1.1. Foi usado nesta dissertação para comparar dois grupos independentes, no caso, tendo por base a variável "V1_Genero", já que as restantes situações, que têm por base as variáveis "V2_Idade_recod", "V3_Anos_Banca_recod", "V4_Habilita" e "V5_Funcoes", implicam sempre a existência de 3 ou mais grupos.

Observou-se um valor de *sig* (*p-value*) de 0,139 (conforme anexo X) logo maior que 0,05, pelo que não é possível rejeitar a hipótese nula, hipótese que assume que não é possível afastar o facto de existir igualdade na distribuição dos grupos, que o género masculino ou feminino, não apresenta diferenças estatisticamente significativas na perceção de compatibilização dos três referenciais (Regulamento Geral de Proteção de Dados, Lei de combate ao Branqueamento de Capitais e Sigilo Bancário).

Já para as variáveis "V2_Idade_recod", "V3_Anos_Banca_recod", "V4_Habilita" e "V5_Funcoes", existiu recurso ao teste de Kruskal-Wallis (conforme anexo XI). Neste âmbito, as hipóteses consideradas foram as mesmas que se consideraram para o teste U de Mann-Whitney, hipóteses H1.0 e H1.1, mas, naturalmente, aplicado a situações onde existiam três ou mais grupos. Observaram-se aqui os valores de *sig* (*p-value*) de 0,328, 0,560, 0,167 e 0,260, respetivamente, pelo que também aqui não foi possível rejeitar a hipótese nula, que enquadra a existência de igualdade na distribuição desses grupos.

No domínio da estatística descritiva e para avaliar as hipóteses H2.0 e H2.1. e tendo em consideração a variável "V6_Perc_compatib", os respondentes assumiram a perceção de compatibilização dos referenciais legais com as pontuações 6, 7 e 8, respetivamente, na proporção de 16,9%, 19,5% e 27,3%. Já quanto à aplicação operativa, 55,8% classificam-na como difícil e apenas 44,2% a classificam como aplicação operativa fácil. Ao se cruzarem estas duas variáveis observa-se que nos três casos, onde os respondentes classificaram a compatibilização com a pontuação 6, 7 e 8, em todos eles existiram 9 respondentes que classificaram essa aplicação como difícil, enquanto 4, 6 e 12, respetivamente, a classificaram como fácil. Estes valores denotam a dualidade de, por um lado, existir a necessidade de cumprimento dos normativos legais e, por outro, desse cumprimento nem sempre ser uma tarefa operativa fácil.

Relembra-se o facto de uma das razões justificativa deste trabalho é ter ponderado a eventual dificuldade operativa para compatibilizar o RGPD, com a Lei de Combate ao Branqueamento de Capitais e com o Sigilo Bancário. Ora as respostas dadas pela maioria dos questionados aponta para essa dificuldade, no âmbito descritivo, ainda que numa proporção de apenas 55,8%.

Quanto ao procedimento seguinte, consistiu na aferição da consistência dos itens usados para explicar o grau de dificuldade na compatibilização operacional. Foi por isso usado o teste Alfa de Cronbach para avaliar a consistência dos itens, variáveis V_8.1 a V_8.9, inclusive. Para perceber como

poderia ser aumentada a confiabilidade e, conseqüentemente, o valor do coeficiente Alfa de Cronbach, no SPSS, foi selecionada a opção “*scale if item deleted*”. O procedimento foi remetido na aplicação JAMOVI e confirmada a obtenção dos mesmos resultados. Por outro lado, ao se constatar que todos os valores do coeficiente eram aceitáveis e se encontravam acima de 0,723, a opção foi de mantê-los a todos. Mantendo-os a todos, o coeficiente Alfa de Cronbach baseado nos itens padronizados apresentou o valor de 0,773, atestando assim a existência de boa consistência entre itens.

O procedimento descrito no parágrafo anterior foi repetido para avaliar a consistência das variáveis “V_9.1” a “V_9.10”. Estes itens focam a potenciação da eficiência. Acresce o facto de a variável “V9_Eficiencia” ter resposta afirmativa para 93,5% dos respondentes, isto é, dos 77 apenas 5 indicaram não ser possível aumentar a eficiência operativa na compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário. Ao ser aqui calculado o coeficiente Alfa de Cronbach, as estatísticas de confiabilidade apresentaram o valor de 0,781 baseado nos itens padronizados. Por outro lado, ponderada a eliminação de itens, apenas se eliminado item “V_9.3” o valor do coeficiente aumentaria para 0,785, não justificando assim tal eliminação, atendendo ao pequeno aumento.

Quanto à comparação dos grupos que consideram a aplicação do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário, fácil ou difícil, e aos fatores críticos na implementação, recorreu-se aqui também ao teste U de Mann-Whitney. Recurso que foi repetido para os grupos que indicaram que a eficiência poderia ser potenciada, comparativamente aos que negaram essa possibilidade. Neste último caso foram tidas em conta as variáveis “V_9.1” a “V_9.10” enquanto no primeiro caso as variáveis “V_8.1” a “V_8.9”.

Em todas as variáveis, da “V_8.1” à “V_8.9” foram obtidos valores de sig (p-value) superiores a 0,05. Em concreto, foram obtidos os valores de 0,504, 0,437, 0,756, 0,937, 0,987, 0,331, 0,185, 0,366 e 0,062, respetivamente (conforme Anexo XII). Quanto às variáveis, da “V_9.1” à “V_9.10” foram também obtidos valores de sig (p-value) superiores a 0,05. Em concreto, foram obtidos os valores de 0,528, 0,876, 0,819, 0,177, 0,496, 0,239, 0,065, 0,130, 0,047 e 0,108, respetivamente (conforme Anexo XIII).

A análise às respostas das questões compreendidas entre a questão “V7_Compatibilizacao” e a questão “V_9.10” recorreu ainda a tabelas cruzadas, no sentido de permitir relacionar as dimensões quantitativa e qualitativa do estudo de caso onde, entre as questões “V7_Compatibilizacao” e “V_8.9”, se enumeraram fatores críticos de implementação, fatores que podem facilitar ou dificultar essa implementação e, posteriormente, entre as questões “V9_Eficiencia” e “V_9.10”, enumeraram-se elementos que podem potenciar, ou não, a eficiência. De referir que estas questões quantitativas são seguidas de uma questão qualitativa disponibilizada com recurso ao questionário que procurava sinalizar dificuldades práticas e fundamentos para a sua enunciação.

Assim, no que respeita às questões compreendidas entre “V7_Compatibilizacao” e “V_8.9”, as tabelas cruzadas permitem observar que na escala *Likert* de 6 pontos utilizada (em que 1 significa “Discordo Totalmente e 6 “Concordo Totalmente”) os respondentes concentraram as suas repostas maioritariamente nos pontos 4 e 5, demonstrando a tendência para a concordância para os pontos escolhidos como indicadores de fatores críticos e que tiveram origem nos fatores indicados pelos entrevistados. Esta tendência para a concordância não apresenta diferenças entre os respondentes que consideram a compatibilização “fácil” ou “difícil”, permitindo concluir que mesmo aqueles que consideram “fácil” a compatibilização no domínio operativo, identificam, sensivelmente na mesma escala, os mesmos fatores críticos.

Em cada um dos 9 fatores críticos identificados as percentagens mais altas de concordância situam-se entre os 30% e os 40%, sendo as mais expressivas em “V_8.1” com 38,2% dos respondentes, que consideram a compatibilização fácil, no ponto 5 e em “V_8.3” com 37,2% dos respondentes que consideram a compatibilização difícil também no ponto 5.

Acima dos 40%, mas sem chegar aos 50% observa-se “V_8.4”, “V_8.5” e “V_8.7” com a mesma exata observação, ou seja, as três com 41,2% dos respondentes que consideram a compatibilização fácil, no ponto 4. Estes fatores referem-se respetivamente à necessidade de formação, tempestividade e elevado número de dados a recolher. Com 44,1% dos respondentes que consideram a compatibilização fácil no ponto 4 destaca-se a “V_8.6” que se refere à linguagem dúbia nos reportes de BC/FT e com 47,1% destacam-se os respondentes que consideram a compatibilização fácil no ponto 4 “V_8.8”, que se refere à padronização de processos de BC/FT.

Contrariamente ao expectável, o único fator crítico que não apresentou qualquer percentagem acima dos 30% foi “V_8.9”, com 29,4% dos respondentes que consideram a compatibilização fácil no ponto 4 e 29,9% dos respondentes que consideram a compatibilização difícil no ponto 5. Na análise de conteúdo das entrevistas esta foi a unidade de registo que foi mencionada mais vezes (4) está, precisamente, relacionada com o tempo que é despendido no processo de aceitação de clientes de risco elevado.

Já no que respeita às questões que emolduram a eficiência na aplicação do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário, questões “V9_Eficiencia” e “V_9.10”, observa-se que apenas 5 dos respondentes não consideram que, num domínio operativo, prático, a eficiência na compatibilização dos normativos possa ser potenciada. Nas entrevistas todos, sem exceção, responderam pela possibilidade de potenciação da eficiência.

Também neste ponto as tabelas cruzadas permitem observar que na escala *Likert* de 6 pontos utilizada (em que 1 significa “Discordo Totalmente e 6 “Concordo Totalmente”) os respondentes concentraram as respostas maioritariamente nos pontos 4 e 5, demonstrando a tendência para a concordância para os pontos escolhidos como indicadores de fatores que permitem o aumento da

eficiência que tiveram origem nos fatores indicados pelos entrevistados. Contrariamente às questões compreendidas entre “V7_Compatibilizacao” e “V_8.9”, não se verificou totalmente a tendência para a concordância entre os respondentes que responderam “sim” ou “não”, pois em 4 dos 10 fatores os respondentes do “não” apresentam percentagens acima dos 40% entre os pontos 1 e 3 na escala de *Likert*.

Em cada um dos 10 fatores identificados como potenciadores de eficiência as percentagens mais altas de concordância relativamente aos respondentes do “sim” situam-se entre os 20% e os 30%, sendo as mais expressivas em “V_9.2” com 47,2% dos respondentes no ponto 5 e em “V_9.3” com 38,9% dos respondentes também no ponto 5. O fator referido em “V_9.2” refere-se à consulta mais rápida do consentimento RGPD associado a cada cliente, sendo um fator que não foi enfatizado nas entrevistas, já o fator da “V_9.3” refere-se ao extravio de documentos, preocupação bem acentuada nas entrevistas.

4.4 Síntese

A análise qualitativa permitiu nesta dissertação sistematizar elementos que respondem à questão de investigação que foca a forma como pode ser maximizada a eficiência.

Já a questão centrada na aferição de diferenças entre grupos foi respondida com recuso à análise quantitativa, onde foi possível testar as hipóteses assumidas.

Consequência do que se indicou, por opção, esta síntese não é ampliada e as respostas são apresentadas no capítulo seguinte.

5. Conclusões

O presente capítulo pretende, em forma de conclusão, referir os pontos principais do presente estudo, tentando responder às questões de investigação, referindo os nossos resultados e o seu alinhamento com os objetivos e sequência de procedimentos desenvolvidos. Far-se-á também menção às limitações encontradas na realização do estudo de caso, bem como se indicarão alguma ideias para eventuais futuras investigações.

Espera-se que com o presente estudo seja dada uma contribuição positiva à instituição bancária que foi objeto deste estudo de caso, e por analogia, a qualquer instituição bancária em Portugal. Essa contribuição dá-se essencialmente pela tentativa de prossecução de processos mais simplificados, automatizados e céleres, e por isso mais eficientes.

À comunidade académica também se espera dar uma contribuição positiva, na medida em que poderá ser um ponto de referência e eventual fonte de revisão de literatura no que toca às temáticas de RGPD, Sigilo Bancário e BC/FT, enquanto matérias que se podem estudar em simultâneo e não só de forma desagregada, como até agora.

5.1 Resposta às questões de investigação

O nosso estudo focou-se na atividade de um banco, entidade privada que tem como seu objetivo primordial a obtenção de lucro. A contabilidade de gestão ou de custos, subsistema da contabilidade em que pretendemos integrar a nossa análise, é direcionada para o interior da entidade, e ajustável a cada realidade e aos objetivos a alcançar. Os bancos lidam diariamente com inúmeras questões e decisões que afetam diretamente a gestão da organização como sejam a concorrência, as necessárias adaptações a um mercado cada vez mais digital, as exigências e necessidades dos clientes, os produtos bancários, as estratégias de venda e de *marketing* e o necessário cumprimento das obrigações legais a que estão sujeitos. A necessidade de possuírem informação relevante e o controlo de custos e recursos, na ótica da eficiência, são essenciais à tomada de decisões na prossecução do objetivo da geração de lucro para os seus acionistas.

O presente trabalho pretende assim responder a duas questões de investigação, tendo sido utilizada como estratégia de investigação o estudo de caso único, de natureza mista, aplicado no Banco BPI S.A, Grupo *Caixabank*. Como fontes de informação foram utilizadas a observação, a análise documental e de registos de entrevistas semiestruturadas gravadas e inquéritos por questionário. Seguidamente, a informação foi tratada com recurso à estratégia da análise categorial de conteúdo e análise estatística, o que nos permitiu não só responder às questões de investigação, como atingir os objetivos gerais e específicos propostos.

5.1.1 Questão 1

Relativamente à primeira questão “Como maximizar a eficiência na compatibilização da operacionalização do RGPD, com o sigilo bancário e com as restrições inerentes ao branqueamento de capitais, na entidade bancária objeto de estudo?” foram reunidas, e já antes descritas, algumas propostas de melhoria em termos de procedimentos internos e sistemas de informação, bem como identificadas situações potencialmente geradoras de ineficiência, principalmente as que tornam os processos lentos.

Na verdade, e antes de responder em concreto à primeira questão, consideramos que importa referir o seguinte:

A nossa dissertação ocorreu numa fase em que a entidade bancária em estudo estava já a desenvolver grandes alterações em matérias de BC/FT, precisamente numa ótica de “fazer mais com menos” e de cultura de *compliance* transversal a todo o banco. Tem existido um esforço na melhor e mais eficiente utilização dos recursos e na alteração e simplificação de processos (algumas das propostas estavam já em curso e ou iniciaram-se no decorrer do presente estudo), exemplo disso é a utilização de robôs, de *machine learning* e de processos automáticos de atualização de dados. Os processos de *compliance* pretendem-se mais ágeis, modernos e omnipresentes, como já vem acontecendo com o RGPD, ou seja, todos os processos de *compliance* tendem a estar alinhados com os processos do banco, com o desenvolvimento informático e com os objetivos do banco, que é fazer negócio e gerar lucro para os seus acionistas.

No nosso estudo pudemos aferir que a área comercial ainda considera que os procedimentos obrigatórios em matéria de BC/FT são tarefas muito burocráticas e administrativas e que tiram tempo à sua atividade principal que é o atendimento comercial e a venda ao cliente. Assim, e como forma de aumentar a eficiência é importante que esta área tenha mais informação e formação quanto à necessidade de cumprimento dos normativos de BC/FT e clara noção das consequências do seu incumprimento para o banco e para os colaboradores. Para além da padronização dos processos e da constante melhoria dos sistemas informáticos é importante que exista uma verdadeira cultura de *compliance* transversal a toda a instituição. A rede comercial é a primeira linha de contacto com o cliente e a primeira que trata dados, dados estes sem os quais não é possível gerir o risco de *compliance* e manter uma relação de negócio.

A legislação de BC/FT tem de ser escrupulosamente cumprida e estar harmonizada com a matéria da proteção de dados pessoais. Existem sim, e já foram sinalizadas, exceções previstas nos normativos que permitem derrogar os princípios do RGPD, no caso concreto. Só uma alteração legislativa a qualquer um dos normativos permitiria que a situação fosse diferente, existindo obviamente argumentos a favor e contra a primazia de um dos institutos sobre o outro, tendo em conta os seus princípios estruturantes.

Em concreto, respondendo à primeira questão de investigação e tendo em conta a sistematização de dados que resultou da análise qualitativa, a eficiência pode ser potenciada, consumindo menos recursos para fazer o mesmo ou quando consumindo os mesmos recursos é possível fazer mais, sendo

nesta dissertação relevadas as seguintes formas:

- Atualização de dados e consentimento RGPD a realizar nos canais digitais, o que evita o processo de recolha e digitalização de documentos, de assinatura e deslocação ao balcão. Exemplo disto é a aceitação de documentos digitalizados ou fotos através dos canais digitais;
- Massificação da assinatura digital e chave móvel digital, o que evita uma vez mais a deslocação ao balcão, para assinatura de formulários. A título de exemplo, qualquer alteração que seja feita na base de dados dos clientes necessita de uma assinatura em papel. Ao ser permitido o envio, via canais digitais, com aceitação da leitura do cartão de cidadão, ou documento assinado digitalmente, seja com recurso a cartão de cidadão ou chave móvel digital, seria evitada, não só a deslocação ao balcão, como todo o processo subsequente de tratamento de formulários, desde a digitalização até ao envio do documento físico para arquivo. Esta situação pode evitar várias horas de trabalho;
- Substituição do formulário RGPD por gravação de chamada, o que evita a deslocação ao balcão e o processo subsequente de recolha de assinatura e digitalização. Por exemplo em clientes mais idosos ou avessos à utilização dos canais digitais, a possibilidade de autorizar, ou não, o tratamento de dados por telefone e em chamadas gravadas, pode simplificar a interação com clientes e reduzir tempo de trabalho ao banco;
- Uniformização, através de publicação em diploma legal, dos procedimentos de tratamento de dados no âmbito da lei de BC/FT. Isto porque não há definição legal dos procedimentos em concreto (podendo estes ser mais ou menos invasivos) mas, a existir, evita ou pelo menos minimiza a discricionariedade e tratamento de dados desnecessário, otimizando processos de trabalho;
- Massificação da assinatura eletrónica porque esta é efetuada por ficheiro, independentemente do número de páginas que esse ficheiro apresente, e não uma a uma. Exemplo disto é a ficha individual de cada cliente que tem várias páginas que têm de ser digitalizadas e enviadas para arquivo físico, esta alteração consubstancia uma redução de várias tarefas e a consequente redução do tempo despendido;
- Colocar o tema do RGPD no fluxo de todos os processos e permitir que tal tema seja propagado entre processos. A título de exemplo na contratação de um seguro o tema do RGPD estar disponível para consentimento e este seja propagado aos restantes processos futuros, e tendo em conta que a qualquer momento pode ser retirado, ou alterado, pelo cliente;
- Criação de uma *check-list* de tarefas e documentos a recolher em procedimentos

decorrentes do cumprimento da legislação de BC/FT, o que evita a devolução de processos incompletos, tornando-os mais rápidos. A verificação de todos os passos e documentos a recolher diminui a devolução de processos incompletos ou mal instruídos, e a sua repetição. Como alternativa à *check-list* o uso exclusivo de formulários digitais que apenas permitam a submissão depois de validado o preenchimento pode igualmente ser uma medida capaz de limitar a submissão de processos incompletos;

- Reforço do princípio do *privacy by default* pois evita a recolha de dados desnecessários ou que rapidamente se desatualizam. Como exemplo podemos identificar a existência, ou não, de carro ou habitação própria, que atualmente, à data de finalização desta dissertação, até já não são dados a recolher;
- Criação de um canal próprio para comunicações com entidades externas, evitando a dispersão de informação nas trocas de *e-mails*. Não só está em causa a questão da segurança na troca de informação confidencial como a possibilidade de estar agregada toda a informação relativa a um processo. Esta alteração permite o acesso a quem possa e necessite interagir no processo e não só aos remetentes e destinatários dos *e-mails* trocados;
- Utilização de *robôs* o que torna o processo de recolha de informação interna e externa muito mais rápida e segura. Desta forma a pesquisa e recolha de informação é feita automaticamente e de forma estruturada, uma vez que um sistema informático apenas se reporta ao que está programado para executar e não se dispersa com dados que não são essenciais;
- Comunicação entre os vários sistemas que guardam dados de clientes, reaproveitando dados que já estão arquivados, evitando a repetição do envio por parte do cliente. Por exemplo, os dados recolhidos no âmbito de um processo de crédito de um não cliente e que são inseridos nesse processo, como o recibo de vencimento ou o cartão de cidadão, possam ser propagados aos outros sistemas e evitando nova recolha, no momento da abertura da conta. Naturalmente que esta medida implica o alargamento do consentimento informado inicial, que poderá, a qualquer momento, ser alterado pelo cliente;
- Reforço das aplicações informáticas de arquivo digital e, conseqüentemente, fim da utilização de fotocópias para os mesmos documentos, evitando a duplicação de tarefas. O receio da perda de informação digital, que obriga a nova recolha, evita-se com um sistema de arquivo digital que pode conter mecanismos redundantes a acionar em caso de quebra de segurança;
- Alteração legislativa que preveja que os reportes no âmbito do BC/FT sejam feitos a uma única entidade, ou num único formulário eletrónico que possa, depois, ser tornado

acessível a uma ou a várias entidades. Esta alteração permite a futura utilização de *software* avançado de troca de informação, que já existe noutros países;

- Comunicação entre os diferentes setores dos reguladores o que evita que estes solicitem a mesma informação mais do que uma vez. Esta proposta sai obviamente fora do âmbito interno da entidade uma vez que é uma alteração que se propõe ao nível das entidades de reporte, ainda que a alteração provoque nos bancos uma redução das tarefas associadas a cada processo.

