Escola de Ciências Sociais e Humanas

Departamento de Economia Politica

Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo: Ferramentas Tecnológicas Utilizadas

Joana Inês Fernandes dos Santos

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Economia Monetária e Financeira

Dissertação orientada pelo Prof. Doutor Sandro Mendonça

Prof. Auxiliar, ISCTE Business School, Departamento de Economia

Outubro 2018

Agradecimentos

Chega ao fim mais uma etapa da minha vida, que foi o colmatar de dias e noites dedicadas a investigar, com o apoio das “minhas” pessoas, que tornaram este percurso possível e bom.

Como tal, não poderia deixar de lhes agradecer pois, cada um à sua maneira, ajudou a tornar esta tese possível.

Agradeço ao meu orientador, Prof. Sandro Mendonça pelas palavras de força, de motivação e pelo contributo através da partilha de ideias e sugestões. Foi uma peça fundamental neste percurso.

Aos meus pais, família e padrinhos, por todos os esforços e sacrifícios feitos, por todo o amor que sempre tiveram para comigo e por acreditarem sempre em mim.

Agradeço também aos meus amigos do coração, que nunca me deixaram desistir e que me mostram que era capaz: Rita Ferreira, Marta Machado, Sara Roseira, João Correia, João Jaime, Diogo Neves e João Fernandes.

Ao meu Pê, por ser um pilar importante da minha vida e pelo seu apoio incondicional.

E por fim, aos meus colegas de curso que também sempre me apoiaram e me deram força para continuar.

Resumo

O Branqueamento de Capitais e o Terrorismo são temáticas que estão cada vez mais presentes no nosso dia-a-dia, principalmente o terrorismo. Como tal torna-se importante perceber que temáticas são estas, como são combatidas e que entidades estão por detrás disto.

A presente tese tem enfoque nas ferramentas tecnológicas utilizadas no combate do Branqueamento de Capitais e ao Financiamento do Terrorismo, mais concretamente nos sistemas que utilizam agentes inteligentes, existentes no mercado e no papel que o Banco de Portugal tem nesta temática, como supervisor.

Para auxílio da investigação recorreu-se à metodologia qualitativa utilizando como método de recolha de dados: a análise documental e a realização de uma entrevista a um especialista na área de Segurança de Redes e Computadores e Sistemas Distribuídos.

Na presente dissertação aborda-se um protótipo de um Sistema Inteligente Anti-Branqueamento de Capitais feito pela Universidade de Hong Kong e propõem-se um Sistema Inteligente melhorado, que tem por base este protótipo. Nesta proposta de Sistema Inteligente Anti-Branqueamento de Capitais, é explicada a sua estrutura e componentes, o seu funcionamento, formas de o proteger e quais as vantagens e desvantagens deste sistema face aos sistemas inteligentes existentes no mercado.

Palavras-Chave: Sistemas Inteligentes, Ferramentas Tecnológicas, Branqueamento de Capitais, Financiamento do Terrorismo, Banco de Portugal.

Classificação JEL: O30 (*Innovation; Research and Development; Technological Change; Intellectual Property Rights: General*); G21 (*Financial Economics and Services: Banks; Depository Institutions; Micro Finance Institutions; Mortgages*).

Abstract

Money laundering and terrorism are issues that are more and more present in our lives. Specially terrorism. As such, it becomes important to understand what exactly are these issues, how they can be fought and who or what is behind them.

This thesis is focused on the technological tools used by financial institutions, in particular the systems that use intelligent agents, and what exactly is available in the market and the supervising role of Banco the Portugal.

This investigation was carried out using the qualitative method and document analysis was used to collect data. An interview to a specialist in Network Security and Distributed Systems was also used.

In this dissertation an Intelligent Anti-Money Laundering System developed by the University of Hong Kong is discussed and an improved system, based on the referred prototype is proposed and its structure, architecture and components are explained, as well as the way it functions, the best ways to protect it and the advantages and disadvantages of such system versus the systems that are available today.

Key-words: Intelligent Systems, Technological Tools, Money Laundering, Terrorism Financing, Bank of Portugal

JEL Classification: O30 (Innovation; Research and Development; Technological Change; Intellectual Property Rights: General); G21 (Financial Economics and Services: Banks; Depository Institutions; Micro Finance Institutions; Mortgages).

Índice

Índice de figuras

Índice de tabelas

Lista de abreviaturas e siglas

AI - Agentes Inteligentes
ABC – Anti-Branqueamento de Capitais
ABR - Abordagem Baseada em Risco
APNFDs - Atividades e Profissões Não-Financeiras Designadas
ASAE - Autoridade de Segurança Alimentar e Económica
ASF - Autoridade de Supervisão de Seguros e Fundos de Pensões
ASR - Avaliação Supranacional dos Riscos
BC - Branqueamento de Capitais
BdP - Banco de Portugal
BIIA - Base de Informação de Inspeções e Averiguações
CFT - Combate ao Financiamento do Terrorismo
CMVM - Comissão do Mercado de Valores Mobiliários
DCIAP - Departamento Central de Investigação e Ação Penal
DAS – Departamento de Ação Sancionatória
DMZ - *Demilitarized Zone*
EI – Estado Islâmico
FMI - Fundo Monetário Internacional
FT - Financiamento do Terrorismo
GAFI - Grupo de Ação Financeira Internacional
IAS - Índice de Atenção Supervisiva
IF - Instituição Financeira
IGCP - Instituto de Gestão da Tesouraria e do Crédito Publico
InCI - Instituto da Construção e do Imobiliário
IRN - Instituto dos Registos e Notariado
KYC - *Know your Customer*
KYT - *Know your Transactions*
MP - Ministério Público
ONU - Organização das Nações Unidas
OTAN/NATO - Organização do Tratado do Atlântico Norte/ *North Atlantic Treaty Organization*
ORTGs - Organismos Regionais do Tipo GAFI
PEP - Pessoas Expostas Politicamente
RAS - Relatório de Atividades Suspeitas
RTS - Relatório de Transações Suspeitas
SBR - Supervisão Baseada no Risco
SMAS - Sistema Multi-Agentes
SRIJ - Serviço de Regulação e Inspeção de Jogos
UIF - Unidade de Informação Financeira
UTM - *Unified Threat Manager*

1. Introdução

As Tecnologias de Informação permitem que as instituições, a nível mundial, funcionem e sem elas os mercados não seriam capazes de reagir a desenvolvimentos globais, as instituições financeiras não conseguiriam adquirir informação em tempo útil, não seria possível manter os dados dos clientes atualizados, não seria possível fazer transações na bolsa de valores, registar os ganhos de um negócio, calcular rapidamente estatísticas financeiras ou simplesmente transferir dinheiro.

De acordo com o Professor Jane K. Winn (2000: 144), da University of Washington School of Law "Os mercados financeiros podem ser considerados os primeiros mercados globais organizados, a operar com base em computadores ligados em rede".

As perguntas de partida para esta investigação são as seguintes: Que ferramentas tecnológicas são utilizadas para combater o Branqueamento de Capitais e o Financiamento do Terrorismo? Qual a função do Banco de Portugal enquanto regulador e supervisor? Como se podem proteger estas ferramentas? Que soluções de ferramentas tecnologias é que o mercado oferece?

Para auxiliar esta investigação recorreu-se à metodologia qualitativa, utilizando como método de recolha de dados a análise documental e a realização de uma entrevista ao Prof. Dr. Miguel Pardal, professor assistente do Instituto Superior Técnico na área de Segurança de Redes e Computadores e Sistemas Distribuídos.