Sistematizada a resposta à questão um o ponto seguinte responde à questão dois.

5.1.2 Questão 2

Quanto à segunda questão, especificamente, “existem diferenças entre grupos quanto à forma como percecionam a compatibilização, esforço requerido e a eficiência de aplicação do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário”, foram consideradas as hipóteses e obtidas as seguintes conclusões:

- H1.0: existe igualdade na distribuição dos grupos quanto à perceção de compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário;
- H1.1: existem diferenças na distribuição dos grupos quanto à perceção de compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário.

Não foi possível rejeitar a hipótese nula, pelo que se conclui pela não existência de diferenças entre os grupos quanto ao reconhecimento da dificuldade de compatibilização dos três referenciais.

- H2.0: existe igualdade na distribuição dos grupos quanto ao reconhecimento da dificuldade na compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário;
- H2.1: existem diferenças na distribuição dos grupos quanto ao reconhecimento da dificuldade na compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário.

Não foi possível rejeitar a hipótese nula, pelo que se conclui pela não existência de diferenças entre os grupos quanto à perceção de compatibilização dos três referenciais.

- H3.0: existe igualdade na distribuição dos grupos quanto à eficiência na compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário;

- H3.1: existem diferenças na distribuição dos grupos quanto à eficiência na compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário.

Não foi possível rejeitar a hipótese nula, pelo que se conclui pela não existência de diferenças entre os grupos quanto à eficiência na compatibilização dos três referenciais.

Apresentadas as respostas às questões de investigação desta dissertação, no ponto seguinte assinalam-se as limitações e apresentam-se as perspectivas de investigação futura.

5.2 Limitações e investigação futura

Durante a realização do presente trabalho foram encontradas diversas limitações, muitas delas que já eram esperadas desde o início, mas faremos referência apenas às mais significativas.

Uma das limitações resultou da pandemia de COVID-19 que alterou rotinas e restringiu a disponibilidade das pessoas. Esta limitação foi contornada com recurso à realização das entrevistas através da aplicação *Teams*, elemento que supriu a impossibilidade de realização das entrevistas presenciais.

O facto de a temática ser vasta e implicar a leitura, estudo e análise de muita legislação também constituiu um obstáculo. Particularmente se considerado o facto do RGPD traduzir legislação relativamente recente e ainda não muito estudada na comunidade científica. Ainda que também a legislação de enquadramento do BC/FT esteja em constante atualização, o que conduz à preocupação de ter sempre presente as últimas alterações.

É de referir também o tempo e a necessidade de conjugar distintos papéis sociais. E, nesse âmbito, uma das maiores dificuldades resulta da necessidade da conjugação do tempo que é necessário para a realização de uma dissertação com a vida de trabalhadora e de mãe a tempo inteiro, sem interrupção de nenhum desses papéis.

Um outro obstáculo foi resultado de se tentarem encontrar entidades que dessem uma resposta positiva ao nosso pedido para realizar um estudo de caso múltiplo.

Importa ainda referir, por último, as limitações que surgem quanto à utilização de entrevistas e questionários, que não dependem só do investigador, mas que têm, por sua vez, que ter em conta a disponibilidade e agenda dos respondentes. E aqui outra limitação refere-se ao número de entrevistados e ao tamanho da amostra do questionário, que pode ser considerado reduzido. Contudo o questionário foi aqui complementar e a escolha da temática foi validada no decorrer das várias entrevistas, pois todos sem exceção, e ainda que nunca se tivessem debruçado sobre o tema, reconheceram a pertinência do estudo, pensaram sobre o assunto e formularam a sua opinião, acrescentando propostas de melhoria.

Sinaliza-se ainda que o resultado da nossa investigação, tratando-se de um estudo de caso, não

pode ser generalizado a todas as instituições bancárias, tratando-se obviamente de uma limitação clássica desta estratégia de investigação. Contudo, e tendo em conta o propósito da presente dissertação, as suas conclusões no âmbito da resposta à questão 1 podem ser replicadas, se ainda não aplicadas.

Como sugestões para investigação futura destacamos a possibilidade de alargar o universo estudado, não só em número de colaboradores entrevistados, mas também aumentar a quantidade de questionários respondidos. Seria igualmente interessante a realização de um estudo de caso múltiplo, alargado a várias instituições bancárias.

6. Bibliografia

- Acórdão n.º 672/2006. (28 de setembro de 2021). *Tribunal Constitucional Acórdãos índices gerais*. Obtido de Tribunal Constitucional Portugal: <http://www.tribunalconstitucional.pt/tc/acordaos/20060672.html>
- Almeida, L. S., & Freire, T. (2000). *Metodologia de Investigação em psicologia e educação*. Braga: Psiquilibrios.
- Alter, S. (1992). *Information Systems: A Management Perspective*. Cornell, California: Addison-Wesley.
- Alves, M. T. (jul/set de 2011). Análise de Conteúdo: sua aplicação nas publicações de contabilidade. *Revista Universo Contábil*, v.7, n.º 3, pp. 146-166.
- Antunes, M. d. (2008). *Influência da gestão por processos no desempenho organizacional: um estudo empírico na área social*. Lisboa: Dissertação apresentada à Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa.
- Assis, D. (2018). Metodologia de Pesquisa. *Metodologia de Pesquisa*. Belém, Pará, Brasil: AEDI.
- Associação Portuguesa de Bancos. (7 de julho de 2022). *Setor Bancário*. Obtido de Setor Bancário Português: https://www.apb.pt/setor_bancario/setor_bancario_portugues/
- Athayde, A., Athayde, A. A., & Athayde, D. d. (2009). *Curso de Direito Bancário*. Lisboa: Coimbra Editora.
- Aviso n.º 2/2018 do BdP. (26 de fevereiro de 2018).
- Azevedo, M. E. (2012). O segredo bancário e a fiscalidade na ordem jurídica portuguesa. *Lusíada. Direito. Lisboa*, n.º 10, pp. 213-236.
- Banco BPI. (10 de maio de 2021). Obtido de <https://www.bancobpi.pt/particulares>
- Banco de Portugal. (7 de julho de 2022). *Missão e funções*. Obtido de Banco de Portugal: <https://www.bportugal.pt/page/missao-e-funcoes?mlid=808>
- bancobpi.pt*. (17 de abril de 2022). Obtido de [bancobpi.pt](https://www.bancobpi.pt/grupo-bpi/grupo-bpi-grupo-bpi/o-que-e-o-bpi): <https://www.bancobpi.pt/grupo-bpi/grupo-bpi-grupo-bpi/o-que-e-o-bpi>
- bancobpi.pt/regulamento-geral-protacao-dados*. (20 de maio de 2022). Obtido de <https://www.bancobpi.pt/particulares>: <https://www.bancobpi.pt/regulamento-geral-protacao-dados>
- Bardin, L. (2016). *Análise de Conteúdo*. São Paulo: Edições 70.
- Bauer, M. W., & Gaskell, G. (2007). *Pesquisa Qualitativa com texto, imagem e som: um manual prático*. Petrópolis: Vozes.
- Berelson, B. (1952). *Content Analysis*. New York: Hafner Press.
- Borrvalho, C. (2018). *Sistema de Planeamento e Controlo de Gestão: fundamentos e ferramentas de suporte*. Lisboa: Sílabo.
- Borrvalho, C. (2019). *Informação e Gestão de Processos de Negócio*. Lisboa: Sílabo.
- Braga, A. C. (2020). *Branqueamento de capitais e Financiamento do Terrorismo. Ações preventivas da ASAE*. Porto: Dissertação apresentada à Universidade Fernando Pessoa da Faculdade de Ciências Humanas e Sociais.
- Braguês, J. L. (2009). *O processo de branqueamento de capitais. OBEGEF - Observatório de Economia e Gestão de Fraude, Working Papers*, n.º 2. Edições Húmus.
- Branco, F. M. (2018). *O Regulamento Geral sobre Proteção de Dados - Direitos dos Utilizadores*. Coimbra: Dissertação apresentada ao Instituto Superior de Contabilidade e Administração de Coimbra do Instituto Politécnico de Coimbra.
- Brandão, N. (2002). *Branqueamento de Capitais: o sistema comunitário de prevenção*. Coimbra : Coimbra Editora.
- Buttarelli, G. (2018). Parecer da Autoridade Europeia para a Proteção de Dados sobre "Corresponder aos desafios dos grandes volumes de dados: Um apelo à transparência, controlo do utilizador, proteção de dados desde a conceção e responsabilidade. *Jornal Oficial da União Europeia*, 2.
- Campos, C. J. (setembro/outubro de 2004). Método de Análise de Conteúdo: ferramenta para a análise de dados qualitativos no campo da saúde. *Rev Bras Enferm (DF)*, pp. 611-14.
- Campos, D. L. (1997). *O sigilo bancário, Colóquio Luso-Brasileiro sobre sigilo bancário, Instituto de direito bancário*. Lisboa : Edições Cosmos.
- Canas, V. (2004). *O crime de branqueamento: Regime de Prevenção e de Repressão*. Coimbra:

- Almedina.
- Canotilho, G., & Moreira, V. (2014). *Constituição da República Portuguesa Anotada*. Coimbra: Coimbra Editora.
- Cardoso, M. R., Oliveira, G. S., & Ghelli, K. G. (2021). Análise de Conteúdo: Uma metodologia de pesquisa qualitativa. *Cadernos da Fucamp, Vol. 20, n.º 43*, pp. 98-111.
- Carlomagno, M. C., & Rocha, L. C. (2016). Como criar e classificar categorias para fazer análise de conteúdos: uma questão metodológica. *Revista Eletrônica de Ciência Política, vol , n.º 1*, pp. 173-188.
- Código Penal. (15 de março de 1995). Decreto-Lei 48/95 Código Penal.
- Coelho, V. R. (2012). *Sigilo Bancário: Problemas Fiscais e Constitucionais*. Porto: Dissertação apresentada à Escola de Direito da Universidade Católica Portuguesa - Centro Regional do Porto.
- Cordeiro, A. B. (2018). *Dados Pessoais: conceito, extensão e limites*. Obtido de BLOOK.PT: <https://blook.pt/publications/publication/e38a9928dbce/>
- Cordeiro, A. M., Leitão, L. M., & Gomes, J. d. (2002). *Estudos em homenagem ao Professor Dr. Inocêncio Galvão Teles, Vol. II, Direito Bancário*. Coimbra: Almedina .
- Coreni, E. (2018). *Regulamento Geral de Proteção de Dados - o impacto causado numa organização*. Lisboa: Dissertação apresentada à Lisbon School of Economics & Management da Universidade de Lisboa.
- Coutinho, C. P. (2014). *Metodologia de Investigação em Ciências Sociais e Humanas: Teoria e Prática*. Coimbra: Almedina.
- Davenport, T. H. (1994). Managing in the New World of Processes. *Public Productivity and Management Review*, pp. 133-147.
- Decreto-Lei n.º 313/93. (15 de setembro de 1993).
- Decreto-Lei n.º 325/95. (2 de dezembro de 1995).
- Decreto-Lei n.º 15/93. (22 de janeiro de 1993). Lei da Droga.
- Decreto-Lei n.º 289/98. (17 de dezembro de 1998). Lei Geral Tributária.
- Decreto-Lei n.º 298/92. (21 de dezembro de 1992). RGICSF.
- Decreto-Lei n.º 47909. (07 de setembro de 1967).
- Diretiva 91/308/CEE. (s.d.).
- Duarte, C. C. (2019). *O efeito da implementação dos regulamentos contra o Branqueamento de Capitais no desempenho financeiro dos Bancos em Portugal*. Lisboa: Dissertação apresentada ao Instituto Superior de Contabilidade e Administração de Lisboa do Instituto Politécnico de Lisboa.
- Duarte, S. A. (2018). *Aplicação do Regulamento Geral sobre a Proteção de Dados (RGPD): Caso de estudo de uma IPSS*. Braga : Dissertação apresentada à Escola de Direito da Universidade do Minho.
- Eco, U. (2007). *Como se faz um tese em ciências humanas*. Lisboa : Editorial Presença .
- Ferreira, E. P. (1999). *O Branqueamento de Capitais, in Separata de Estudos de Direito Bancário, Faculdade de Direito da Universidade de Coimbra*. Coimbra: Coimbra Editora.
- Ferreira, M. N. (2017). *Monitorização dos resultados: uma ferramenta para a tomada de decisão na melhoria da escola*. Lisboa: Dissertação apresentada à Escola Superior de Educação de Lisboa do Instituto Politécnico de Lisboa.
- Firmino, M. J. (2015). *Testes de hipóteses: uma abordagem não paramétrica*. Lisboa : Dissertação apresentada ao Departamento de Estatística e Investigação Operacional da Faculdade de Ciências da Universidade de Lisboa.
- Fonseca, A., Lourenço, A., Balinha, H., Martins, J., Dinis, J., & Marques, L. (18 de outubro de 2018). O RGPD: a articulação entre a gestão da informação e a gestão da segurança da informação. *Associação Portuguesa de Bibliotecários, Arquivistas e Documentalistas, Portugal*, pp. 1-16.
- Fortin, M. F. (2003). *O processo de investigação: da conceção à realização*. 3ª edição: Lusociência.
- Fortin, M. F. (2009). *Fundamentos e etapas do processo de investigação*. Loures: Lusodidacta.
- Francisco, D., & Francisco, S. (2019). *RGPD - Regulamento Geral de Proteção de Dados 7 passos para uma metodologia de implementação do RGPD na Administração Pública*. Lisboa: Edições Sílabo.
- Freitas, H. M., Júnior, M. V., & Mascarola, J. (jul/set de 1997). Aplicação de sistemas de software

- para auxílio na análise de conteúdo. *RAUSP V. 32, N° 3*, pp. 97-109.
- Freitas, W. R., & Jabbour, C. J. (22 de julho de 2017). Utilizando estudo de caso(s) como estratégia de pesquisa qualitativa: boas práticas e sugestões. *Estudo & Debate*, pp. 07-22.
- Freixo, M. J. (2011). *Metodologia Científica: Fundamentos, métodos e técnicas*. Lisboa : Instituto Piaget.
- Gades Solutions. (7 de julho de 2022). *Nvivo*. Obtido de Análise de Dados: <https://gades-solutions.com/project/nvivo/>
- Garrigues. (08 de setembro de 2021). *A Garrigues Comunica*. Obtido de Garrigues: <https://www.garrigues.com/pt/pt-PT/news/portugal-procedeu-transposicao-das-diretivas-europeias-combate-ao-branqueamento-capitais-e>
- Gil, A. C. (2009). *Como elaborar projetos de pesquisa*. São Paulo: Atlas.
- Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. New Brunswick (USA); London (UK): Aldine Transaction.
- Godoy, A. S. (março/abril de 1995). Introdução à pesquisa qualitativa e suas possibilidades. *Revista de Administração de Empresas*, pp. 57-63.
- Gomes, J. G. (18 de abril de 2022). *Novo pacote europeu de AML/CFT*. Obtido de servulo.com: <https://www.servulo.com/pt/investigacao-e-conhecimento/Novo-pacote-europeu-de-AMLCFT/7695/>
- Gomes, N. (2006). *Segredo Bancário e Direito Fiscal*. Lisboa: Almedina.
- Gonçalves, M. E. (2003). *Direito da informação: novos direitos e formas de regulação da informação*. Coimbra: Almedina.
- Guazi, T. S. (2021). Diretrizes para uso de entrevistas semiestruturadas em investigações científicas. *Revista educação, Pesquisa e Inclusão, Vol. 2*, pp. 1-20.
- Guerreiro, A. S. (2018). *As regras vinculativas para as empresas (Binding corporate rules) no novo regulamento geral de proteção de dados: o reconhecimento da co-regulação e do "princípio da responsabilidade" como meio para passar da teoria à prática na proteção de dados pessoais*. Lisboa: Dissertação apresentada à Faculdade de Direito da Universidade Nova de Lisboa.
- Harrington, H. J. (1998). Business Process management: a review and evaluation. *Business Process Management Journal*, pp. 214-225.
- Hill, M. M., & Hill, A. (2012). *Investigação por Questionário*. Lisboa: Edições Sílabo. https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_pt. (10 de abril de 2022). Obtido de https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_pt
- <https://gades-solutions.com/>. (21 de maio de 2011). Obtido de GADES Data Analysis Solutions : <https://gades-solutions.com/project/nvivo/>
- https://www.apb.pt/setor_bancario/modelo_de_supervisao/. (23 de maio de 2022). Obtido de www.apb.pt: https://www.apb.pt/setor_bancario/modelo_de_supervisao/
- https://www.apb.pt/setor_bancario/setor_bancario_portugues/. (23 de maio de 2022). Obtido de [apb.pt](https://www.apb.pt): https://www.apb.pt/setor_bancario/enquadramento_legislativo/entidades_reguladoras_e_de_supervisao
- https://www.apb.pt/setor_bancario/setor_bancario_portugues/. (23 de maio de 2022). Obtido de <https://www.apb.pt/>: https://www.apb.pt/setor_bancario/enquadramento_legislativo/processo_legislativo_e_regulamentar_da_uniao_europeia/
- <https://www.bportugal.pt/page/missao-e-funcoes?mlid=808>. (23 de 05 de 2022). Obtido de <https://www.bportugal.pt/>: <https://www.bportugal.pt/page/missao-e-funcoes?mlid=808>
- <https://www.ifap.pt/home>. (04 de junho de 2022). *Minuto RGPD - As coimas do RGPD, no terceiro trimestre de 2021, atingiram quase mil milhões de euros*. Obtido de <https://www.ifap.pt/home>: https://www.ifap.pt/resultados-pesquisa?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_returnToFullPageURL=https%3A%2F%2Fwww.ifap.pt%2Fen%2Fweb%2Fguest%2Fresultados-pesquisa%3Fp_auth%2F
- Huberman, a. M., & Miles, M. B. (2003). *The Quantitative Researchers Companion*. California : Sage Publications, Inc.

- Informação Financeira*. (17 de 04 de 2022). Obtido de bpi.bancobpi.pt:
<https://bpi.bancobpi.pt/index.asp?riIdArea=AreaDFinanceiros&riId=DContas>
- Instrução do Banco de Portugal n.º 2/2021, 2. d. (s.d.).
- Jelinek, A. (15 de 12 de 2020). *edpb*. Obtido de edpb.europa.eu: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-protection-personal-data-processed-relation_pt
- Jesus, A. J. (2016). *Branqueamento de Capitais - Estudo empírico dos últimos anos em Portugal*. Lisboa: Dissertação apresentada ao Instituto Superior de Contabilidade e Administração de Lisboa do Instituto Politécnico de Lisboa.
- Kerlinger, F. N. (1979). *Metodologia da Pesquisa em Ciências Sociais: um tratamento conceitual*. Amesterdão : Editora Pedagógica e Universitária Lda.
- Kettinger, W. J., & Groven, V. (1995). Special Section: Toward a Theory of Business Process Change Management. *Journal of Management Information Systems*, 9-30.
- Khazanchi, D., & Munkvold, B. E. (2002). On the Rhetoric and Relevance of IS Research Paradigms: A Conceptual Framework and Some Propositions. *Proceedings of the 36th Hawaii International Conference on System Sciences* (pp. 1-11). Hawaii: IEEE.
doi:10.1109/HICSS.2003.1174717
- Laudon, K. C., & Laudon, J. P. (2014). *Management Information System: Managing the Digital Firm*. Nova Iorque : Pearson.
- Laudon, K. C., & Laudon, J. P. (1998). *Management Information Systems: New Approaches to Organization & Technology*. New York: Prentice Hall.
- Lei n.º 10/2002. (10 de fevereiro de 2002).
- Lei n.º 11/2002. (16 de fevereiro de 2002).
- Lei n.º 25/2008. (25 de agosto de 2008). Lei do Combate ao Branqueamento de Capitais e do Financiamento ao Terrorismo.
- Lei n.º 52/2003. (22 de agosto de 2003). Lei de Combate ao Terrorismo .
- Lei n.º 83/2017 . (18 de agosto de 2017).
- Lei n.º 97/2017. (23 de agosto de 2017).
- Liebscher, P. (1998). Quantity with quality? Teaching quantitative and qualitative methods in a LIS Mater's program. *Library Trends* v. 46 n.º 4, pp. 668-689.
- Lima, J. Á. (2013). Por uma análise de conteúdo mais fiável . *Revista Portuguesa de Pedagogia* , pp. 7-29.
- Lima, J. Á., & Pacheco, J. A. (2006). *Fazer Investigação: Contributos para a elaboração de dissertações e teses*. Porto: Porto Editora .
- Lima, J. P., Antunes, M. T., Mendonça, O. R., & Peleias, I. R. (abril de maio de 2012). Estudos de caso e sua aplicação: proposta de um esquema teórico para pesquisas no campo da contabilidade. *Revista de Contabilidade e Organizações*, V. 6, n.º 14, pp. 127-144.
- Luc Van Campenhoudt, R. Q., & Marquet, J. (2019). *Manual de Investigação em Ciências Sociais*. Lisboa: Gradiva.
- Lúcio Agostinho Barreiros dos Santos, F. M., Monteiro, F. T., Lima, J. M., Silva, N. M., Silva, J. C., Piedade, & Afonso, .. F. (2016). *Orientações Metodológicas para elaboração de trabalhos de investigação*. Lisboa : Instituto Universitário Militar.
- Luís, A. (1981). O segredo bancário em Portugal. *Revista da Ordem dos Advogados*, n.º 41 , p. 454.
- Magalhães, F. M., & Pereira, M. L. (2020). *Regulamento Geral de Proteção de Dados* . Porto: Vida Económica.
- Major, M. J., & Vieira, R. (2009). *Contabilidade e Controlo de Gestão: teoria, metodologia e prática*. Lisboa: Escolar Editora.
- Marconi, M. d., & Lakatos, E. M. (2003). *Fundamentos de metodologia científica* . São Paulo : Atlas.
- Maroco, J. (2003). *Análise Estatística com utilização do SPSS*. Lisboa: Edições Sílabo .
- Maroco, J., & Garcia-Marques, T. (2006). Qual a fiabilidade do alfa de Cronbach? Questões antigas e soluções modernas? *Laboratórios de Psicologia*, pp. 65-95.
- Marques, A. C. (2016). *O sigilo bancário na relação jurídica fiscal*. Lisboa : Dissertação apresentada à Faculdade de Direito da Universidade Nova de Lisboa.
- Marques, M. P. (2005). *Para a compreensão de um envolvimento musical - Experiência de alunos de guitarra clássica e de guitarra jazz no ensino superior*. Porto: Dissertação apresentada à Faculdade de Psicologia e de Ciências da Educação da Universidade do Porto.

- Martinez, L. F., & Ferreira, A. I. (2008). *Análise de Dados com SPSS*. Lisboa: Escolar Editora.
- Martins, G. A. (jan/abr de 2008). Estudo de caso: uma reflexão sobre a aplicabilidade em pesquisas no Brasil. *Revista de Contabilidade e Organizações*, v. 2 n. 2, pp. 9-18.
- Melo, A. S. (2019). *Regulamento Geral de Proteção de Dados: Um novo paradigma regulatório*. Coimbra: Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra.
- Mendes, P. A. (2018). *Análise de Risco no GDPR*. Lisboa: Dissertação apresentada à Faculdade de Ciências Departamento de Informática da Universidade de Lisboa.
- Mendes, P. S. (julho a dezembro de 2012). A derrogação do segredo bancário no processo penal. *Revista de Concorrência e Regulação*, 388. Almedina.
- Minayo, M. C. (12 de abril de 2017). Amostragem e Saturação em Pesquisa Qualitativa: Consensos e Controvérsias. *Revista Pesquisa Qualitativa*, pp. 01-12.
- Minayo, M. C., Deslandes, S. F., & Gomes, R. (2007). *Pesquisa Social: Teoria, método e criatividade*. Petrópolis: Vozes.
- Miranda, P. C. (2016). *Framework para os fatores críticos de sucesso na adoção de sistema de e-Learning 3.0*. Lisboa: Dissertação apresentada à Escola de Tecnologias e Arquitetura Departamento de Ciências e Tecnologias da Informação do ISCTE.
- Monteiro, R. F. (2015). *O sigilo bancário e a fraude fiscal: interrelação científica e dogmática*. Lisboa: Dissertação apresentada à Faculdade de Direito da Universidade Nova de Lisboa.
- Morais, J. C. (2018). *A relevância dos meios digitais no setor bancário*. Porto: Dissertação apresentada à Faculdade de Economia da Universidade do Porto.
- Moreira, C. D. (2007). *Teorias e Práticas de Investigação*. Lisboa: Instituto de Ciências Sociais e Políticas.
- Moura, F. V., & Filho, J. M. (24 a 29 de setembro de 2010). Pesquisa em Contabilidade, Teoria Institucional e Análise de Conteúdo - Interfaces e Sinergias. *EnANPAD*, pp. 1-17.
- Nascimento, A., Venturine, C., Demba, J., & Neves, A. T. (2021). Reflexões em torno de Metodologias de Investigação. Em P. Sá, A. P. Costa, & A. Moreira, *Reflexões em torno de Metodologias de Investigação recolha de dados* (pp. 87-100). Aveiro: Universidade de Aveiro.
- Neves, J. L. (V.1, N.º 3 de 1996). Pesquisa Qualitativa - características, usos e possibilidades. *Caderno de Pesquisas em Administração*, pp. 1-5.
- Nunes, M. F. (2019). *Ferramentas para o planeamento e avaliação de risco de dados de investigação: o caso do i3S no âmbito do RGPD*. Porto: Dissertação apresentada à Faculdade de Engenharia da Universidade do Porto.
- Nunes, M. G. (2020). *Aplicação do Custeio Baseado em Atividades na GESAMB – Gestão Ambiental e de Resíduos, EIM*. Beja: Dissertação apresentada à Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Beja.
- O'Brien, J. A. (1994). *Management Information Systems: A Managerial End User Perspective*. Homewood, IL: Richard D. Irwin.
- Oliveira, D. C. (outubro/dezembro de 2008). Análise de conteúdo temático-categorial: uma proposta de sistematização. *Atualidades Revista de Enfermagem*, pp. 569-576.
- Orrit, J. D., & Rizzo, B. (18 de abril de 2022). [www.eesc.europa.eu](https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021XX1229(01)&from=EN). Obtido de [https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021XX1229\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021XX1229(01)&from=EN)
- Pais, L. M. (2016). *Derrogação do sigilo bancário para efeitos tributários*. Lisboa: Dissertação apresentada à Faculdade de Direito da Universidade de Lisboa.
- Pardal, L., & Lopes, E. S. (2011). *Métodos e Técnicas de Investigação Social*. Lisboa: Areal Editores.
- Pestana, M. H., & Gageiro, J. N. (2000). *Análise de Dados para ciências sociais: a complementaridade do SPSS*. Lisboa: Edições Sílabo, Lda.
- Pestana, M. H., & Gageiro, J. N. (2005). *Análise de Dados para Ciências Sociais*. Lisboa: Edições Sílabo.
- Pinho, F. (2017). *Anonimização de Bases de Dados Empresariais de acordo com a nova regulamentação europeia de proteção de dados*. Porto: Dissertação apresentada à Faculdade de Ciências da Universidade do Porto.
- Pinto, P. d. (2002). A limitação voluntária do direito à reserva sobre a intimidade da vida privada. Em *Estudos em homenagem a Cunha Rodrigues* (p. 527 ss). Coimbra: Coimbra.
- Pires, J. M. (1998). *O dever de segredo na atividade bancária*. Rei dos Livros.

- Pires, P. (2018). *A prevenção do Branqueamento de Capitais em Portugal; Papel dos Reguladores Nacionais*. Lisboa: Dissertação apresentada ao Instituto Superior de Contabilidade e Administração de Lisboa do Instituto Politécnico de Lisboa.
- Portal do DPO. (30 de maio de 2022). *Encarregado de Protecção de Dados ou Data Protection Officer (DPO)*. Obtido de <https://www.portaldodpo.pt/funcoes-do-dpo/>
- Quaresma, V. B. (janeiro/julho de 2005). Aprendendo a entrevistar: como fazer entrevistas em Ciências Sociais. *Revista Eletrônica dos Pós-Graduandos em Sociologia Política da UFSC*, pp. 68-80.
- Queiroz, C. (2007). A proteção constitucional da recolha de tratamento de dados pessoais automatizados. Em *Prof. Dr. Inocêncio Galvão Telles: 90 anos: Homenagem da Faculdade de Direito de Lisboa* (pp. 291-315). Coimbra: Almedina.
- Quivy, R., & Campenhoudt, L. v. (2008). *Manual de Investigação em Ciências Sociais 5ªed*. Lisboa: Gradiva.
- Raimundo, J. P. (2012). *Uma nova frente da proteção de dados pessoais: a (im)possibilidade de assegurar um eventual direito ao esquecimento*. Porto: Dissertação apresentada à Faculdade de Direito da Universidade do Porto.
- Ramos, C. (2004). *Desenvolvimentos recentes em matéria de prevenção do branqueamento de capitais. Em F.T. Jacinto, Polícia e Justiça: Branqueamento de Capitais*. Coimbra : Coimbra Editora.
- Ramos, C. C. (28 de janeiro de 2020). *Dia Europeu da Protecção de Dados: das críticas - da CNPD à Lei de Execução do RGPD - às coimas aplicadas*. Obtido de [eco.sapo.pt](https://eco.sapo.pt/opiniao/dia-europeu-da-proteccao-de-dados-das-criticas-da-cnpd-a-lei-de-execucao-do-rgpd-as-coimas-aplicadas)
- Rebelo, D. M., Analide, C., & Abreu, J. C. (abril de 2020). *O mercado úncio digital e a (leigo)ritmia da pontuação de crédito na era da inteligência artificial*. Obtido de <https://blook.pt/publications/publication/66689aed966b/>
- Reis, F. L. (2010). *Como Elaborar uma Dissertação de Mestrado*. Lisboa: Pactor.
- Ribeiro, P. J. (2011). *Dados bancários enquanto dados sensíveis*. Porto: Dissertação apresentada à Faculdade de Direito da Universidade do Porto.
- Riffe, D., Lacy, S., Watson, B., & Fico, F. (2019). *Analyzing Media Messages: using quantitative Content Analysis in Research*. Londres: Routledge.
- Rodrigues, J. d. (2010). *Sistemas de Informação e Gestão Automatizada de Processos - o impacto da sua implementação no Serviço de Estrangeiros e Fronteiras*. Lisboa: Dissertação apresentada à Universidade de Lisboa.
- Rodrigues, L. S. (2002). *Arquitecturas dos Sistemas de Informação*. Lisboa: FCA.
- Rodrigues, S. M. (2010). *O branqueamento de capitais e a droga*. Lisboa: Dissertação apresentada ao Instituto Superior de Contabilidade e Administração de Lisboa do Instituto Politécnico de Lisboa.
- Sá, P., Costa, A. P., & Moreira, A. (2021). *Reflexões em torno de Metodologias de Investigação*. Aveiro: Universidade de Aveiro.
- Salgado, F. R. (2015). *Branqueamento de capitais: uma análise empírica*. Coimbra : Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra.
- Sampaio, R. C., & Lycarião, D. (2021). *Análise de conteúdo categorial: manual de aplicação*. Brasília : Enap.
- Sanches, J. L. (1995). *O segredo bancário e a tributação do lucro real. In Cadernos de Ciência e Técnica Fiscal, 377*. Coimbra: Coimbra Editora.
- Sanches, J. L. (2007). *Manual de Direito Fiscal*. Coimbra: Coimbra Editora.
- Santos, L. A., & Lima, J. M. (13 de outubro de 2019). *Orientações Metodológicas para a elaboração de trabalhos de investigação (2ª ed., revista e atualizada)*. Obtido de [ium.pt](https://www.iium.pt/)
- Santos, L. M. (11 de abril de 2021). *Intervenção do Vice-Governador, Luís Máximo dos Santos, no encerramento do Colóquio CNSF - Três anos de RGPD*. Obtido de Banco de Portugal: <https://www.bportugal.pt/print/1311743>
- Schott, P. A. (2004). *Guia de referência Anti-branqueamento de Capitais e de Combate ao Financiamento do Terrorismo - Segunda Edição e Suplemento sobre a Recomendação*

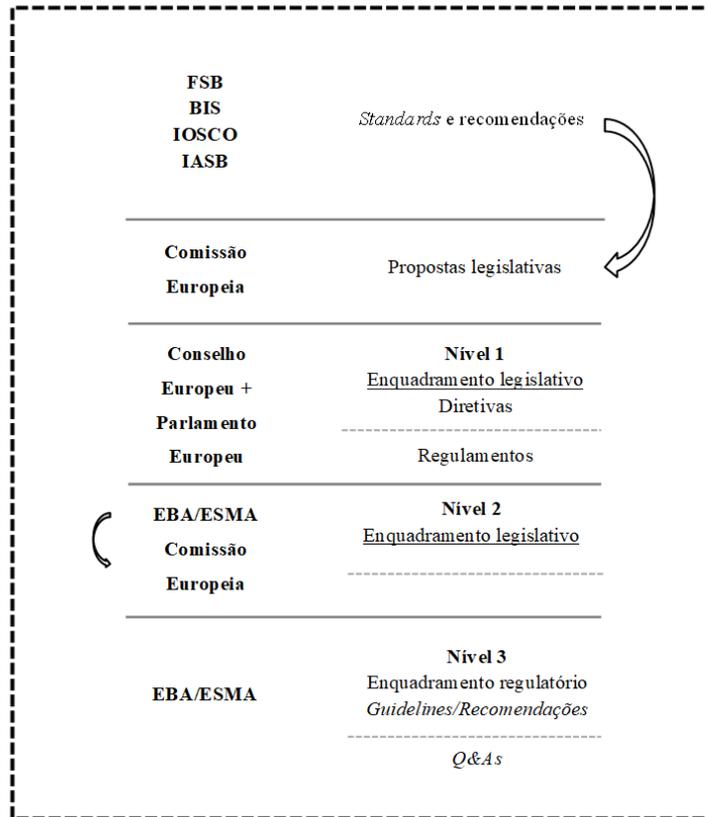
sobre o pacote de propostas legislativas de combate ao branqueamento de capitais e ao terrorismo. *Jornal Oficial da União Europeia*, C 544/10.

Yin, R. K. (1994). *Pesquisa Estudo de Caso- Desenho e Métodos (2ª ed.)*. Porto Alegre: Bookman.

Yin, R. K. (2004). *Estudo de caso: planejamento e métodos (2ª edição)*. São Paulo: Bookman.

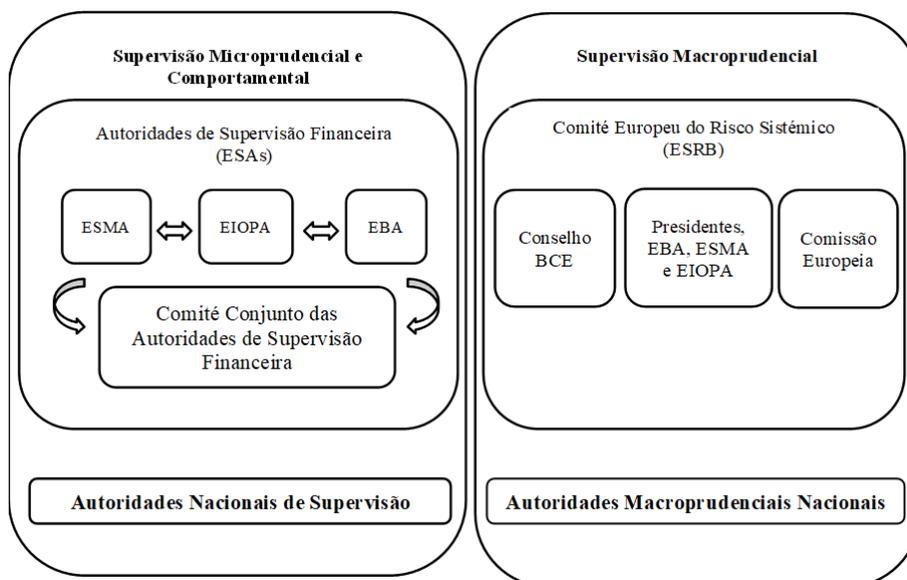
7. Anexos

Anexo I – Processo legislativo e regulamentar da EU



Fonte: Associação Portuguesa de Bancos

Anexo II – Sistema europeu de supervisão financeira



Fonte: Associação Portuguesa de Bancos

Anexo III – Atual modelo de supervisão do sistema financeiro português

Autoridade de Supervisão	Banco de Portugal	CMVM	Autoridade de Supervisão de Seguros e Fundos de Pensões
Âmbito de Supervisão	Instituições de Crédito Supervisão Macroprudencial e Comportamental. Autoridade Nacional de Resolução e Autoridade Macroprudencial Nacional	Mercados de valores mobiliários e instrumentos financeiros derivados e atividade dos agentes que neles atuam	Atividade seguradora, resseguradora, mediação de seguros e de fundos de pensões. Supervisão Microprudencial e Comportamental
Segmento de mercado	Banca	Mercados de Instrumentos Financeiros	Seguros e Fundos de Pensões

Fonte: Associação Portuguesa de Bancos

Anexo IV – Guião de Entrevistas

Dimensão	Objetivos	Questões
Enquadrar a entrevista e motivar os entrevistados	Legitimar a entrevista (agradecer e informar sobre o tema e objetivos do trabalho; informar sobre a possibilidade de aceder aos resultados da investigação; perceber a familiaridade do entrevistado com a temática; obter autorização prévia para recolher dados e proceder ao registo da gravação áudio)	<p>1. Autoriza a gravação da presente entrevista, para efeitos de investigação, tendo em conta que no tratamento de dados o anonimato dos respondentes será considerado?</p> <p>2. Está familiarizado com os normativos legais que regulam a proteção de dados pessoais, o sigilo bancário e BC/FT?</p>
Caracterização dos entrevistados	Enquadrar o perfil profissional dos entrevistados	<p>3. Há quantos anos exerce atividade na banca e em que área desempenha funções?</p> <p>4. Qual a sua área de formação?</p>

<p>RGPD e Sigilo Bancário</p>	<p>Conhecer as práticas diárias no que toca a tratamento de dados pessoais dos clientes</p> <p>Perceber as dimensões subjacentes do sigilo bancário</p> <p>Perceber a importância do cumprimento do sigilo bancário</p> <p>Ponderar as fronteiras do sigilo bancário à luz do novo RGPD</p> <p>Ponderar as fronteiras do sigilo bancário à luz do combate ao B/C e F/T</p> <p>Identificar possíveis formas de melhoria</p>	<p>5. No seu dia-a-dia, que procedimentos realiza que se relacionem com a proteção de dados? A entrada em vigor do RGPD teve impacto nas práticas do banco? E nas atividades que desenvolve? Que alterações notou, quais os efeitos principais? Porquê?</p> <p>6. Existem diferentes procedimentos no tratamento de dados, consoante o tipo de autorização prestada? Pode apresentar exemplos?</p> <p>7. Como é possível compatibilizar o cumprimento do sigilo bancário e o tratamento de dados pessoais, nomeadamente com a partilha de dados?</p> <p>8. Existem tarefas que não pode executar porque estaria a violar o dever de sigilo bancário? E a proteção de dados? Pode apresentar exemplos?</p> <p>9. De que forma a preocupação com o cumprimento do sigilo bancário está presente no seu dia-a-dia? E com o RGPD? Que procedimentos devem ocorrer se existir uma quebra de sigilo bancário? E em caso de incidente de violação de dados pessoais?</p> <p>10. É possível melhorar a recolha e o tratamento de dados no âmbito do RGPD? Se sim, como e porquê?</p>
<p>LBC/FT</p>	<p>Perceber a familiaridade do entrevistado com a temática</p> <p>Conhecer as práticas diárias no que toca a tratamento de dados pessoais dos clientes</p>	<p>11. Esta é uma temática com a qual se cruz no seu dia-a-dia? Trouxe-lhe acréscimo de tarefas e preocupações?</p> <p>12. Consegue elencar os dados obrigatórios que é necessário recolher para cumprimentos dos normativos relativos a BC/FT?</p> <p>13. No seu dia-a-dia que procedimentos realiza que se relacionem com a prevenção do BC/FT? Em que formato recebe a informação? De que forma trata os documentos e a quem os remete?</p> <p>14. Existem diferentes procedimentos no tratamento de dados, consoante o tipo de risco em causa?</p>

		<p>15. Como procede num caso de suspeita de B/C e F/T?</p> <p>16. É possível melhorar a recolha e o tratamento de dados no âmbito do LBC? Se sim, como e porquê?</p>
<p>Compatibilização do RGPD com LBC/FT e com o Sigilo Bancário</p>	<p>Ponderar a necessidade de compatibilização entre o RGPD e o cumprimento dos requisitos impostos pela lei do B/C e F/T nos diferentes setores do banco</p>	<p>17. Considera que o RGPD, o BC/FT e o Sigilo Bancário são matérias fáceis de compatibilizar? Porquê? Como é possível a compatibilização? Na sua opinião, qual é o instituto que deve prevalecer? Como é possível compatibilizar o cumprimento do sigilo bancário e o combate ao B/C e F/T?</p> <p>18. Os dados a remeter às entidades de supervisão, o formato de envio e o momento, são claros, quer no que respeita ao RGPD, quer no que respeita ao BC/FT? Porquê?</p> <p>19. A remessa de dados para as entidades de supervisão está otimizada e, por isso, nada pode ser feito no sentido de melhorar fluxos de trabalho? Porquê?</p> <p>20. Caso existam possíveis melhorias, quais? Porquê e como poderiam ser implementadas?</p> <p>21. Os canais de comunicação com as entidades externas são eficazes? Como poderiam ser melhorados?</p> <p>22. Considera que os procedimentos, os circuitos, e os documentos de reporte estão bem definidos pelo regulador ou há margem para a discricionariedade? Porquê?</p> <p>23. Considera que de alguma forma existem tarefas e fluxos de trabalho que podiam ser eliminados ou uniformizados? Quais e como otimizá-los?</p> <p>24. Numa perspetiva de mecanismos de</p>

		operacionalização consegue elencar, tendo em conta as três dimensões, o que pode melhorar a recolha e o tratamento de dados, bem como a compatibilização dos 3 referenciais? Como e porquê?
--	--	---

Anexo V – Questionário

CONSENTIMENTO INFORMADO

O questionário intitulado **“O combate ao branqueamento de capitais à luz do Regime Geral de Proteção de Dados (RGPD): informação, circuitos e documentos de suporte”** destina-se, exclusivamente, à realização de trabalho científico, sendo integralmente assegurado o anonimato dos respondentes no tratamento de dados.