Assim, a Dissertação encontra-se estruturada em cinco capítulos. O presente Capítulo 1, onde é feita a introdução. O Capítulo 2, onde é feito o enquadramento teórico dos temas do Branqueamento de Capitais e do Financiamento do Terrorismo, explicada a função do Banco de Portugal e apresentado um protótipo de Sistema Inteligente Anti-Branqueamento de Capitais. O Capítulo 3, onde é abordada a metodologia de investigação qualitativa, em particular a entrevista efetuada. Caracteriza-se o entrevistado e é apresentado o guião da entrevista e os moldes da realização da entrevista. O Capítulo 4, onde é efetuada a análise e discussão de resultados, no qual se fica a conhecer a metodologia utilizada para a proteção de aplicações financeiras e o funcionamento de sistemas inteligentes. Neste mesmo capítulo, propõem-se um Sistema Inteligente Anti-Branqueamento de Capitais baseado num protótipo feito pela Universidade de Hong Kong e nos dados obtidos na entrevista. Explica-se a estrutura e componentes do sistema, o seu funcionamento e o mecanismo de proteção, e por fim indica-se as desvantagens e vantagens deste sistema face aos Sistemas Inteligentes existentes no mercado. Por último, no capítulo 5, apresentam-se as conclusões da investigação, bem como as limitações encontradas no estudo, sugerem-se temas para investigação futura e expõem-se as *policy implications*, ou seja, os contributos da minha dissertação para melhorar o mundo.

2. Enquadramento Teórico

2.1. Introdução

Este capítulo visa contextualizar a temática do Branqueamento de Capitais (BC) e do Financiamento do Terrorismo (FT): os conceitos, a sua relação, as entidades envolvidas na prevenção e os organismos de cooperação internacional e regional. Neste capítulo, foca-se também na função do Banco de Portugal enquanto supervisor e as ferramentas tecnológicas utilizadas pelo mesmo.

Para finalizar, neste capítulo, aborda-se um protótipo de Sistema Inteligente Anti-Branqueamento de Capitais feito pela Universidade de Hong Kong e as ferramentas tecnológicas de Sistemas Inteligentes existentes no mercado para fazer face a estes atos ilícitos.

2.2. Branqueamento de Capitais

O Branqueamento de Capitais (BC) consiste no processo ou atividade de ocultação da origem criminosa de capitais, bens ou produtos através de práticas ilícitas de forma a dar lhes uma aparência final legal. “É o processo pelo qual os proveitos de atividade criminosa são disfarçados de forma a encobrir a sua origem ilícita.” (Schott, 2005: I-1)

> “O branqueamento de capitais é um processo dinâmico, desenvolvido através das fases de colocação, circulação e integração, e visa transformar dinheiro, bens ou valores obtidos através da prática de determinados crimes, em património aparentemente lícito, que possa ser usado perante todos como se legítimo se tratasse”. (Braguês, 2009:16)

Segundo o Grupo de Ação Financeira Internacional (GAFI), o BC consiste na utilização e transformação de produtos do crime para dissimular a sua origem ilícita com o objetivo de justificar os rendimentos resultantes da atividade criminosa.

A Convenção de Viena limita as infrações ao tráfico de droga, contudo a comunidade internacional concluiu que as infrações subjacentes deveriam ser mais amplas. Deste modo, o GAFI e outros organismos internacionais ampliaram o acordado na Convenção de Viena, e passaram a incluir outros crimes graves.

No nº 2 a), do artigo 6.º, da Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional é explícito a aplicação de infrações pelos Estados Partes ao maior número possível de infrações subjacentes. Esta convenção foi assinada a 20 de dezembro de 1988, em Viena e ratificada por Portugal em 1991 contento um estudo aprofundado do BC e a obrigar a sua criminalização em caso de tráfico de drogas.

Os Estados Unidos da América foram pioneiros na criminalização do BC, através do *Money Laundering Control Act* de 1986. Contudo a Inglaterra e a Suíça introduziram as primeiras normas penais do BC, posteriormente à entrada em vigor das disposições dos EUA.

Em Portugal começou a ser criminalizado através do Decreto-Lei nº 15/93, de 22 janeiro associado ao tráfico de droga.

2.2.1.Processo de Branqueamento de Capitais

O GAFI adota como "processo-tipo" do BC, o "Modelo das 3 Fases", que consiste num processo composto por três fases distintas e sucessivas: 1) Colocação; 2) Circulação; 3) Integração. Cada uma destas fases será descrita nos subcapítulos seguintes.