Assim, através desta declaração, atesta que a sua participação é voluntária, informada e devidamente autorizada por si, antes de responder ao questionário.

Adicionalmente atesta que:

1. Foram explicados os objetivos do questionário, especificamente ponderar a compatibilização da aplicação do Regime Geral de Proteção de Dados, Lei de combate ao Branqueamento de Capitais e Sigilo Bancário, e aceita participar no estudo de livre vontade;
2. Compreende que é livre para responder a qualquer pergunta e que pode desistir a qualquer momento, sem que essa decisão acarrete qualquer prejuízo para si;
3. Compreende que os dados pessoais recolhidos serão alterados tendo em vista o anonimato dos respondentes no tratamento desses dados;
4. Confirma que a resposta ao questionário será realizada em condições de privacidade, com total liberdade de resposta, ou seja, sem que as respostas que apresentar possam ser condicionadas, seja de que forma for.

Data: _____

Participante: _____

Número da resposta: _____

Questionário

O combate ao branqueamento de capitais à luz do Regime Geral de Proteção de Dados (RGPD): informação, circuitos e documentos de suporte

Secção I

(caracterização do respondente)

1. Género

- Feminino
- Masculino

2. Idade ____ anos (até 30 de junho de 2022)

3. Anos de experiência na banca ____ anos (até 30 de junho de 2022)

4. Habilitações Literárias

- Ensino Básico
- Secundário
- Bacharelato
- Licenciatura
- Pós-graduação
- Doutoramento

5. Área funcional

- Área Comercial
- Direção de *Compliance*
- Direção de Auditoria
- DMPN
- Direção Jurídica

Secção II

(perceção de compatibilização operativa do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário)

6. Numa escala de 0 a 10, indique a sua perceção de compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário?

Totalmente incompatível

Totalmente compatível

1	2	3	4	5	6	7	8	9	10
----------	----------	----------	----------	----------	----------	----------	----------	----------	-----------

Considere fatores críticos na implementação como os elementos que, quando descuidados, podem limitar, ou mesmo impedir, o alcance dos propósitos que os diplomas legais procuram obter.

7. Num domínio operativo, prático, como classifica a aplicação do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário?

- Fácil
- Difícil

8. Assinale com um “○” entre discordo totalmente (1) e concordo totalmente (6) em relação às afirmações que se seguem:

Fatores críticos na implementação do Regulamento Geral de Proteção de Dados, Lei de combate ao Branqueamento de Capitais e Sigilo Bancário

Itens	Discordo totalmente			Concordo totalmente		
	1	2	3	4	5	6
8.1. Necessidade de recolha obrigatória do consentimento.	1	2	3	4	5	6
8.2. Linguagem dúbia utilizada nos formulários de RGPD.	1	2	3	4	5	6
8.3. Aplicações informáticas utilizadas.	1	2	3	4	5	6
8.4. Formação do pessoal ao serviço.	1	2	3	4	5	6
8.5. Tempestividade da recolha de dados.	1	2	3	4	5	6
8.6. Linguagem dúbia utilizada nos formulários de reporte de BC/FT.	1	2	3	4	5	6
8.7. Elevado número de dados a recolher.	1	2	3	4	5	6
8.8. Padronização de processos de BC/FT	1	2	3	4	5	6
8.9. Processos de análise de risco muito morosos	1	2	3	4	5	6

Considere a eficiência organizacional enquanto a capacidade de fazer mais com o mesmo consumo de recursos ou fazer o mesmo consumindo menos recursos.

9. Assim, num domínio operativo, prático, a eficiência na compatibilização do Regulamento Geral de Proteção de Dados, com a Lei de combate ao Branqueamento de Capitais e com o Sigilo Bancário, pode ser potenciada?

- Sim
- Não

Assinale com um “○” entre discordo totalmente (1) e concordo totalmente (6) em relação às afirmações que se seguem:

Eficiência na implementação do Regulamento Geral de Proteção de Dados, Lei de combate ao Branqueamento de Capitais e Sigilo Bancário

Itens	Discordo			Concordo		
	totalmente			totalmente		
9.1. Consentimento RGPD através de gravação de chamadas telefónicas.	1	2	3	4	5	6
9.2. Consulta mais rápida do consentimento RGPD associado a cada cliente	1	2	3	4	5	6
9.3. Limitação do extravio de documentos.	1	2	3	4	5	6
9.4. Inexistência de assinatura digitalizada das fichas de informação de cliente.	1	2	3	4	5	6
9.5. Colocar o consentimento informado imposto pelo RGPD no fluxo de todos os processos.	1	2	3	4	5	6
9.6. Obrigação de recolha da assinatura do cliente em todas as alterações de dados.	1	2	3	4	5	6
9.7. Inexistência de canais expeditos de comunicação entre as áreas.	1	2	3	4	5	6
9.8. Inexistência de <i>check-list</i> de dados a recolher para tornar os processos mais rápidos.	1	2	3	4	5	6
9.9. Relatórios de risco muito extensos.	1	2	3	4	5	6
9.10. Utilização massiva de chaves móveis digitais.	1	2	3	4	5	6

Secção III

(informação adicional)

10.1. Existem dificuldades práticas na implementação dos diplomas (Regulamento Geral de Proteção de Dados, Lei de combate ao Branqueamento de Capitais e Sigilo Bancário)?

- Sim
- Não

10.2. Porquê? _____

Questionário concluído. Muito obrigado pela sua colaboração!

Anexo VI Etapas na análise de conteúdo

ETAPAS DA ANÁLISE DE CONTEÚDO
Conceituação
1. Identificar o problema
2. Questões de pesquisa e hipóteses
Desenho
3. Seleccionar a(s) unidade(s) e subunidade(s) de análise
4. Criar e definir categorias
a. elaboração do livro de códigos
b. elaborar a planilha de codificação
5. Amostragem
6. Pré-teste das categorias e da regras de codificação
a. treinamento
b. revisão do livro de códigos
c. teste de confiabilidade piloto
7. Treinamento final e teste e teste de confoabilidade das categorias
8. Codificação
9. Testes de confiabilidade intermédio
Análise
10. Tabulação e aplicação de procedimentos estatísticos
11. Interpretar e reportar os resultados
12. Validação e replicabilidade

Fonte: (Sampaio & Lycarião, 2021)

Anexo VII – Análise Categorical de Conteúdo

Categoria I: Importância da compatibilização harmoniosa dos diplomas		
Unidade de contexto	Unidade de registo	Frequência
“...se o cliente autorizar que a partilha de dados seja efetuada julgo que o sigilo bancário já está um pouco, ultrapassado...” E1	Autorização de partilha pelo cliente derroga o sigilo (E1)	1
“...temos que ter mais um consentimento dos clientes, estes têm uma palavra a dizer sobre o tratamento dos dados que eles nos facultam e estejam alertados para essa situação...” E3	Consciência da importância do RGPD e da necessidade de respeitar o consentimento do cliente para tratar dados para fins	4

Categoria I: Importância da compatibilização harmoniosa dos diplomas

Unidade de contexto	Unidade de registo	Frequência
<p>“...a nível do dos contactos, as restrições isso é definido pelo cliente: como é que prefere ser contactado, em que horário, o telemarketing... o cliente veio definir o que é mais conveniente para si e que o banco neste caso é obrigado a respeitar de acordo com a vontade do cliente...” E4</p> <p>“...o tratamento de dados que fazemos... só podem ser usados para o fim a que se destinam...portanto se recolhemos dados para fins de marketing e publicidade, se o cliente dá consentimento para aquele fim nós não podemos usar aqueles dados para outro fim a não ser para aquele, a não ser que tenhamos, por outra via, legitimidade para fazê-lo...” E7</p> <p>“...a questão do RGPD que reforça o tratamento desses dados, perante autorizações do cliente... ou seja eu posso recolher, tratar e partilhar os dados com entidades do grupo, etc , posso tentar monitorizar a atividade do cliente e entregar-lhe uma oferta específica, hoje mais do que nunca, até com o <i>business intelligence</i>, que o Banco está a criar até com o RGPD, de permitir seguir a atividade, a minha conta, para me fazerem ofertas mais específicas, mais direcionadas, quer através da monitorização direta ou através de cookies... isto é o que estamos a dar direito ao cliente com o RGPD, eu quero ou não quero, que fale comigo sobre isto...” E10</p>	<p>de marketing e publicidade, aplica-se à oferta comercial, contactos e definição de perfis (E3), (E4), (E7), (E10)</p>	
<p>“...o que se preconiza é só utilizar os dados para as finalidades específicas para as quais são recolhidas ou então de acordo com a lei pois a lei também possibilita, sem consentimento, fazer a gestão dos dados...” E7</p>	<p>A lei também preconiza o tratamento de dados sem o consentimento do titular (E7)</p>	<p align="center">1</p>
<p>“...RGPD permite evitar o trafico de informação de clientes entre grandes empresas...” E10</p> <p>“... o RGPD vem em complemento, vem reforçar de facto essas medidas e fazer com que o banco não utilize essa informação dos clientes ou potenciais de forma abusiva...” E10</p>	<p>RGPD visa evitar o trafico de informações entre empresas e uso abusivo dos dados dos clientes (E10)</p>	<p align="center">1</p>
<p>“...nós no fundo aquilo que fizemos foi ter a certeza que com a introdução do RGPD, toda a informação que circulava entre nós e os parceiros foi devidamente autorizada porque a questão do sigilo bancário nunca esteve em causa com os parceiros. Aqui está em causa é a utilização dos dados dos clientes de um lado para o outro...” E10</p>	<p>RGPD evita a circulação de dados entre o banco e os parceiros, sem consentimento (E10)</p>	<p align="center">1</p>

Categoria I: Importância da compatibilização harmoniosa dos diplomas

Unidade de contexto	Unidade de registo	Frequência
<p>“... partilha de dados muitas vezes é para ofertas comerciais não para revelar aquilo que os clientes dispõem, uma oferta genérica, até relacionada com o perfil do cliente. O sigilo bancário é mais pessoal, tem a ver mesmo com aquilo que o cliente detém e não com as suas apetências...são perfeitamente compatíveis...” E3</p> <p>“...o sigilo bancário faz parte da proteção de dados, é um aspeto que engloba a proteção de dados. Esta depois tem outras dimensões... mas a confidencialidade e o sigilo bancário é precisamente uma delas, portanto, é completamente conciliável. A partilha de dados quando é feita tem de ser fundamentada e com as regras de segurança possíveis, mas digamos que há um casamento perfeito aqui...” E6</p> <p>“... sigilo bancário está assegurado, na medida em que o cliente até pode partilhar os dados connosco se entender que quer estabelecer e manter a relação de negócio connosco... está assegurado na medida em que o banco cumpra e não saiam para fora e da instituição e para fora daquilo que é o âmbito da relação de negócio... que os dados não sejam utilizados para outro fim...” E8</p> <p>“...considero que sim, que são fáceis de compatibilizar...(E8)</p> <p>“...acho que é perfeitamente possível, aliás uma coisa até reforça e complementa a outra... o RGPD veio reforçar, em primeira instância aquilo que é o sigilo bancário, para não andar nenhum documento descuidado, para não andar informação descuidada fora do circuito, para não se partilhar dados sem necessidade e sem autorização prévia dos clientes...” E10</p> <p>“... o RGPD, de uma forma genérica, visa proteger a informação relativa às pessoas e para que ela seja utilizada para o propósito a que se destina...E11</p>	<p>Perfeita compatibilização do RGPD e do sigilo bancário, reforçam-se e complementam-se, na medida em que os dados sejam apenas usados no âmbito da relação de negócio e não sejam usados para outro fim (E3), (E6), (E8), (E10)</p>	<p align="center">4</p>
<p>“...e no que respeita à compatibilização do sigilo bancário a as comunicações que têm de ser efetuadas é algo que está previsto pela lei do sigilo bancário e do RGPD...estas comunicações só podem ser efetuadas com as entidades já especificadas na lei e só para esse efeito.... E8</p>	<p>As comunicações que são feitas estão especificadas, a que entidades e para que efeitos (E8)</p>	<p align="center">1</p>
<p>“... se a partilha de dados não vai sair do âmbito do que é nossa instituição do que é o nosso banco, não vai mais além... porque se foi mais além já está interferindo no sigilo bancário...” E4</p>	<p>A partilha de dados dentro da instituição não colide com o sigilo bancário (E4)</p>	<p align="center">1</p>

Categoria I: Importância da compatibilização harmoniosa dos diplomas

Unidade de contexto	Unidade de registo	Frequência
<p>“... a proteção de dados aparece aqui também como um reforço ao sigilo bancário ... “E5</p> <p>...” o sigilo bancário é algo que está inerentemente ligado ao RGPD ainda que eventualmente não o mencione expressamente... “E11</p>	<p>RGPD vem reforçar o sigilo bancário, estão inerentemente ligados (E5), (E11)</p>	2
<p>...” poderia por vezes haver interesse em partilhar certo tipo de informação fora do banco... seria se calhar para benefício do próprio sistema bancário e isto numa ótica de prevenção de BC, para mitigação desses riscos... não o podemos fazer por causa do sigilo bancário... E11</p>	<p>Há informação que na ótica da prevenção de BC/FT não pode ser partilhada por causa do sigilo bancário (E11)</p>	1
<p>“... o RGPD protege os dados que são recolhidos dentro do banco com as várias finalidades que deles existem... dados, estamos a falar de informação das pessoas e, portanto temos informações financeiras, patrimoniais tudo o que é recolhido no banco nós olhamos para isso... mas eu não tenho dados específicos para o RGPD, isso não existe...Eu trato com os dados que o banco trata... portanto com dados do branqueamento de capitais, com os dados do risco, com dados comerciais que são oferecidos, com tudo isto não é, não tenho dados específicos de RGPD...” E6</p> <p>“...por exemplo nós quando abrimos uma conta... vamos usufruir daqueles dados que estamos a recolher para a restante relação contratual...no fim relação contratual temos de os conservar pelo prazo legal de 7 anos, por via da prevenção BC/FT... findo desse prazo temos que eliminar os dados e não podemos fazer uso a não ser para a gestão da relação contratual...” E7</p> <p>“... toda a informação com que trabalhamos está relacionada com a proteção de dados... E9</p>	<p>Não há dados específicos de RGPD, o banco trata dados, informação que recolhe por via de outras fontes (dados recolhidos na abertura de conta servem a relação contratual) e são eliminados ao fim de 7 anos após o fim dessa relação (A6), (A7), (A9)</p>	3
<p>“... RGPD é um tema recente, que ainda não está amadurecido, acho que obviamente aquilo que está na sua génese é claramente positivo, mas ele conflitua com uma série de áreas... E11</p>	<p>RGPD é um tema recente que conflitua com várias áreas (E11)</p>	1
<p>“...o sigilo bancário sim é uma preocupação que nós temos que ter, é algo que temos que respeitar bastante no nosso trabalho... tem que haver sempre esse cuidado de nós quando falamos com o cliente não falar em alto para outros clientes não ouvirem... nas perguntas de outro cliente nós não podemos partilhar</p>	<p>Consciência da importância do sigilo e do RGPD no dia-a-dia e da sua presença em todas as atividades (E1), (E2), (E4), (E5), (E6), (E8), (E9), (E10), (E11)</p>	9

Categoria I: Importância da compatibilização harmoniosa dos diplomas

Unidade de contexto	Unidade de registo	Frequência
<p>dados, temos que ter sempre cuidado às vezes mesmo em termos informais...” E1</p> <p>“...eu acho que o sigilo bancário é muito importante acho que na nossa na nossa atividade é dos mais importantes, mas lá está, eu também estou a pensar no sigilo bancário de nós em relação aos nossos clientes, não é?...E2</p> <p>“...não podemos fornecer informações sobre determinados clientes nomeadamente o número de telefone ou morada ou rendimentos auferidos a não ser ao próprio, falar de processos de outras pessoas, se calhar estes são os exemplos mais comuns...” E4</p> <p>“...do sigilo é essa mesmo, não passar informações de nenhum cliente a terceiros e a proteção de dados é igual...” E4</p> <p>“... primeiro as violações de sigilo bancário implicam que sempre que alguém partilhe para fora dados de clientes, e que não deveria... E5</p> <p>“a base é o sigilo bancário, mas até para evitar situações mais dramáticas, quando necessário temos de informar e ponto.” E6</p> <p>“... o sigilo bancário é absolutamente essencial à nossa função... E8</p> <p>“...toda a informação com que trabalho, sejam de processos estamos sob sigilo bancário...na nossa globalidade temos o sigilo e o RGPD com tudo o que envolve clientes...” E9</p> <p>“...sigilo bancário está desde o primeiro momento da carreira de um bancário, não há forma de fugir e de facto quem não o cumprir não está a fazer nada na profissão...” E10</p> <p>“...toda a gente tem consciência de manter esse pilar de relação com o mercado, com os clientes e com os parceiros, para o bem de todos, de uma forma muito transparente e também de uma forma muito clara dizer que não, que não podemos dar essa informação, face ao sigilo bancário...” E10</p> <p>...” está sempre presente porque nós temos o artigo 54º da Lei 83/2017 que é o dever de não divulgação que está constantemente a dar-nos nota de que não podemos partilhar certo tipo de informação... E11</p>		
<p>“...sim tenho esse cuidado de não partilhar os dados dos clientes que não o autorizaram até porque o banco faz diversas formações a esse nível e todos</p>	<p>Banco dá importância a estas matérias (E1)</p>	<p align="right">1</p>

Categoria I: Importância da compatibilização harmoniosa dos diplomas

Unidade de contexto	Unidade de registo	Frequência
<p>estamos alertados para essas situações e para as multas a que o banco está sujeito...” E1</p>		
<p>“...eu acho que o sigilo bancário é indispensável sempre, a não ser que sejam outras entidades por outros motivos que entraram em contato e que são públicas e naturalmente aqui é obrigado a responder, agora tipo se colide com RGPD eu não sei...” E2</p> <p>“...existem as exceções, nomeadamente o sigilo pode ser quebrado se houver alguma suspeitas, nomeadamente a nível das autoridades. Nessas situações deve estar tudo definido e nessas situações o banco terá que ser obrigado a fazê-lo, dentro dessas exceções...” E4</p> <p>“...eu acho que é à exceção de quando no BC/FT haja autorização expressa de uma entidade judicial a pedir esses documentos e nós temos de os facultar à luz da lei. Eu sou a favor do sigilo, não tenho dúvidas de que é importantíssimo neste processo, mas se houver necessidade de partilhar os dados de determinado cliente por questões de duvidosas que eu desconheço, e que de acordo com a lei terei de facultar...” E10</p> <p>...” nós não podemos partilhar oficialmente informação fora do banco sem termos a necessária autorização para a derrogação do sigilo bancário...” E11</p>	<p>A quebra do sigilo bancário pode existir com autorização expressa de entidades judiciais (E1), (E2), (E4), (E10), (E11)</p>	<p align="center">5</p>
<p>“...mesmo em relação ao sigilo bancário temos perfeita consciência que os bancos são repositórios gigantes de informação muito importante e que a mesma partilhada de forma indistinta, sem filtros ou sem qualquer cuidado poderá ser utilizada de forma indevida por parte de terceiros.... E11</p>	<p>Os bancos são repositórios gigantes de informação importantes (E11)</p>	<p align="center">1</p>
<p>“...não é muito fácil... há áreas que se tocam e há áreas que se repelem. Muitas vezes temos que ver temos que dar prioridade àquelas que sejam mais urgentes. Por vezes para dar seguimento a uma proteção de dados não poderíamos revelar certas coisas que serão do âmbito do BC. Há que ter um certo bom senso para saber qual delas é mais urgente tratar e dar prioridade...” E3</p>	<p>Necessidade de ponderação de valores e interesses em causa e em conflito (E3)</p>	<p align="center">1</p>
<p>“... e depois a questão da luta contra o BC aquilo que está em causa é a própria transparência do setor, o reconhecer o cliente, o definir regras de atuação com clareza e evita o FT ou tráfico de estupefacientes, pessoas, etc. ...garantir que no sistema bancário</p>	<p>BC/FT tem a ver com a transparência do setor e evita a sua contribuição para a prática de crimes (E10)</p>	<p align="center">1</p>

Categoria I: Importância da compatibilização harmoniosa dos diplomas

Unidade de contexto	Unidade de registo	Frequência
<p>estão atividades lícitas, que ajudam a economia a crescer, com transparência e rigor e com toda aquilo que é o contributo positivo de cada empresa ou particular para aquilo que são os impostos de cada país...se toda a gente tiver essa consciência é tudo mais fácil para todos...” E10</p>		
<p>“...já com o branqueamento de capitais não é bem a mesma coisa...” E6</p>	<p>A compatibilização entre RGPD e sigilo com BC/FT não é tão fácil (A6)</p>	<p align="center">1</p>
<p>“... a prevenção de BC para garantir o cumprimento da lei, que deriva das diretivas da UE, consagra uma série de deveres em que sobretudo dois: o dever de exame e o dever de diligência, fazem com que o nosso trabalho tenha de ser um bocado intrusivo; admito que por vezes para garantirmos o cumprimento e a análise de risco de BC... podemos ter de recolher informação que eventualmente colida com o que está definido no RGPD...” E11</p>	<p>O dever de exame e diligência fazem com que a análise seja intrusiva e que recolha informação que colide com o RGPD (E11)</p>	<p align="center">1</p>
<p>“...dos 3 sem dúvida que para mim é o branqueamento de capitais, sigilo bancário e proteção de dados também não temos dúvida, mas sem dúvida que a prevenção e branqueamento de capitais deve prevalecer porque quem faz isso está a prejudicar outras pessoas e acho que aí não se deve colocar a questão do sigilo bancário, ou a proteção de dados...” E1</p> <p>“...ok estava a falar dos direitos liberdades e garantias do sigilo, mas o BC/FT é um crime e provavelmente aqueles deixam de ter tanta importância senão seria um encobrimento desse crime” E3</p> <p>“...coloco no topo o BC porque tem implícito o RGPD e o sigilo, abarca os dois: os dados sensíveis têm de ser tratados com cuidado e simultaneamente é o sigilo completo...” E9</p> <p>“...o sigilo é a base, a luta contra o BC está na segunda etapa e o RGPD, é um direito do consumidor, mas tem menos impacto naquilo que é uma irregularidade que possa haver.... o RGPD, do meu ponto de vista é o que cria menos efeitos. Eu até posso partilhar alguns dados com empresas do grupo, mas não é isso que vai causar um problema grave, apesar de o consumidor ter direito a definir se eu posso partilhar ou não. Se eu quebrar o sigilo bancário é muito grave e a quebra de controlo das regras de BC também é muito grave. Sigilo equivalente com a luta da questão do BC, e depois</p>	<p>Prevenção de BC/FT mais importante que o sigilo bancário e proteção de dados e engloba os outros dois (E1), (E3), (E9), (E10), (E11)</p>	<p align="center">5</p>

Categoria I: Importância da compatibilização harmoniosa dos diplomas

Unidade de contexto	Unidade de registo	Frequência
<p>uma segunda terceira etapa para o RGPD. Acho que este é mais teórico do que pratico...” E10</p> <p>...” tem sido entendido como uma premissa até agora que as matérias sobre prevenção de BC sobrepõem-se às matérias de proteção de dados... obviamente que eu tendo a concordar com isto...” E11</p>		
<p>“... se a lei não for alterada, existe um interesse específico mais importante que exceciona o RGPD (E11)</p> <p>“... se fores pesar os bens jurídicos que se pretendem acautelar acho que é legítimo que devemos recolher para esta finalidade específica os documentos de identificação dos clientes porque é um bem superior que estamos a combater... e a utilização das instituições como veículos para a prática de crimes.... acho que a grande maioria dos clientes não se opõe ao cumprimento e no limite quando muito, dão o consentimento...” E7</p>	<p>Se a lei não for alterada, existe um interesse específico mais importante que exceciona o RGPD (E7), (E11)</p>	<p align="center">1</p>
<p>“... ou seja, respeitando na mesma o sigilo bancário, mas depois só o quebrar quando efetivamente há alguma suspeita e nós temos que fazer a comunicação das operações suspeitas a quem de direito... eu acho que eles na prática se ajudam uns aos outros...por isso acho que eles se complementam e que são indispensáveis, apesar de parecerem conceitos um bocadinho opostos...” E2</p>	<p>Sigilo bancário e BC/FT complementam-se (E2)</p>	<p align="center">1</p>
<p>“...temos os direitos, liberdades e garantias que o sigilo e a proteção de dados dão, mas por outro lado temos o BC/FT que poderá trazer graves consequências caso os procedimentos não sejam cumpridos. É difícil, essa é muito difícil” E3</p> <p>“.. nem sempre a CNPD tem abertura suficiente para entender que os deveres que nós temos no âmbito da prevenção do BC/FT se devem sobrepor aos deveres que resultam diretamente da lei da proteção de dados...”E7</p>	<p>Conflito de deveres do RGPD e BC/FT e dificuldade em saber qual o direito mais importante a proteger (E3), (E7)</p>	<p align="center">2</p>
<p>“...acho que o sigilo bancário é primordial e também já existe há muito tempo... quer dizer, o BC também, mas o sigilo bancário é daquelas coisas que é transversal a todos os clientes e o branqueamento de capital não. Não toca a todos os clientes, nem sequer à maioria dos clientes e só acabamos por ter um tratamento naqueles clientes em que existe alguma suspeita...E4”</p>	<p>Sigilo bancário mais abrangente que o BC/FT (E4)</p>	<p align="center">1</p>

Categoria I: Importância da compatibilização harmoniosa dos diplomas

Unidade de contexto	Unidade de registo	Frequência
<p>“...acho que não punha de lado nenhum... são importantes os 3, apesar de parecerem conceitos que colidem, acho que se complementam acho que é difícil dispensar um...” E2</p> <p>“...acho que se complementam apesar de serem coisas diferentes, mas não chegam a tocar uma nas outras. Acho que vão todas no mesmo sentido, vão todas na mesma direção que é a proteção do cliente, mas sempre dentro de atividades legais não fugindo daí...” E4</p> <p>“...não consigo dizer porque honestamente eu vejo os dois com igualdade de importância porque no fim do dia, havendo alguma falha grande da parte do Banco em algum dos dois o impacto reputacional para o banco, a nível de risco reputacional será igualmente grande. À data de hoje se calhar uma reportagem na TVI e na SIC etc, sobre temas de BC/FT é mais prejudicial para o banco do que uma reportagem equivalente a nível de RGPD, de sigilo bancário. Por esta razão eu diria que à data de hoje se calhar o BC/FT mas no fim do dia e na definição global, os dois. E na teoria eu diria equivalentes...” E5</p> <p>“...São leis, que podemos dizer que, basicamente são comuns. Podemos dizer que o sigilo bancário basicamente se confunde com o dever de guarda da confidencialidade do tratamento de dados... e quando há exceções são exceções concretas e determinadas e conseguimos comprovar o porquê da exceção...E7</p> <p>“...acho que a própria lei é bastante clara em relação a isso e, portanto, não há aqui qualquer incompatibilidade e não me parece que seja difícil...” E8</p> <p>“...dentro da banca e onde trabalhamos nós estamos todos obrigados ao sigilo bancário. Entre nós temos de ter esse cuidado... depois com o relacionamento com outras entidades, mesmo entre a nossa direção com outra partilhamos situações, mas nunca detalhando clientes ou informação sensível, pessoal, por exemplo nos seguros de saúde...mas sim é possível compatibilizar...” E9</p> <p>“...eu acho que são possíveis de compatibilizar. A questão da transparência da banca que queremos dar para com o mercado, do rigor e salvaguardar os interesses quer do consumidor, quer de todos, neste caso até da própria nação, acho que tudo isto são complementos necessários para a nossa atividade. O sigilo bancário por aquilo que é o reconhecimento da nossa discrição e da nossa reserva sobre a partilha de</p>	<p>Equiparação dos 3 regimes: complementam-se e não colidem (E2), (E4), (E5), (E7), (E8), (E9), (E10)</p>	<p align="center">7</p>

Categoria I: Importância da compatibilização harmoniosa dos diplomas

Unidade de contexto	Unidade de registo	Frequência
informações dos clientes, que é o primeiro fator de confiança...” E10		
“... as exceções são documentadas e temos um fundamento específico para excecionar o sigilo ou para excecionar a confidencialidade dos dados... no fundo, mas são basicamente, eu diria que em termos práticos que se confundem... porque o objetivo é o mesmo: salvaguardar os dados... E7	As exceções são documentadas para poder comprovar às entidades de supervisão (E7)	1
<p>“... sigilo e a proteção de dados é o casamento perfeito... o sigilo é uma componente da proteção de dados... No BC/FT quanto menos sigilo tiver que cumprir, quanto mais souber melhor... aliás esta é uma temática que é muito discutida a nível europeu também e das instituições e como é que estas duas realidades se conjugam...” E6</p> <p>...” são dois regimes que não estão harmonizados, que são algo conflitantes... há um cuidado acrescido no que toca ao tratamento de informação... mas no que toca à parte de termos informação necessária para analisar o risco fazemo-lo em respeito daquilo que é a lei do BC... que nos dá margem para pedir determinado tipo de informação...” E11</p>	A compatibilização entre RGD e sigilo com BC/FT não é tão fácil e é muito discutida; são regimes que não estão harmonizados e são conflitantes, mas a lei dá margem para se pedir determinado tipo de informação (A6), (A11)	2
<p>“...existem vários fundamentos de licitude do tratamento dos dados. Há aqui 4 fundamentos que estão sempre presentes: 1, o óbvio, o legal: há circunstâncias em que nós temos que tratar os dados propostos por força da lei e posições do Banco de Portugal ou do BCE, por exemplo a abertura de conta, que obrigatoriamente tem que ser tratado um conjunto de dados que não está na vontade das partes deixá-lo de fazer ou não; depois temos um outro, o contratual nós como temos contratos com os nossos clientes para determinado tipo funções ou serviços temos de tratar os dados deles, a banca digital por exemplo... temos que tratar para efeitos do cumprimento do nosso contrato com clientes e depois existe uma coisa que é consentimento. O consentimento é muito específico e só aplicado em 2 circunstâncias muito concretas, que é para efeitos da perfilagem clientes, do seu comportamento para lhes poder fazer ofertas e para efeitos de ações de marketing enviadas por e-mail, por telefone ou carta... só para este dois se utiliza o consentimento. E depois existe ainda um quarto grupo que é o do legítimo interesse do banco, há circunstâncias em que o banco trata dados dos clientes, um conjunto restrito de dados, no seu legítimo interesse, mas até já muitas vezes em formato quase a anonimizado ou pseudo-anonimizado... o regulamento também</p>	Existem 4 fundamentos para a licitude do tratamento de dados: legal, contratual, consentimento e legítimo interesse do Banco (E6)	

Categoria I: Importância da compatibilização harmoniosa dos diplomas

Unidade de contexto	Unidade de registo	Frequência
<p>permite que ele possa existir, mas sempre precedido de uma análise de equilíbrio entre o que é o interesse do Banco e do titular dos dados. O legítimo interesse do banco não se pode sobrepor, àquilo que seria o legítimo interesse titular dos dados... mas existem muitas circunstâncias que têm a ver com a gestão, com a contabilidade, com auditorias que obrigam a que sejam tratados dados dos clientes e mesmo dos colaboradores e que a base deles é muitas vezes o legítimo interesse do banco, como o BC/FT” ... B6</p>		
<p>“...tens que por um lado a prevenção do BC/FT que visa basicamente combater a prática de crimes que são muito danosos para a sociedade como um todo, mas em particular para o sistema financeiro...obviamente que isto mina completamente a sociedade. Estamos a fomentar aqui a incidência de crimes que estão na origem, na base de crimes de BC.... a lei do branqueamento de capitais existe com um racional bastante compreensível para o comum dos cidadãos...E7</p> <p>“... se fores pesar os bens jurídicos que se pretendem acautelar acho que é legítimo que devemos recolher para esta finalidade específica os documentos de identificação dos clientes porque é um bem superior que estamos a combater... e a utilização das instituições como veículos para a prática de crimes.... acho que a grande maioria dos clientes não se opõe ao cumprimento e no limite quando muito, dão o consentimento...” E7</p>	<p>Fundamentos da lei de BC/FT são compreendidos por todos (E7)</p>	<p align="center">1</p>
<p>“...a Lei de BC... fala no dever de não divulgação e, portanto, no que toca à proteção de dados há um cuidado acrescido no que diz respeito ao tratamento da informação para garantir que o banco não informa terceiras pessoas de que há clientes que estão a ser alvo de uma análise especial ...tudo o que sejam clientes comunicados às autoridades, o próprio cliente não pode ter conhecimento disto e está inclusivamente consagrado na lei e há uma pena de prisão até 3 anos para quem violar isto...” E11</p>	<p>Lei BC consagra o dever de não divulgação que se relaciona com o cuidado acrescido na proteção de dados (E11)</p>	<p align="center">1</p>
<p>“...no que toca à proteção de dados há um tratamento da informação na área de prevenção de BC que tem uma natureza confidencial... as análises que fazemos e os resultados dessas análises são só mantidos dentro da área e não são partilhados para fora...E11</p>	<p>A área de prevenção BC/FT trata de informação confidencial e que não pode ser partilhada (E11)</p>	<p align="center">1</p>

Categoria II: Fatores críticos na implementação (RGPD, LBC e SB)

Unidade de Contexto	Unidade de Registo	Frequência
<p>“...nós todos os dias para podermos contactar os clientes, temos que ter em consideração se eles têm o RGPD no sistema ou não...se já foi recolhido...se o cliente não tiver RGPD sempre que estamos com o cliente ou que temos a oportunidade, temos que recolher para ter esse ponto tratado, para respeitarmos as respostas do cliente... “E1</p> <p>“...depois da entrada do RGPD na nossa atividade tivemos que ir atualizando a ficha de cliente à medida que tínhamos cá o cliente, os contactos, moradas e outras informações que até vieram a ser adicionadas à ficha de cada cliente. Dá-lhes uma proteção maior e desde essa altura passaram a ter mais confiança...” E4</p> <p>“... julgo que aqui ao nosso nível está ligado com o facto de ligarmos ou não ligarmos aos clientes, conforme eles queiram ou não ser abordados e aquilo que eles indicaram quando estabeleceram ou quando quiserem alterar esse tipo de informação...” E8</p> <p>“...mudou de facto porque todos os processos têm de ser desenhados numa lógica de recolher o consentimento, portanto no desenho, na conceção dos processos temos de ter em mente a proteção de dados...” E9</p> <p>“... a pessoa pode dar-nos o consentimento e ser alvo de campanhas, pode ser selecionado por mailings para enviarmos. Não sendo, fica restrita esta informação, não pode ser selecionado para campanhas, não podemos enviar por exemplo o dia de aniversário...” E9</p> <p>“...com a introdução desse documento obrigatório o banco tomou logo uma série de medidas para implementar essa proteção de dados do consumidor, foi o primeiro banco a fazê-lo, pediu para em todos os momentos, desde uma pequena simulação aos parceiros, o que criou logo um constrangimento naquilo que foi a procura dos parceiros ao CH do Banco BPI...” E10</p> <p>“...não, não é um documento generalista que exatamente permite que o nosso parceiro que tem um contrato de intermediação de crédito conosco e que está devidamente autorizado no BdP, possa recolher os dados desse cliente ou potencial cliente, enviar para o Banco BPI e este com base nesse documento poder dar a resposta ao parceiro mediante a autorização do cliente...” (E10)</p>	<p>Obrigatoriedade de recolha do RGPD, atualização de dados e recolha de assinatura (E1), (E4), (E8), (E9) (E10)</p>	<p align="center">5</p>
		<p align="center">2</p>

Categoria II: Fatores críticos na implementação (RGPD, LBC e SB)

Unidade de Contexto	Unidade de Registo	Frequência
<p>“...os bancos e a maior parte das empresas não tinham tratado e logo aí foi necessário grande trabalho de recolha e que ainda estamos a fazer... alguns clientes ainda não conseguimos contactar e nesse sentido foi uma foi um grande acréscimo em termos de trabalho para os balcões...” E1</p> <p>“...temos que recolher a ficha de informação, o cliente tem que assinar, tem de dizer o que é que quer em termos de proteção de dados, aceitar ou não aceitar e aí depois temos todo o processo de digitalizar, assinar digitaliza, enviar, ou seja, toda a parte documental que não é não é assim às vezes tão rápido... e depois há sempre situações em que um documento se extraviou, temos que recolher novos documentos, ou seja um acréscimo de trabalho...” E1</p> <p>“...RGPD foi bastante disruptivo porque veio criar obrigações muito superiores às que existiam e com um impacto muito grande para as instituições não estavam adaptadas às obrigações do RGPD... também muito impacto em sistemas sobretudo, no desenvolvimento de sistemas de execução das tarefas porque tivemos que criar um gabinete específico de proteção de dados... veio criar obrigatoriedade de termos um DPO...” E7</p> <p>“...todas as restantes áreas tiveram impacto sejam operacionais sejam depois na motorização na segunda linha do risco e depois pela terceira linha na motorização como um todo do sistema de adequação ao RGPD...” E7</p>	<p>Após a entrada em vigor do RGPD os impactos foram grandes e houve necessidade de várias adaptações em todas as áreas do banco, com acréscimos de trabalho e novas obrigações para os colaboradores, nomeadamente a criação do DPO (E1), (E7)</p>	
<p>“...esta parte muito burocrática da assinatura, da constante recolha da FII e como disse muitas vezes até de clientes que estão longe e que não têm acesso aos canais automáticos, até pela idade dos clientes acho que deveriam pensar numa forma de otimizar isto e o próprio banco se são clientes há tanto tempo poder uma análise e uma filtragem dos clientes a contactar para fazer a recolha da proteção de dados e do branqueamento de capitais...” E1</p>	<p>Recolha constante da assinatura da FII, com acréscimo de dificuldade nos clientes emigrantes e mais idosos (E1)</p>	<p align="center">1</p>
<p>“...claro que os clientes acabam por ficar mais salvaguardados nesse sentido porque tem a certeza de que os dados deles não vão ser utilizados para além daquilo que eles nos autorizaram...mas em termos do nosso dia a dia, do nosso trabalho foi muito complicado e depois também em termos da prática comercial...” E1</p> <p>“...a grande novidade, digamos que agora assumiu uma proporção um bocadinho diferente, mas que tem a ver com o tratamento dos dados precisamente</p>	<p>Importância do RGPG para os clientes (E1), (E6), (E9), (E11)</p>	<p align="center">4</p>

Categoria II: Fatores críticos na implementação (RGPD, LBC e SB)

Unidade de Contexto	Unidade de Registo	Frequência
<p>para efeitos de <i>marketing</i> direto ou para efeito de ofertas personalizadas, portanto de marketing direto... E6</p> <p>“dever e obrigação das entidades que tratam dados pessoais de informarem os seus clientes sobre os termos do tratamento e uma delas é a transferência desses dados... é uma das caracterizações que nós fazemos do tratamento de dados que registámos na aplicação, uma das perguntas tem a ver precisamente se são transferidos dados para fora, nesses casos para quem são transferidos temos que identificar as entidades e porquê...” E6</p> <p>“... a pessoa pode dar-nos o consentimento e ser alvo de campanhas, pode ser selecionado por mailings para enviarmos. Não sendo, fica restrita esta informação, não pode ser selecionado para campanhas, não podemos enviar por exemplo o dia de aniversário...” E9</p> <p>“... o RGPD determina que não se podem copiar os documentos dos clientes... mas já é um princípio de tentar harmonizar... a questão da chave móvel digital mas todos caminhamos para lá... seguramente esta barreira vai ser ultrapassada a favor daquilo que é o RGPD e de futuramente não copiarmos certos documentos dos clientes...” E11</p>		
<p>“...não teve se calhar tanto impacto como era esperado porque acho que honestamente é um requisito legal que o banco tem de cumprir, não é algo que a instituição compreenda exatamente. Teve impacto na medida em que são mais 6 perguntas que o cliente tem de responder e em que foi obrigatório nós recolhermos essa mesma informação. Honestamente em termos de impacto acho que não aconteceu absolutamente nada...” E8</p>	<p>RGPD não teve impacto que nas práticas do banco, que não a recolha do consentimento (E8)</p>	<p align="center">1</p>
<p>“...há clientes para quem provavelmente o que está prescrito é suficiente, mas há outros que obrigariam a existir situações mais específicas e numa linguagem mais abrangente face à situação sócio profissional de cada um...” E3</p>	<p>Necessidade de adaptar o texto do RGPD face ao perfil e situação socio profissional do cliente (E3)</p>	<p align="center">1</p>
<p>“...esse normativo aliás prevê todas estas situações que possam existir e obriga a estes incidentes sejam tratados dentro de 72 horas que deles tomamos conhecimento, que é outra coisa que também não casa muito bem com as violações de sigilo não é, porque nestes casos banco vai gerindo, aqui não, eu tenho 72 horas para resolver esse problema, para fazer uma análise dele eu e a direção de segurança,</p>	<p>Obrigaçãõ acrescida de comunicar ao titular dos dados o que lhe for especialmente prejudicial, em 72 horas (E6), (E7)</p>	<p align="center">2</p>