Este modelo, que é o aceite e o mais divulgado pelos autores, é baseado no convencionado pela Organização das Nações Unidas (ONU) que define que o modelo de BC é "primeiramente, a dissociação dos proveitos económicos da infração da prática cometida, em segundo lugar, o apagar do respetivo rasto para iludir as investigações, e, finalmente, a sua recuperação pelo criminoso, já após ter sido dissimulada a sua origem económica e geográfica".

2.2.1.1. Colocação

Numa primeira fase procede-se à introdução dos capitais, bens ou produtos que se pretende branquear no sistema económico-financeiro através da utilização de diversos meios ou instrumentos oferecidos pelo sistema.

O numerário é o produto de crime mais frequentemente branqueado, pois o tráfico de droga, falsificação de documentos, lenocínio e tráfico de pessoas gera imediatamente dinheiro. Por exemplo, um cliente que compra estupefacientes não vai pagar o produto via cartão de crédito ou cheque.

Nesta fase os métodos utilizados servem para evitar o "rasto documental" pelas autoridades, ou seja, evitar que haja o cruzamento de dados que identifiquem a sua origem e o seu respetivo titular passado e presente.

São utilizadas frequentemente as seguintes técnicas:

- Bancos – é através de instituições bancárias que se pretende camuflar a introdução de elevados montantes de dinheiro. Este sector apresenta uma elevada vigilância através da existência de legislação apertada;
- Casa de câmbios – são utilizadas para alterar o caracter do dinheiro, pois procede-se primeiramente a um depósito de dinheiro nestas casas de câmbio no qual se entrega um

documento respeitante ao respetivo câmbio, diminuindo assim a incerteza a quando da colocação do dinheiro em bancos;

- Setor imobiliário – é um sector com grandes potencialidades de branqueamento, pois é possível fazer um pagamento parcial nas aquisições de imobiliário em numerário;
- Sociedades em empresas em falência – baseia-se na utilização de empresas em dificuldades para injeção de dinheiro nas contas dessas empresas e consequentemente no sistema financeiro;
- Salas de Jogo/Casinos – é um sector vulnerável nesta fase, principalmente em casinos não supervisionados pelo Serviço de Regulação e Inspeção de Jogos (SRIJ), todavia, os casinos tradicionais já não se apresentam tão vulneráveis devido às inspeções regulares de que são alvos.

Esta é a fase mais crítica pois é onde os fluxos são mais facilmente detetados e mais próximos se encontram da sua origem, existindo uma grande facilidade de ligação entre o crime precedente e o criminoso.

2.2.1.2. Circulação

Numa segunda fase é necessário que haja grande rotatividade de titularidade dos capitais, bens ou produtos, de forma a permitir um maior afastamento entre a sua origem e a forma de obtenção e aquele que ficará na posse do mesmo.

Nesta fase ocorrem múltiplas operações, se possível em mais de um país, pois em caso de investigação ou perseguição pelas entidades competentes, as ocultações realizadas impedem a prossecução das intenções da justiça.

Em zonas de regimes especiais com determinados ordenamentos jurídicos, como as Offshore ou territórios que protegem o património, como a Suíça e Liechtenstein, as instituições financeiras possuem ferramentas específicas como o *walking account* que permite que se proceda à execução de instruções dadas pelos seus clientes para a movimentação de contas para outro domínio em resposta ao mínimo sinal de investigação criminal.

Na fase da circulação é habitual recorrer-se a determinadas profissões como mediadores de seguros, bancários, advogados, solicitadores que tenham obrigações com a panóplia de leis do branqueamento, de forma a permitir "oficiosamente" ocultar o verdadeiro titular dos fundos investidos, aplicados e depositados, uma vez que, quanto mais extensa for esta fase, quanto mais etapas e ordenamentos jurídicos tiver, melhor para o branqueador.

Atualmente, para se dissimular a origem dos ativos são utilizados os seguintes processos: *Offshore Banking*, empresas fictícias e de fachada, negócios fictícios, contabilidade paralela em empresas com atividade regular e mistura de ativos "sujos" com ativos "limpos" dentro de estruturas empresariais regulares.

De todas as fases constituintes do processo de branqueamento, esta é a fase que exige um maior grau de especialização e criatividade.