Categoria II: Fatores críticos na implementação (RGPD, LBC e SB)

Unidade de Contexto	Unidade de Registo	Frequência
<p>que é um pivô muito importante deste procedimento...” E6</p> <p>“...basicamente a DPO tem uma intervenção grande, a direção de segurança, como sabes temos 72 horas para se apurar que a violação de dados com está dentro dos requisitos estabelecidos para comunicação ao regulador ou supervisor, portanto eu diria que aí tens que cumprir o circuito estabelecido no normativo específico de violação de dados...” E7</p>		
<p>“...mas eu depreendo que mesmos os próprios colaboradores só podem... utilizar os dados de clientes para um fim concreto e determinado da sua atividade... não é suposto consultar dados de outros clientes senão estás a violar o dever de confidencialidade e de segredo dos dados, a fazer um uso indevido dos dados dos clientes porque não tens legitimidade para consultar aqueles dados, portanto eu diria que se calhar, nas áreas de negócio isso tem mais impacto...” E7</p>	<p>O sigilo e a confidencialidade têm mais impacto nas áreas comerciais (E7)</p>	<p align="center">1</p>
<p>“...primeiro o banco teve de ser adaptar e o que nós fizemos foi um levantamento das situações internas do banco e que podiam não estar tão adequadas ao RGPD e desse levantamento que foi feito resultaram 21 medidas necessárias de implementar. Umás óbvias não é, como processos relacionados com a violação de dados, que não existiam, processos relacionados com o exercício de direitos, não existiam, uma política de privacidade que não existia, o registo dos tratamentos que não existiam, a avaliação de risco que não existia, mas depois há todo um conjunto de medidas mais tecnológicas relacionadas mais com a segurança que também tivemos que começar a desenvolver e são essas que atrasam mais os efeitos...” E6</p> <p>“...mudou de facto porque todos os processos têm de ser desenhados numa lógica de recolher o consentimento, portanto no desenho, na conceção dos processos temos de ter em mente a proteção de dados...” E9</p> <p>“...depois com a adaptação que fizemos aos sistemas, no fundo fomos aliviando, pelo menos a primeira etapa que é uma pequena consulta que muitas vezes até nem traz grandes dados dos clientes, mas garantindo que o banco ao final de 30 dias destruiria todas a documentação que tem...E10</p>	<p>RGPD teve impacto nas práticas do banco e no desenho de todos os processos, houve necessidade de implementar 21 medidas internas e adaptar os sistemas para cumprir o RGPD (E6), (E9) (E10)</p>	

Categoria II: Fatores críticos na implementação (RGPD, LBC e SB)

Unidade de Contexto	Unidade de Registo	Frequência
“...o banco tem que dinamizar um pouquinho mais também a parte de sensibilização das pessoas... isto é um tema que está mais administrativo...” E5	Necessidade de sensibilização de todos os colaboradores para esta temática (E5)	1
“...vai depender muito da capacidade e da vontade do interlocutor de nos dar essa informação porque muitas vezes quando tratamos por exemplo com emigrantes que já estão afastados de Portugal há muito tempo é difícil a recolha de algum tipo de informações, ou porque não dominam os meios informáticos ou porque nem entendem algumas das expressões...” E3	Dificuldade de recolha de informação de clientes emigrantes e explicar-lhes essa necessidade (E3)	1
“... mas a lei portuguesa já consagra que no âmbito da recolha da informação de pessoas sempre que o cliente der nota que o pretende fazer através da chave móvel digital deve ser disponibilizado isso.... mais uma vez há um problema de operacionalidade disto, porque a chave móvel digital ainda não é uma ferramenta largamente disseminada quer na sociedade, quer mesmo nos bancos...” E11	Utilização da chave móvel digital como forma de cumprimento do RGPD, mas com o problema de operacionalidade porque a chave móvel digital não está amplamente disseminada (E11)	1
...e essa adaptação foi feita, também foi feito o reconhecimento, nomeadamente em grandes parceiros do seu próprio RGPD dando nota daquilo que eram correções necessárias para o banco, no fundo, validar esse documento em substituição do nosso e por isso posso-lhe dizer que teve impacto na minha atividade para o CH, nomeadamente no canal de intermediação de crédito que são os parceiros imobiliários... E10	Validação e correção do documento de consentimento remetido através de parceiros (E10)	1
“... a questão da proteção de dados ainda é imatura, ela tem de ser mais atuante, quando tiver de ser penalizante que penalize, que não pode demorar eternidades... perceber que a proteção de dados, ao dia de hoje, é como tentar parar um tsunami...” E11 “... o regime de proteção de dados é muito recente, nasceu de uma forma algo utópica e precisa de se compatibilizar com a vida real... numa altura em que as redes sociais, internet das coisas, mundo digital... nossos dados, numa altura em que cada vez circula mais informação, mais depressa, acho que o regime de proteção de dados precisa de evoluir para perceber, em concreto, como é que ele próprio se compatibiliza com esta partilha cada vez maior de dados que existe e cada vez mais depressa e cada vez para mais sítios...” E11	Imaturidade e falta de eficácia do RGPD, que tem, ele próprio, de se compatibilizar com a vida real de circulação de informação rápida e por todo o lado (E11)	1
“...teve este alerta, hoje em dia quando é criada qualquer coisa, qualquer serviço para fora ou mesmo qualquer processo interno, que envolve	Necessidade de todos os processos de negócio estarem de acordo com o RGPD (E6)	1

Categoria II: Fatores críticos na implementação (RGPD, LBC e SB)

Unidade de Contexto	Unidade de Registo	Frequência
<p>colaboradores normalmente a proteção de dados está sempre presente porque sempre que implique tratamento de dados pessoais deverá ter sempre a nossa análise, e tendo em consideração isso mesmo o desenho dos próprios processos...” E6</p> <p>“...a questão da proteção de dados nessa componente do sigilo bancário não é uma novidade para o setor bancário que teve sempre uma preocupação muito grande com sigilo bancário e com a confidencialidade e, portanto, sempre montou os seus processos com base nesse pressuposto...” E6</p>		
<p>“... agora sim há uma preocupação acrescida porque existem obrigações acrescidas relativamente à confidencialidade que é eu ser obrigada a comunicar quando ela seja especialmente prejudicial para os titulares de dados...essa proteção não existia efetivamente, mas na sua génese, na sua substância a confidencialidade já era uma preocupação...” E6</p> <p>“...a questão da proteção de dados nessa componente do sigilo bancário não é uma novidade para o setor bancário que teve sempre uma preocupação muito grande com sigilo bancário e com a confidencialidade e, portanto, sempre montou os seus processos com base nesse pressuposto...” E6</p>	<p>O sigilo bancário e a confidencialidade sempre estiveram nos pressupostos de todos os processos (E6)</p>	
<p>“... as pessoas não se preocupam muito com essa situação, muitas vezes até se coloca tudo sim ou não para não aborrecer o cliente e para ele não estar a fazer perguntas.... em primeiro lugar, e que é muito simples, é explicar exatamente às pessoas a importância do RGPD e não isto ser-nos imposto e ser feito em e-learning com 200 slides para justificar à entidade reguladora...porque é que isto é obrigatório, porque é que nós temos de saber isto, quais são as consequências legais e envolvermos as pessoas que tratam disto diariamente...essa é a principal lacuna...” E8</p>	<p>Colaboradores pouco preocupados com o RGPD e desconhecimento das consequências em caso de incumprimento (E8)</p>	<p align="center">1</p>
<p>“...mas acho que para mim a parte em que são mais incompatíveis entre si e gerando-se alertas branqueamento de capitais e tendo que se ir atrás dos clientes a pedir documentação comprovativa da origem de fundos e a pessoa diz ah foi uma herança e a seguir o banco diz ok mas queremos uma escritura da herança, precisamos de evidências não serve só palavra... uma pessoa fazer um depósito em numerário superior a x e tem que dizer onde é</p>	<p>Incompatibilidade entre o RGPD, que supõe o mínimo de informação de dados pessoais e o BC/FT, que supõe o máximo de informação, a conciliação é difícil por terem objetivos, princípios e prazos de conservação opostos (E5), (E6), (E7), (E11)</p>	<p align="center">4</p>

Categoria II: Fatores críticos na implementação (RGPD, LBC e SB)

Unidade de Contexto	Unidade de Registo	Frequência
<p>que vem o dinheiro e em caso de ter alguma situação mais estranha vão-lhe pedir evidências, ou seja, as coisas não são incompatíveis neste sentido mas há um meio termo que acho que vai difícil mas possível de encontrar, no fim do dia...” E5</p> <p>“...BC/FT versus RGPD eu acho que existe sempre um ponto em que é possível compatibilizar, mas acho que são os 2 temas em que se calhar é mais difícil, são os temas que mais chocam por exemplo na perspetiva dos clientes... para cumprirmos com a legislação de prevenção de branqueamento de capitais temos de recolher um mundo sobre o cliente... acaba por se calhar, ser um bocadinho contra o princípio do RGPD em si, portanto eu vejo-os como incompatíveis nesta perspetiva, ou seja um caminha para um lado e outro caminho para o lado completamente oposto, mas acho que há formas de compatibilizar qb...” E5</p> <p>“... às vezes e o banco tem que reportar muita coisa a entidades oficiais, que são da vida dos seus clientes e estes não sabem que estão a ser reportadas, portanto também diria que se calhar é um casamento um bocadinho complicado...” E6</p> <p>“... vamos lá ver as questões de BC /FT vivem costas voltadas para as questões da proteção de dados, elas não casam bem... no BC/FT quero saber mais, uma maior informação possível sobre os clientes e não clientes...quero saber de tudo, guardar tudo e durante o maior tempo possível. Na proteção de dados o que é que nos diz? só devo recolher aquilo que eu preciso, pelo tempo que eu preciso e só devo usar para isso mesmo. Portanto vivem de costas voltadas umas para as outras e esta conciliação às vezes é difícil sem dúvida nenhuma...” E7</p> <p>“...acho que não são fáceis de compatibilizar porque o RGPD procura proteger a informação das pessoas de uma forma simples e no que toca ao BC/FT uma das coisas que contribui para esta situação é a opacidade é a ausência de informação... isto conflitua um bocado com o RGPD porque este entende que a informação só deve ser disponibilizada o mínimo possível ou ser a estritamente necessária... nós temos de ter uma análise muito alargada no tempo para perceber qual é o padrão que está a acontecer ou então temos de alargar o perímetro de informação e temos, pedir mais informação... E11</p> <p>“... há um risco a gerir que é o risco de BC e esse risco gere-se com informação... portanto eu acho</p>		

Categoria II: Fatores críticos na implementação (RGPD, LBC e SB)

Unidade de Contexto	Unidade de Registo	Frequência
que eles conflituam os dois e não sei como se vão harmonizar... E11		
<p>“...quer dizer há uma série de preocupações que nós temos hoje que não tinha há algum tempo atrás... acresce tarefas? claro, porque tem que haver aqui um controlo diário das contas dos nossos clientes...” E2</p> <p>“...é um dos temas que está sempre muito em cima da mesa na nossa atividade sobretudo a nível de formações e aí uma coisa que temos de fazer é ter atenção à movimentação das contas, mas não, acréscimo de tarefas e preocupações não, a mim não. Acho que não é só uma questão de estarmos mais atentos a alguma movimentação anormal das contas ou quem faz caixa também se aperceber um bocadinho daquilo que está a passar com cada cliente e realmente o que se achar estranho reportar...” E4</p> <p>“...eu tenho metade da minha carteira para analisar... isto é completamente incompatível com uma relação de negócio... o cliente sente que está a ser escrutinado..., mas por outro lado isto não pode ser feito por outra pessoa que não o gestor...” E8</p>	Acréscimo de tarefas para cumprir a prevenção de BC/FT, como por exemplo controlo de movimentação de contas e que atrapalha a relação comercial (E2), (E4), (E8)	
<p>“...acho que se devia encontrar um equilíbrio porque também em nome de uma segurança que nunca é uma segurança a 100 % porque não existe risco zero, em nome de uma segurança que as pessoas hoje em dia procuram, deixam atropelar um conjunto de direitos que têm, e eu não sou muito favorável a isso confesso, mas é essa a realidade que nós vivemos hoje em dia e por isso é que cada vez mais é difícil este diálogo. Nas sociedades ocidentais o que se vive é essa a tendência para o risco zero e no que diz respeito então ao BC/FT as pessoas aceitam que muitas vezes os seus direitos sejam arrasados em nome desse dessa segurança. Eu como não acho essa segurança exista, nem acho que deva ser assim, eu acho que tem que se arranjar um ponto de equilíbrio...” E6</p>	Dificuldade em encontrar um ponto de equilíbrio entre os direitos que o RGPD preconiza e a segurança a 100% e o risco zero (E6)	1
<p>“...houve de facto um reajustamento interno, quer em processos quer em pessoas... há uma dinâmica e uma evolução constante que faz com que nos tenhamos que constantemente a adaptar, muitas vezes até mais a reagir.... E11</p>	Reajustamentos internos de pessoas e processos para responder à constante evolução das matérias de BC/FT (E11)	1
<p>“...muitas vezes também criamos processos que não são exatamente aqueles que a lei diz... a lei dá-nos um objetivo que é o combate ao BC/FT, mas</p>	A forma e procedimentos de tratamento de dados não é dada	

Categoria II: Fatores críticos na implementação (RGPD, LBC e SB)

Unidade de Contexto	Unidade de Registo	Frequência
<p>não nos diz como é que fazemos e a forma como fazemos, que pode ser mais ou menos invasiva dos direitos e interesses dos clientes...” E6</p>	<p>pela lei e pode ser mais ou menos invasiva (E6)</p>	
<p>“...no fundo acho que já está compatibilizado e tens justificação para a recolha por isso acredito que está sempre compatibilizado” E7</p> <p>...” mas acho que havendo conflito aqui deve prevalecer o que mais protege não só as instituições e as pessoas de forma individual, mas a própria sociedade...qui teremos sempre legitimidade e a CNPD tem dificuldade em refutar que não temos uma lógica muito válida subjacente à recolha desses elementos e da documentação relacionada...” E7</p> <p>“...no <i>compliance</i> nós temos de tratar os dados, independentemente de RGPD, de aceitação ou não do tratamento. É completamente diferente o tratamento do RGPD para um marketing ou para um <i>compliance</i>... para o marketing ou rede comercial o RGPD tipifica o cliente, consegue uma oferta consoante as suas características, etc....no <i>compliance</i> não se verifica, eu não quero que me entre dentro de casa alguém que não é suposto, que nós não queremos,... traz risco reputacional, financeiro, etc... portanto os dados são trabalhados, têm outro tipo de sigilo, outro tipo de cuidados e acho que é tudo compatível...”E9</p> <p>“...houve uma comunicação há uns meses ao nível das autoridades bancárias da europa que basicamente alertaram para que os futuros regimes do branqueamento de capitais devam ter em atenção a proteção de dados... estão a ser lançadas novas diretivas que depois são transpostas para a lei de cada país... questão que essa autoridade falou foi no sentido de tentar harmonizar ao máximo possível estas duas questões... E11</p>	<p>Compatibilização entre RGPD e BC/FT (E7), (E9), (E11)</p>	<p align="center">3</p>
<p>“...basicamente é o KYC, que é o conhecermos o cliente e qual a movimentação esperada da conta, saber se tem contacto com outras jurisdições, se são jurisdições de risco, nível de rendimentos, tipo de rendimentos, para onde vais transferir, de onde é que vem o dinheiro, tentar perceber partes relacionadas com as quais poderá ou não receber ou enviar valores. E depois de termos estas fotografia do cliente é perceber se o perfil dele enquadra ou não com aquela que é a movimentação real da conta...” E8</p>	<p>Importância do KYC (E8)</p>	<p align="center">1</p>
		<p align="center">1</p>

Categoria II: Fatores críticos na implementação (RGPD, LBC e SB)

Unidade de Contexto	Unidade de Registo	Frequência
<p>“...e depois temos de ter os dados comprovados em algum lado...temos de garantir que essa informação fica disponível como um documento de suporte...” E9</p> <p>“...depois é segregado, quem faz a admissão de clientes não faz a investigação de clientes, eu própria estando numa área de projetos não tenho determinados acessos. É só o estritamente necessário...” E9</p> <p>“... rede comercial é que envia sempre, faz a captação do cliente e conhece e deve conhecer em primeira linha... todas a informação está residente na aplicação de pessoas e contas e depois de comprovados os dados vão para outra área para se fazer a aceitação do risco... “E9</p> <p>“...essa aceitação do risco requer uma análise prévia da documentação, se foi entregue, se é verdadeira, se está atualizada e tudo mais, isto através da aplicação GP que comunica connosco...” e dá-se a decisão, o risco é aceite e o cliente pode a partir daí abrir conta...não sendo aceite, procede-se à desvinculação do cliente, ou ao bloqueio daquele cliente até que nos dê a informação que nós achemos necessária para a aceitação do cliente, abertura de conta, operações de crédito, etc...” E9</p>	<p>Necessidade de garantir a existência de documentos de suporte de comprovação de dados e como se faz a admissão de um cliente (E9)</p>	
<p>“...a evolução da sociedade, da informação faz com que vão surgindo novas tipologias no que toca à utilização indevida dos sistemas financeiros para efetuar BC... a legislação e a regulação se vá alterando, se vá ajustando e consequentemente nos vivemos quase que num período de transformação constante... os controles que nós temos ao dia de hoje para mitigar o risco de BC, não se mantém durante a mesma forma durante muito tempo... vão evoluindo porque vão surgindo ou tipologias novas, situações que nós vamos detetando ou legislação e regulação nova que obriga o banco a adaptar-se... E11</p>	<p>A evolução da sociedade, da informação, da tipologia de utilização do sistema financeiro as alterações legislativas obrigam o banco a constantes adaptações (E11)</p>	<p align="center">1</p>
<p>“...tudo o que fazemos é registado e deve ser disponibilizado às autoridades sempre que elas peçam, e porque a lei também determina o dever de colaboração...mas é muito importante que esta independência consiga produzir uma decisão que seja auditável, que seja clara que seja perceptível por um terceiro que a venha ler...” E11</p>	<p>Registo de toda a informação que possa ser disponibilizada às autoridades judiciais e setoriais de forma que seja auditável e perceptível a terceiros (E11)</p>	<p align="center">1</p>
<p>“... na questão do BC existe a necessidade, pela natureza da análise, de ser melhor quanto mais informação houver, o que significa que podemos ter</p>	<p>Na questão do BC/FT a informação nunca é a mais (E11)</p>	<p align="center">1</p>

Categoria II: Fatores críticos na implementação (RGPD, LBC e SB)

Unidade de Contexto	Unidade de Registo	Frequência
informação a mais, mas a informação para BC nunca é a mais porque quando muito vai servir para ser utilizada pela negativa, ou seja, vai servir para concluir que não há suspeita... E11		

Categoria III: Aumento da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
<p>“...eu acho que poderia ser feito tipo uma SMS com um alerta para o cliente fazer nos canais digitais e não ter que se estar à espera do cliente vir ao banco para tratar disso... alguma coisa que fosse mais intuitiva e que alertasse o cliente para essa necessidade... para irem à APP... naqueles que só vão ao balcão aí só mesmo aguardando que eles vão...” E1</p> <p>“...eu acho que podia ser o próprio cliente que fazia numa aplicação, não há outra forma que não seja o próprio cliente, mas acho que tem que haver depois do controle da nossa parte por isso acho que sim, sempre com controlo da nossa parte. Nós tiramos cópia, digitalizamos no momento, tens a certeza que é original... não há grande alternativa...” E2</p> <p>“...no sentido de permitir que os clientes possam atualizar dados sobretudo para os clientes que são dos canais digitais...porque hoje em dia esses podem atualizar os seus dados dentro dos canais que é outra coisa que é uma preocupação muito grande do RGPD, que é eu tratar dados atualizados e que é também uma preocupação do branqueamento de capitais, mas com objetivos diferentes não é?...porque eu quando tenho dados desatualizados o resultado é que eu faço um tratamento mal feito da informação...permite às pessoas fazerem essas atualizações aos que não são vamos tentando sempre que há um ponto de contato com eles fazer essa atualização e tem havido muitas campanhas...porque é uma preocupação muito grande do banco, com várias dimensões e uma delas é proteção de dados.” E6</p> <p>“...tentar eliminar coisas que não interessavam e eliminar coisas que ficam desatualizadas rapidamente e conseguimos esse trabalho sobretudo no digital quando a pessoa abre a conta à distância. Hoje em dia a informação que é recolhida do cliente é inferior àquela que é nos balcões e onde ainda não conseguimos lá chegar...” E6</p> <p>“...estando no banco BPI e estando em projetos eu diria que já estamos bastante avançados na recolha dos dados nos balcões é muito fácil, os consentimentos são muito rápidos... poder fazê-los através das Apps, das linhas telefónicas, eu acho que estamos muito desenvolvidos... acho que é uma boa prática... é uma preocupação ser realmente simples, ter todas a informação disponível, mas ser algo simples para o cliente... E9</p>	<p>Alerta por SMS, com avisos para RGPD e atualização de dados a realizar nos canais digitais (E1), (E2), (E6), (E9)</p>	<p align="center">4</p>
		<p align="center">1</p>

Categoria III: Aumento da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
<p>“...se fosse por exemplo esta situação em termos de telefone e ser feito nos serviços centrais passava para zero trabalho para o balcão. Se não passar pelo balcão era muito mais rápido porque uma gravação de 5 10 minutos e ficava feito já não era preciso da outra parte todo do tratamento processual...” E1</p> <p>“...seria a gravação por telefone pelos serviços centrais que contactasse os clientes e fizessem o questionário, de ficar com a gravação telefónica... porque não... não obrigar a nova ficha de informação individual, a nova assinatura, ao cliente ter que ir ao balcão... acho que facilitava muito se houvesse uma possibilidade de ser dessa forma, retirando toda a parte burocrática de recolha de documentos de assinaturas de papéis... seria bastante mais simples ...” E1</p>	<p>Autorizações RGPD por gravação de chamada de voz, o que reduzia tempo de tratamento do processo (E1)</p>	
<p>“...eu acho que o que podia ser mais simples e que estamos a implementar já é a comprovação de dados através das chaves móveis digitais, que é um passo bastante bom...” E9</p> <p>“...a única coisa que eu acho, e já temos essa possibilidade, mas que é pouco utilizada é a chave móvel digital e o cartão de cidadão por PIN e a assinatura... mas os clientes particulares usam pouco...” E10</p> <p>“...para já aquilo que me ocorre é mesmo a chave móvel digital...” E11</p>	<p>Aposta nas chaves móveis digitais para recolha, tratamento e comprovação de dados e CC com PIN (E9), (E10), (E11)</p>	<p align="center">2</p>
<p>“...como posso tornar isto mais digital? só mesmo através dos dois fatores, assinatura digital certificado ou PIN do CC, só assim sabemos que foi a pessoa... Portanto só mesmo com uma assinatura, não consigo simplificar mais este processo para garantir que cumpro...” E10</p>	<p>Assinatura do cliente é a única prova do consentimento, se for digital, melhor (E10)</p>	<p align="center">1</p>
<p>“...acho que já está simplificado e não está muito exaustivo... são perguntas praticamente de sim ou não... a partir do cartão de cidadão hoje já se consegue comprovar várias coisas, identificação pessoal, o contribuinte, a morada está tudo já muito facilitado a esse nível... não vejo nada a melhorar...” E4</p>	<p>Procedimento de RGPD simplificado, com perguntas de sim ou não e não há aspetos a melhorar nos processos de recolha e tratamento de dados (E4)</p>	<p align="center">2</p>

Categoria III: Aumento da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
<p>“...mas no limite acho que podem desconhecer as consequências das suas ações e se isto não for amplamente divulgado primeiro numa ótica de sensibilização, de não deve ser feito e avançando depois para uma ótica de sensibilização de o que acontece se for feito, acho que em tudo o que diz respeito a sigilo bancário, RGPD e outros tantos temas acho que é uma coisa que o banco tem imenso para melhorar e pode robustecer bastante todos estes processos mesmo o BC/FT, que entre os 3 acaba por ser o tema mais divulgado. Acho que com mais sensibilização certas coisas não digo, não acontecem, mas acontecem menos...” E5</p> <p>documento e há sempre formas de tornar as coisas mais compatíveis...” E5</p>		
<p>“... A partir do cartão de cidadão hoje já se consegue comprovar várias coisas, identificação pessoal, o contribuinte, a morada está tudo já muito facilitado esse nível...” (E4)</p> <p>“...por exemplo o banco atualmente já está a aceitar para abertura de conta a leitura eletrónica do cartão de cidadão e com isto é possível fazer a comprovação por exemplo da morada da residência da pessoa, se calhar já não temos que pedir a fatura da luz, etc é menos uma série de documentos...” (E5)</p>	<p>Importância da leitura do CC na atualização de vários dados (E4), (E5)</p>	<p align="center">2</p>
<p>“... há pequenas iniciativas que vão com certeza ajudar, como é a questão da chave móvel digital, para evitar que se andem a tirar cópias de documentos...isso também traz benefícios para a própria questão do BC pois a informação por via digital e eletrónica e vir de entidade oficiais, partimos do princípio que é fidedigna e não manipulada, portanto aí há uma melhoria... E11</p>	<p>Tratamento de informação por via digital e eletrónica como a chave móvel evita informação manipulada e crença na sua fidedignidade (E11)</p>	<p align="center">1</p>
<p>“...nas Apps as fotografias servirem também como comprovativo e a pessoa não ter de se deslocar é uma boa pratica e a informação chega logo, o que torna o processo muito mais célere...” E9</p>	<p>Aposta na utilização de fotografias enviadas pela APP para comprovação de dados (E9)</p>	<p align="center">1</p>
<p>“...poderia ser mais uma situação para se fazer uma assinatura digital, que nós já temos, após preenchimento no sistema, ... e já não nos obrigar a fazer a digitalização, a imprimir, o cliente assinar a ficha de informação individual, que nós digitalizamos e enviarmos para arquivo... e aquilo ficava lá, já não obrigando a que nós fôssemos fazer digitalizações e tudo mais acho que poderia ser mais fácil...” E1</p>	<p>Assinatura digital e fim da assinatura em papel (E1), (E7)</p>	<p align="center">2</p>

Categoria III: Aumento da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
<p>“...eu acho que se calhar o que podemos fazer e apostar nos canais digitais, na recolha digital, usar tablet, em vez de nos focarmos tanto no papel... acredito que a digitalização possa ser um caminho útil para as primeiras linhas, agora em termos legais quero crer que estamos sempre a cumprir com o motivo de recolha... E7</p>		
<p>“... eu peço os documentos comprovativos de rendimentos, nacionalidades, várias moradas, que me trazem pessoalmente, em papel ou digital, através de email...o que acontece é que após introduzirmos a informação informaticamente, porque quanto mais informatizada estiver a informação mais facilmente chegamos a coerências ou incoerências...” E8</p> <p>“...depois de introduzidas no sistema informático, a informação é digitalizada e fica disponível no nosso arquivo digital. E depois os colegas que analisam também têm acesso por essa via à documentação...” E8</p>	<p>Importância da informatização dos dados para estar ao acesso de todos (E8)</p>	<p align="center">1</p>
<p>“... aquilo que fizemos primeiro foi salvaguardar o banco, ao destruir a documentação das simulações e decisões prévias que não avancem para propostas, ao fim de 30 dias e garantir que todas as propostas que entrem em sistema têm o documento de RGD devidamente assinado pelo cliente a dar autorização ao nosso parceiro para poder enviar para cá os documentos e nós podermos responder ao nosso parceiro...” E10</p>	<p>Salvaguarda do banco no que toca à troca e análise de dados pessoais enviados pelos parceiros (E10)</p>	<p align="center">1</p>
<p>“...é por email e o que nós estamos a preparar uma plataforma de comunicação às grandes redes para o fluxo poder ser integrado diretamente no nosso GPC, que é no fundo o motor de decisão de crédito...” E10</p> <p>“... e depois aquilo que queremos fazer ao longo deste ano é fazer uma evolução para integrar também os documentos ou de uma forma manual ou de uma forma, enfim com um robot por trás, a fazer a integração dos documentos nas pastas respetivas ...” E10</p>	<p>Evolução operacional na recolha e tratamento de documentos com a criação de nova plataforma que permite a comunicação dos sistemas dos parceiros com o sistema do banco, o motor de decisão (E10)</p>	<p align="center">1</p>
<p>“...conseguimos ajustar o mecanismo do GP para limpar todo o sistema ao fim de 30 dias, desaparece tudo o que nos permite nessas duas etapas... E10</p>	<p>Dados desaparecem ao fim de 30 dias sem evolução (E10)</p>	<p align="center">1</p>
<p>“...podemos sempre automatizar e é isso que estamos a fazer... há reportes que têm de ser feitos, obrigatoriamente de informação e estamos a automatizá-los, para não haver erros, quebras de sigilo...” E8</p>	<p>Banco está a postar na automatização (E8)</p>	<p align="center">1</p>

Categoria III: Aumento da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
<p>“... e a sistematização de procedimentos internos do Banco que irão ajudar a que o próprio sistema tenha menos quebras do sigilo bancário...ou seja se os sistemas do Banco já estiver pré parametrizados para evitar determinado tipo de situações, de fugas...” E5</p>	<p>Necessidade de os sistemas informáticos estarem parametrizados na identificação de quebras de sigilo e de RGPD (E5)</p>	
<p>“...eventualmente só mesmo tendo o cliente alguma plataforma onde pudesse descarregar a informação e que alguém pudesse controlar, confirmar a fiabilidade da documentação e da informação e eventualmente não houvesse intervenção do balcão..., mas acho que é sempre importante passar pelo gestor...” E2</p>	<p>Existência de plataforma para descarregar documentos enviados pelos clientes, sem intervenção do balcão e do gestor (E2)</p>	1
<p>“...estamos a tentar desenvolver também a fiabilização dos mails, quando os recolhemos não é, porque os clientes às vezes enganam-se escreveu mal ou colaborador engana-se a ouvir..., portanto sim existem coisas que podem ser melhoradas neste nível, estamos num processo de mudança...” E6</p>	<p>Executar a fiabilização dos emails dos clientes para evitar perdas de informação (E6)</p>	1
<p>“...ter por exemplo os emails encriptados em vez de emails simples quando se remete a informação... da parte da informática e sempre a encriptação para proteção desses dados...” E9</p>	<p>Importância da encriptação de emails para troca de informação com dados pessoais (E9)</p>	1
<p>“... desde que tenhamos os canais expedidos de comunicação com a DPO ou com as áreas que têm o dever de melhorar a qualidade... é quase como funcionar com a perspetiva de controlo interno, todos os colaboradores se identificam uma possibilidade de melhoria...devem conseguir comunicar uma deficiência e haver um plano de ação...” portanto eu diria que aqui se o banco, cada um dos colaboradores, atuar no âmbito do modelo de controlo interno acho que conseguimos sempre corrigir as eventuais fragilidades que existam no sistema” E7</p> <p>“...eu acho que era muito importante nós percebermos exatamente aquilo que os colegas precisam e nós tínhamos de ter canais mais diretos com eles...”</p>	<p>Necessidade de existência de canais expeditos para todos os colaboradores comunicarem a identificação de melhorias, comunicação e deficiências e existir um plano de ação (E7), (E8)</p>	2
<p>“... eu diria que para RGPD é continuar o que estamos a fazer, que é em todos os processos de negócio, ou de crédito, o que seja, a temática do RGPD tem de estar lá. Em todos os produtos, para além da informação contratual tem uma parte para o cliente assinar o RGPD, mesmos nos canais digitais...estar no fluxo...” E9</p>	<p>Colocar o tema do RGPD e do consentimento no fluxo de todos os processos (E9)</p>	1

Categoria III: Aumento da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
<p>“...o ideal era que não fosse a rede a tratar disso, acho que se conseguíssemos ter alguém no banco a tratar disso era excelente, mas claro que contato com cliente tem que ser sempre nosso, nós é que somos os gestores de conta é natural que o contato e os pedidos sejam nossos... mas eventualmente tentar descentralizar um bocadinho esta responsabilidade... que houvesse alguém que pudesse fazer o controlo dos movimentos diários...” E2</p>	<p>Descentralizar a monitorização dos movimentos de conta (E2)</p>	1
<p>“...eu acho que podia ser melhor eu acho que podemos sempre melhorar aqui algumas coisas do ponto de vista processual: uma coisa que depois não implique perda de qualidade da informação que recolhemos. eu acho que é que é mais nesse sentido, ou seja, em prol de poupar algum tempo, não descurar uma parte que depois é importante para nós e para o banco...” E2</p>	<p>Reconhecimento da importância de agilização de processos, mas sem perda de qualidade de informação (E2)</p>	1
<p>“...acesso a mais informação para quem trata destes assuntos e até dar opiniões sobre melhorias a efetuar... passa tudo pelo acesso ao conhecimento...” E3</p> <p>“...eu acho que era muito importante nós percebermos exatamente aquilo que os colegas precisam e nós tínhamos de ter canais mais diretos com eles...” E8</p>	<p>Necessidade de mais informação e conhecimento sobre estas matérias, para melhor as executar e dar opinião sobre os processos e tarefas (E3), (E8)</p>	2
<p>“... a questão dos emigrantes que são clientes há muito tempo e com patrimónios não muito elevados poderia ser perfeitamente eliminada...” E3</p>	<p>Eliminação da remediação para clientes antigos e com patrimónios elevados (E3)</p>	1
<p>“...acho que devia haver uma alguma listagem com aquilo que eles realmente pretendem, e eu acho que também depende um bocadinho de quem trata...que me tenha percebido uns pedem a inscrição no SEF, há outros que não pedem...devia haver um parâmetro para todos e para ser mais fácil chegarmos à aceitação mais rápido possível...” E4</p>	<p>Necessidade de existência de uma <i>check-list</i> para orientar o processo de recolha e uniformização da parte de quem trata, para tornar os processos mais rápidos (E4)</p>	1
<p>“... para mim não vejo se haveria mais alguma coisa que pudesse adicionar àquele impresso...” E4</p>	<p>Informação a preencher é suficiente (E4)</p>	1
<p>“... mas no limite acho que podem desconhecer as consequências das suas ações e se isto não for amplamente divulgado primeiro numa ótica de sensibilização, de não deve ser feito e avançando depois para uma ótica de sensibilização de o que acontece se for feito, acho que em tudo o que diz</p>	<p>Necessidade de sensibilização de todos os colaboradores para esta temática (E5)</p>	1

Categoria III: Aumento da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
respeito a sigilo bancário, RGD e outros tantos temas acho que é uma coisa que o banco tem imenso para melhorar e pode robustecer bastante todos estes processos mesmo o BC/FT, que entre os 3 acaba por ser o tema mais divulgado. Acho que com mais sensibilização certas coisas não digo, não acontecem, mas acontecem menos...” E5		
“...olhe uma coisa com a qual nós debatemos e que é uma obrigação, e que é uma novidade é quando nós recolhemos dados através de terceiros, nossos parceiros... existe sempre uma obrigação da nossa parte de informar os titulares dos dados sobre o que é que nós vamos fazer com aqueles dados, não é? e portanto aí há todo um trabalho que nós temos andado a fazer e que é uma melhoria passível de ser feita...” E6	Obrigação de informar os titulares dos dados que chegam através de parceiros sobre o tratamento que vai ser dado aos seus dados pessoais (E6)	1
” ...outras é os tipos de dados que nós recolhemos...não vale a pena que recolher dados desnecessários ou dados que se desatualizam muito... nesse aspeto o banco tem feito um esforço de só recolher efetivamente aquilo que é necessário, é o princípio do <i>privacy by default</i> ... os processos do banco estão a ir nesse sentido... a ter essa evolução e portanto nos momentos em que eu recolho os dados, tenho de tem que informar os meus clientes e só devo ter recolher aquilo que necessito mesmo.” E6	Princípio do <i>privacy by default</i> (E6)	1
“...no fundo se as primeiras linhas tivessem se calhar o trabalho mais eficiente se calhar os resultados que nós temos com os reguladores, os processos não tinham tanto impacto no nosso dia-a-dia, mas isso é uma questão de otimizar sempre as tarefas de primeira linha e não tanto de segunda...” E7	Otimização dos processos na fase inicial, a de contacto com o cliente, vai otimizar os processos com os reguladores (E7)	1
“...tarefas que se podem eliminar penso que ainda não estamos nessa fase de poder eliminar, tudo o que se faz é realmente necessário... o que pode ser padronizado está-se a padronizar...” E9	Ainda não estamos numa fase de eliminação de tarefas, mas de padronização (E9)	1
“...no BC/FT, pensando mais na admissão e sendo um tema novo a remediação penso e partir de agora que já temos definido o que se pretende e que a rede já o conhece a necessidade de conhecer o cliente e perceber o que está em causa e não meramente executar, sabe que cuidados se devem ter...” E9	Importância de definir bem o que se pretende nos processos de KYC e explicar o porque dessa necessidade (E9)	1
“...criámos uma <i>task force</i> de apoio à rede comercial para saberem exatamente quais são os documentos	Criação de <i>task force</i> de apoio para explicar os processos e procedimentos necessários (E9)	1

Categoria III: Aumento da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
<p>que tinham de enviar e como é que se processava basicamente...”E9</p> <p>“...ou até haver um helpesk direto para nós... pessoas formadas e familiarizadas que despachem entre colegas, sem superioridade. tem de haver um espírito comum de entreajuda...” E8</p>		
<p>...” a proposta de melhoria seria a própria formação...” E3</p> <p>“...apostámos fortemente em formação, tínhamos uma colega quase 100% dedicada à formação, um bocadinho mais de topo, mas também à rede comercial...” E9</p> <p>“...explicar o processo, o que tem de se fazer o que temos de pedir, de enviar... também falar o que é que é isto do BC ... porquê temos de o fazer e o porquê dos procedimentos...” E9</p>	<p>Importância da formação em geral e importância de explicar o porquê dos processos de BC/FT para melhor serem compreendidos por quem os executa (E3), (E9)</p>	<p align="center">2</p>
<p>“...apostámos também em ter um canal para <i>compliance</i> no helpdesk, que não havia...agora há uma linha própria com formação aos elementos...portanto mais canais, formações e informações na intranet cada vez que verificávamos erros frequentes...” (E9)</p>	<p>Criação de canal para dúvidas com elementos formados e mais formações e informação na intranet, com alertas para os erros frequentes (E9)</p>	<p align="center">1</p>
<p>“...claro habilitar as equipas com mais pessoas para o tratamento, que não estava minimamente dimensionado, mas agora estamos a fazer esse trabalho e também acho que será melhor porque a rede já conhece o processo...” E9</p> <p>“...ou então por lá mais recursos humanos...” E10</p>	<p>Mais pessoas na análise dos processos de BC/FT (E9), (E10)</p>	<p align="center">2</p>
<p>“...as autoridades estão a trabalhar na criação de um canal para estas comunicações, mas ao dia de hoje ainda não existe. Portanto o canal que é disponibilizado para os bancos e outras instituições é o email...” E11</p>	<p>Criação de um canal próprio para comunicações com entidades externas (E11)</p>	<p align="center">1</p>
<p>“... no sentido que o GP posso ser segregado apenas pelo órgão de onde vem a informação, ou seja, a informação só fica disponível para o órgão que a enviou... o processo começou de uma forma muito básica, muito arcaica, mas tem tido várias evoluções... ao dia de hoje é uma das melhorias que podia ser feita...” E11</p>	<p>Evolução do processo de troca de informação e disponível só para quem a trata (E11)</p>	<p align="center">1</p>
		<p align="center">1</p>

Categoria III: Aumento da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
<p>...” sugestões de melhoria seria ter um canal dedicado para as comunicações suspeitas...E11</p> <p>...” questão de construir canais privilegiados para troca de informação é sempre um bom princípio até para a própria gestão de informação, para garantir que existe um repositório dedicado... E11</p>	<p>Criação de um canal dedicado à comunicação de operações suspeitas (E11)</p>	
<p>“... o que estamos a fazer é sobretudo na rapidez de processo, estamos a desenvolver robots para obtermos a informação mais depressa, informação que já está dentro do banco para ela ser recolhida...e informação externa ao banco, ou que está em fonte aberta, no google e por aí, ou que está em determinados sites que nós pagamos... que têm bases de dados... E11</p>	<p>Maior rapidez no processo de recolha de informação interna e externa através da criação de robots (E11)</p>	1
<p>“... no caso de BC/FT eu diria que sim, porque o dever de comunicação é instantâneo ... digamos que nunca acontece instantaneamente, mas logo que possível... no caso do RGPD, julgo que é trimestral e posso estar equivocada, não o conheço assim tão bem, mas da última vez que vi alguma coisa sobre isso pareceu-me ser trimestral e, portanto, se calhar eu diria que não, e deveria caminhar mais para o instantâneo...” E5</p>	<p>Necessidade de reportes instantâneos às autoridades de controlo (E5)</p>	1
<p>“...existiam aplicações por exemplo que recolhiam os mesmos dados ficavam lá umas e depois outras elas depois não conversavam... Isso era gerador de muitos erros no envio das comunicações...” E6</p>	<p>Necessidade de comunicação entre os vários sistemas que guardam dados de clientes (E6)</p>	

Categoria IV: Redução da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
<p>“...fez com que nós tivéssemos que recolher todos os documentos novamente, com que os clientes tivessem que assinar a ficha de informação porque muitos dos clientes que estão lá fora não vem cá, não têm a APP nem acesso aos canais digitais foi muito complicado conseguir gerir isso e foi um acréscimo de trabalho muito grave... E1</p>	<p>Recolha constante da assinatura, com acréscimo de dificuldade em clientes emigrantes e idosos (E1)</p>	<p align="center">1</p>
<p>“... termos do relatório de risco que nós temos que preencher...neste momento tem 17 páginas... só para imprimir preencher e digitalizar todo esse esse documento acho que é uma burocracia e um acréscimo de trabalho tremendo para os balcões o que nos tira muitas vezes o nosso tempo para outras tarefas que são muito importantes...” E1</p>	<p>Relatórios de risco muito extensos (E1)</p>	<p align="center">1</p>
<p>“...é o cliente que nos traz em papel, os originais dos documentos, nós fotocopiamos, a nova ficha de informação individual assinada pelo cliente onde nós preenchemos os dados da relação do negócio... onde o cliente nos diz se vai fazer ou vai receber transferências do estrangeiro, ou não, quais os montantes. de que países é que também vai receber ou fazer...porque motivo... essa informação colocamos também no relatório de risco e depois digitalizamos tudo e é criado um processo e se for risco elevado será enviado para a outra área, que irá analisar e depois se necessário mais algum documento ou esclarecimento é nos solicitado... e nós temos que responder e sempre que alteramos uma informação qualquer dos dados pessoais do cliente temos que recolher nova ficha de informação individual e digitalizá-la para acompanharem...” E1</p>	<p>Recolha de documentos e assinatura presencial, digitalização, envio para tratamento e repetição do procedimento sempre há alterações ou correções (E1)</p>	<p align="center">1</p>
<p>“... mas há sempre essa necessidade de pedir os documentos, de nos virem entregar os documentos...não há outra forma de sabermos se os documentos são originais... acho que a análise poderia ser mais célere leva um tempo para clientes novos...mas para quem já é nosso cliente e que não tem qualquer problema ter a conta bloqueada uns quantos meses acho que é chato..., quando entregou tudo e tratou de tudo...” E1</p> <p>“...está a ser uma grande carga para os balcões a questão da remediação, e os clientes de risco elevado são de facto os que nos dão mais trabalho...os médios acabam por ser fáceis de tratar mas todos os clientes que têm um risco elevado já carecem de uma análise</p>	<p>Morosidade na validação dos processos aceitação de clientes de risco elevado torna os processos pouco eficientes (E1), (E4), (E8), (E10)</p>	<p align="center">4</p>

Categoria IV: Redução da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
<p>superior, o que é sempre sempre um processo que é demorado...” E4</p> <p>“...se calhar a média andar por volta de uma semana e meia por aí, até ao fim, até o processo ficar concluído. Há uns mais rápidos e há outros que é bem mais lento, acredito que se calhar ao nível de serviço da área que validada também esteja a ser mais complicado porque estão com muitos processos para tratar...” A4</p> <p>“...eu perco muito tempo, muito... por exemplo, a minha carteira é basicamente de não residentes estrangeiros...pessoas que têm muitos negócios e várias empresas... existe aqui alguma atenção e capacidade até de compreensão... estar a pedir rendimentos, encaixar isto nos <i>templates</i>, naquilo que são os nosso formulários, estar a explicar isto a um colega do que analisa depois a informação tem de bater toda exatamente com que está na ficha de informação com o que está no relatório e bater tudo certo com os documentos de suporte que o cliente nos dá...” E8</p> <p>“...<i>delays</i> de 15 dias ou um mês é impossível...” E8</p> <p>“... única questão que eu sinto é que quando há um cliente novo há demoras significativas na aprovação ou não do cliente... acho que isso é que se poderia efetivamente melhorar, os timings de resposta na análise...” E10</p> <p>“... a minha experiência no exterior foi isso, papeis para cima, papeis para baixo, por correio. ...hoje já não, é digital... a constatação que eu tenho é que o processo de análise é muito moroso e nada contra isso...” E10</p>		
<p>“... em termos de proteção de dados se calhar uma meia hora... o cliente ir ao balcão, nós questionarmos, preencher digitalizar e enviar, mais ou menos uma meia hora se tudo correr bem e a ficha não for extraviada no correio... se por acaso a ficha for extraviada isso duplica porque temos que estar a recolher novamente e ia fazer todo um novo trabalho que acontece porque é papel e por vezes pode acontecer., processo da ficha e tudo mais...” E1</p>	<p>Problema do extravio dos documentos assinados (E1)</p>	<p align="center">1</p>
<p>“...no momento da abertura de conta tudo o que sejam documentos originais normalmente eu tiro sempre fotocópia porque tenho sempre medo da digitalização não funcionar então depois digitalizo, coloco nas pastas para tratamento o e coloco na trituradora...” E2</p>	<p>Utilização de papel e digitalização para os mesmos documentos por medo da perda de informação digital (E2)</p>	<p align="center">1</p>
		<p align="center">1</p>

Categoria IV: Redução da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
<p>“...não sei até que ponto é que se consegue agilizar mais porque a gente pede ao cliente, o cliente envia, nós analisamos e depois encaminhamos, não sei do ponto de vista prático o que é que podíamos fazer de forma diferente tendo em conta que nós temos que analisar também a documentação. É o procedimento possível...” E2</p>	<p>Procedimento atual é o possível dada a necessidade de análise da documentação para efeitos de BC/FT (E2)</p>	
<p>“...se calhar podia ser poupado alguma algum tempo depois na parte da digitalização, do arquivo... se não tivesse a nossa intervenção, mas na prática estava ali alguém para analisar com mais calma e guardava e punha nas pastas e depois não se não esquece de pôr uma página e tens que fazer outra vez o processo e pronto isso leva tempo quando tens 1500 coisas...” E2</p> <p>“... os clientes por vezes são mal-educados, já perderam a paciência...depois são os processos que são devolvidos várias vezes..., porque não bate, porque falta...” E8</p>	<p>Aplicação que gere processos digitais muito morosa, com constantes devoluções por falta de páginas ou de associações erradas às pastas respetivas (E2), (E8)</p>	<p align="center">1</p>
<p>“...depende de cliente para cliente. há situações que podem ser tratadas em meia hora e outras que levarão 2 horas...isto é uma questão até da própria disponibilidade do cliente e da informação que nos presta... na questão da remediação ou do BC... porque muitas vezes o que acontece é que o cliente não está nada familiarizado com isto e até nós próprios não fomos suficientemente formados e que vamos ter que questionar mais do que uma vez, quando bastaria uma...” E3</p>	<p>A eficiência nos processos está muito dependente da resposta e disponibilidade dos clientes (E3)</p>	<p align="center">1</p>
<p>“...acho que se calhar às vezes poderiam ser ligeiramente mais ágeis, ou seja, digo isto porque em Portugal em concreto cada vez que é preciso fazer uma comunicação de BC/FT ela tem que ser feita a duas instituições, coisa que não acontece noutros países... portanto se fosse feita a uma instituição só todo o processo seria mais ágil...para mim isto é um ponto de melhoria... E5</p> <p>“...” em Portugal como somos muitos imaginativos... de comunicarmos para duas entidades a Unidade de Comunicação Financeira da PJ e o DCIAP da PGR...em qualquer outro país só se comunica para as UIF’s... E11</p>	<p>Em Portugal o reporte de BC/FT é feita para duas entidades distintas (E5), (E11)</p>	<p align="center">1</p>
<p>“...eventualmente as dificuldades que sentimos enquanto trabalhamos com mais de um departamento dos órgãos de controlo, que são muito grandes e que eles próprios não comunicam entre si... informação que envias para departamentos diferentes... podia tornar-se mais eficaz se houvesse comunicação interna</p>	<p>Regulador por vezes pede informação mais do que uma vez porque os diferentes setores não comunicam entre si (E7)</p>	<p align="center">1</p>

Categoria IV: Redução da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
<p>dos reguladores e a partilha de informação entre os vários departamentos dos reguladores facilitariam a vida às instituições porque não expediriam informação de mais do que uma vez e duplicada...” E7</p> <p>“...acho que os reguladores/supervisores apesar de ter os canais instituídos quando recebem a informação devia haver uma compatibilização da informação recebida e que fosse acessível aos vários departamentos para tornar o processo com contacto com as instituições mais eficientes, isso claramente sim.” E7</p>		
<p>“...e isso pode até prejudicar o cliente, porque os clientes vão aonde têm a sua conta domiciliada e onde o seu gestor os conhece e ter a imagem e a fotografia do cliente eu vejo como uma medida de segurança, para nós e para o cliente...mas compreendo que o cliente possa ver aí uma exposição da sua imagem e não querer...” E8</p>	<p>Recolha da imagem do CC é uma questão de segurança para todos (E8)</p>	<p align="center">1</p>
<p>“...mas na verdade eu penso que ninguém está preocupada ou tem esse problema em mente, ninguém vai consultar o RGPD do cliente...” E8</p>	<p>RGPD não é consultado frequentemente porque não é de visualização automática e instantânea (E8)</p>	<p align="center">1</p>
<p>“...os colegas que validam a informação em termos de arquivo digital recusam muitas vezes informação que apesar de não cumprir o que eles têm de aceitar, precisam de perceber que ainda que não cumpra exatamente aquele requisito, é importante para ficar associado ao cliente e isso facilitaria muita coisa em termos de tempo...” E8</p>	<p>A importância da documentação arquivada não é consensual (E8)</p>	<p align="center">1</p>
<p>“...com comunicações que só podem acontecer através daquele canal próprio...” E8</p> <p>“...compreendo que não seja possível o envio direto para os colegas, mas facilitaria muito... há um canal intermédio e perde-se muito coisa. Mas compreendo que sejam os outsourcings necessários, mas ou estes são mais envolvidos aqui neste papel, ou há muita coisa que se perde e que não funciona da forma mais eficiente...E8</p> <p>...”eu envio um processo porque considero que tenho todos os documentos...o colega vai-me responder daqui a 15 dias... isto aqui não está bem... e eu volto a pedir ao cliente... passada uma semana, ele envia e eu volto a introduzir no processo e vai faltar outra coisa qualquer...E andamos assim. Isto não é produtivo, não é eficaz. este canal entre a primeira</p>	<p>A dificuldade de comunicação entre as áreas e inexistência de canais diretos dificultam a eficiência (E8)</p>	<p align="center">1</p>

Categoria IV: Redução da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
linha e segunda não poder ser assim, teria de ser um canal direto..."E8		
<p>"...porque o tema é muito delicado... nós que estamos na rede temos interesse em fazer negócio e manter o cliente, mas compreendemos que existam questões muito superiores e que tem de ser esclarecidas... mas isto ainda passar por uma terceira área... o negócio do banco é fazer negócio comercialmente..." E8</p> <p>"... a dificuldade que tem é que o comercial quer vender, e tem objetivos de venda e o de compliance, é a venda tudo bem, mas também é proteger o banco..." E9</p>	Processos de BC/FT prejudicam o negócio e a prática comercial (E8), (E9)	1
<p>"... questão de mobilidade que há de estar estudada a nível estratégico, e faz com que não exista conhecimento de cliente absolutamente nenhum..." E8</p>	Mobilidade como inimiga do KYC (E8)	1
<p>"...nas empresas, a questão do BE, na recolha do RCBE acho que podíamos fazer uma melhoria porque é o balcão que o faz, é um acesso nominativo...s pessoais...acho que é uma situação que podia ser melhorado, que devia ser algo institucional..." E9</p>	Consulta do BE é feita com os dados pessoais do colaborador e devia ser mais institucionalizado (E9)	1
<p>"...o problema das leis que vão saindo, das inspeções, do regulador e exigências que alteram muito rapidamente e que não dá margem para que se padronize um bocadinho mais os processos... enquanto no RGPD já sabemos o que temos de fazer, e no fundo é desenvolver, no outro é um bocadinho mais complexo..." E9</p>	Dificuldade na padronização dos processos de BC/FT (E9)	1
<p>"...em BC/FT obviamente que se podem melhorar os processos, e estamos a fazer por isso, mas não é um caminho fácil porque saem sempre novas leis, novas exigências e depois dependente do que é o cliente, do que ele nos vai enviando pode surgir maior ou menor complexidade..." E9</p>	Está em curso uma melhoria nos processos de BC/FT, mas é um caminho difícil devido à constante alteração legislativa, à complexidade de cada caso e à colaboração do cliente (E9)	1
<p>..." os vários elementos de identificação naquilo que a lei chama o momento do estabelecimento da relação de negócio... pensando bem até repetitiva..." E11</p>	Há pedidos de elementos de identificação que são repetitivos (E11)	1
<p>"...feito por email...os portugueses estão muito atrasados... a informação vai encriptada e com</p>	Utilização de emails encriptados como forma de	1

Categoria IV: Redução da eficiência associada a dados a recolher, momentos e fluxos

Unidade de Contexto	Unidade de Registo	Frequência
password... com a encriptação a informação julgamos que ela vai de forma minimamente segura...” E11	comunicação com as autoridades (E11)	
“... inicialmente fazia-se por email, onde a informação se dispersa e a informação não fica concentrada...” E11	Informação trocada por email leva à sua dispersão e falta de concentração (E11)	1
“...este software que já existe e que está implementado numa série de países só está dedicado para receber para uma entidade e adaptá-lo para receber para duas entidades é complicado...E11	O software que já existe noutros países será difícil de aplicar porque não está adaptado à comunicação para duas entidades (E11)	1
“... pedidos de informação ad hoc que chegam e existe um problema de clareza na transmissão dos pedidos... por vezes têm de estar sujeitos a interpretações e os supervisores, sobretudo o BdP é uma entidade distante, precisa de ser mais claro nos pedidos que nos faz...” E11	Falta de clareza na transmissão dos pedidos da entidade de supervisão (E11)	1

Anexo VIII Mapa de Árvore

dados	informação	clientes	importância	processos	questão	momentos	diplomas	necessidade				
									tratamento	risco	peças	recolha
	cliente	banco	fazer	recolher	compatibiliza	elementos	forma	processo				
									eficiência	documentos	fatores	aquilo
rgpd	sigilo	bancário	sempre	proteção	digital	termos	fluxos	dia				
									lei	unidade	consentiment	várias

Anexo X – Teste Mann-Whitney

Postos

	V1_Genero	N	Posto médio	Soma de Classificações
V6_Perc_compatib	Masculino	36	42,96	1546,50
	Feminino	41	35,52	1456,50
	Total	77		

Estatísticas de teste^a

	V6_Perc_compatib
U de Mann-Whitney	595,500
Wilcoxon W	1456,500
Z	-1,481
Significância Sig. (2 extremidades)	,139

a. Variável de Agrupamento:
V1_Genero

Anexo XI – Testes Kruskal-Wallis

Postos

	V2_Idade_recod	N	Posto médio
V6_Perc_compatib	[18;30[2	28,25
	[30;40[14	31,32
	[40;50[43	39,60
	[50;60[18	44,72
	Total	77	

Estatísticas de teste^{a,b}

	V6_Perc_compatib
H de Kruskal-Wallis	3,442
df	3
Significância Sig.	,328

a. Teste Kruskal Wallis

b. Variável de Agrupamento:
V2_Idade_recod

Postos

	V3_Anos_Banca_recod	N	Posto médio
V6_Perc_compatib	[0;10[8	32,19
	[10;20[28	37,36
	[20;30[34	40,22
	[30;40[7	47,43
	Total	77	

Estatísticas de teste^{a,b}

V6_Perc_com
patib

H de Kruskal-Wallis	2,060
df	3
Significância Sig.	,560

a. Teste Kruskal Wallis

b. Variável de Agrupamento:
V3_Anos_Banca_recod

Postos

	V4_Habilita	N	Posto médio
V6_Perc_compatib	Ensino Secundário	13	49,62
	Bacharelato	46	37,70
	Licenciatura	9	40,28
	Pós-Graduação	9	29,06
	Total	77	

Estatísticas de teste^{a,b}

V6_Perc_com
patib

H de Kruskal-Wallis	5,070
df	3
Significância Sig.	,167

a. Teste Kruskal Wallis

b. Variável de Agrupamento:
V4_Habilita

Postos

	V5_Funcoes	N	Posto médio
V6_Perc_compatib	Área Comercial	47	40,20
	Direção de Compliance	18	33,83
	Direção de Auditoria	4	26,88
	DMPN	5	55,80
	Direção Jurídica	3	39,33
	Total	77	

Estatísticas de teste^{a,b}

V6_Perc_com
patib

H de Kruskal-Wallis	5,277
df	4
Significância Sig.	,260

a. Teste Kruskal Wallis

b. Variável de Agrupamento:
V5_Funcoes

Anexo XII

Matriz de correlações entre itens

	V_8.1	V_8.2	V_8.3	V_8.4	V_8.5	V_8.6	V_8.7	V_8.8	V_8.9
V_8.1	1,000	,162	,353	,121	,144	-,026	,124	,325	,333
V_8.2	,162	1,000	,252	-,013	,481	,762	,357	,145	,371
V_8.3	,353	,252	1,000	,567	,303	,036	,025	,313	-,008
V_8.4	,121	-,013	,567	1,000	,375	,017	,036	,281	,057
V_8.5	,144	,481	,303	,375	1,000	,572	,155	,223	,288
V_8.6	-,026	,762	,036	,017	,572	1,000	,534	,324	,485
V_8.7	,124	,357	,025	,036	,155	,534	1,000	,647	,445
V_8.8	,325	,145	,313	,281	,223	,324	,647	1,000	,329
V_8.9	,333	,371	-,008	,057	,288	,485	,445	,329	1,000

Scale Reliability Statistics

	mean	sd	Cronbach's α
scale	4.23	0.702	0.768

[3]

Estadísticas de item-total

	Média de escala se o item for excluído	Variância de escala se o item for excluído	Correlação de item total corrigida	Correlação múltipla ao quadrado	Alfa de Cronbach se o item for excluído
V_8.1	33,35	34,099	,303	,398	,768
V_8.2	34,16	30,633	,546	,717	,730
V_8.3	33,94	34,325	,364	,557	,758
V_8.4	33,82	34,809	,268	,472	,772
V_8.5	34,04	30,827	,545	,520	,730
V_8.6	34,22	30,516	,590	,799	,723
V_8.7	33,55	33,172	,473	,605	,743
V_8.8	33,75	34,004	,529	,600	,741
V_8.9	33,81	30,080	,481	,417	,742

Item Reliability Statistics

	mean	sd	if item dropped Cronbach's α
V_8.1	4.73	1.232	0.768
V_8.2	3.92	1.275	0.730
V_8.3	4.14	1.060	0.758
V_8.4	4.26	1.185	0.772
V_8.5	4.04	1.251	0.730
V_8.6	3.86	1.222	0.723
V_8.7	4.53	1.046	0.743
V_8.8	4.32	0.850	0.741
V_8.9	4.27	1.466	0.742

Anexo XIII

Estadísticas de teste^a

	V_8.1	V_8.2	V_8.3	V_8.4	V_8.5	V_8.6	V_8.7	V_8.8	V_8.9
U de Mann-Whitney	668,500	658,000	702,000	723,500	729,500	640,000	608,000	648,500	553,500
Wilcoxon W	1614,500	1253,000	1648,000	1669,500	1324,500	1235,000	1203,000	1243,500	1148,500
Z	-,669	-,777	-,311	-,080	-,016	-,972	-,1325	-,904	-,1868
Significância Sig. (2 extremidades)	,504	,437	,756	,937	,987	,331	,185	,366	,062

a. Variável de Agrupamento: V7_Compatibilizacao

Anexo XIV

Estadísticas de teste^a

	V_9.1	V_9.2	V_9.3	V_9.4	V_9.5	V_9.6	V_9.7	V_9.8	V_9.9	V_9.10
U de Mann-Whitney	150,500	173,000	169,500	116,000	148,500	124,500	93,000	108,500	86,500	105,000
Wilcoxon W	2778,500	188,000	2797,500	131,000	163,500	2752,500	108,000	123,500	101,500	120,000
Z	-,631	-,156	-,229	-,1351	-,681	-,1177	-,1845	-,1515	-,1986	-,1606
Significância Sig. (2 extremidades)	,528	,876	,819	,177	,496	,239	,065	,130	,047	,108
Sig exata [2*(Sig. de 1 extremidade)]	,553 ^b	,896 ^b	,833 ^b	,196 ^b	,526 ^b	,260 ^b	,073 ^b	,143 ^b	,051 ^b	,126 ^b

a. Variável de Agrupamento: V_9_Eficiencia

b. Não corrigido para vínculos.