2.2.1.3. Integração

Na terceira e última fase é necessário a integração de capitais, bens ou produtos na esfera patrimonial de quem pertencem. É quando os capitais, bens ou produtos adquiridos ilicitamente, provenientes de vários crimes são usados livremente pelos criminosos sem levantamento de dúvidas sobre a sua proveniência.

Em muitos casos o Estado financia investimentos feitos com ativos “sujos”, de carater duvidoso através de subsídios, apoios e comparticipações. (Braguês, 2009:14)

Em Portugal tem-se verificado casos de integração em cadeias hoteleiras e de restauração, residências e explorações agrícolas, no sector imobiliário e nas partes sociais de sociedades e empresas.

Em suma quantas mais fases o branqueador conseguir alcançar no processo de branqueamento mais difícil será detetar os atos ilícitos pelas autoridades que combatem esta prática, recuperar os valores envolvidos e responsabilizar os seus autores, ou seja, o êxito no processo depende em grande parte no sucesso em ocultar as origens ou fontes dos fundos e branquear os produtos.

No processo de branqueamento a complexidade é tão grande que as operações bancárias podem-se sobrepor, separar ou produzir em simultâneo, dificultando às autoridades a sua deteção, sobretudo se ocorrer a passagem além-fronteiras e a facilidade de comunicação.

Em cada uma das fases do processo é possível detetar práticas ilícitas de branqueamento, havendo uma maior facilidade em determinadas fases.

Por lei os intervenientes do sector económico-financeiro são obrigados a comunicar operações suspeitas ou comportamentos atípicos ao normal funcionamento do mercado às entidades de prevenção do BC. O não cumprimento destas obrigações pode levar a aplicação de elevadas coimas e ao impedimento de continuação da respetiva atividade. Fora de Portugal existem instituições financeiras que foram impedidas de continuar a sua atividade devido a sua participação e utilização de atos de BC. Esta temática é abordada na Lei nº 25/2008, de 5 de Junho, no qual se estabelece as medidas de natureza preventiva e repressiva para o combate do BC/FT.

Segundo o Fundo Monetário Internacional (FMI) no *World Economic Outlook 2010*, “o valor total da economia mundial é de 61,9 triliões de dólares, dos quais 3,1 triliões são produto de branqueamento de capitais.”

Ver anatomia de um ataque de BC no Anexo A.

2.2.2.Consequências do Branqueamento de Capitais

As ações de BC acarretam consequências negativas para as instituições financeiras, como a reputação negativa da "marca" das instituições, perda generalizada dos lucros, perda de negócios lucrativos, problemas de liquidez causados pela retirada repentina de fundos, cancelamento de acordos bancários, custos de investigações e multas, apreensão de ativos, prejuízos em empréstimos e diminuição do valor das suas ações.

2.3. Financiamento do Terrorismo

A ONU tem tido um papel ativo no combate ao terrorismo através de tratados e convenções internacionais, destacando se a Convenção Internacional para a Eliminação do Financiamento do Terrorismo de 1999.

Esta convenção estipula que:

> "Comete uma infracção, nos termos da presente Convenção, quem, por quaisquer meios, directa ou indirectamente, ilegal e deliberadamente, fornecer ou reunir fundos com a intenção de serem utilizados ou sabendo que serão utilizados, total ou parcialmente, tendo em vista a prática: a) De um acto que constitua uma infracção compreendida no âmbito de um dos tratados enumerados no anexo e tal como aí definida; ou b) De qualquer outro acto destinado a causar a morte ou ferimentos corporais graves num civil ou em qualquer pessoa que não participe directamente nas hostilidades numa situação de conflito armado, sempre que o objectivo desse acto, devido à sua natureza ou contexto, vise intimidar uma população ou obrigar um governo ou uma organização internacional a praticar ou a abster-se de praticar qualquer acto. 3 - Para que um acto constitua uma das infracções previstas no n.º 1, não é necessário que os fundos tenham sido efectivamente utilizados para cometer a infracção contemplada nas alíneas"

O conceito de terrorismo não é exato. O seu significado tem implicações políticas, religiosas e nacionais diferindo de pais para pais. Deste modo, o GAFI não se pronuncia quando ao seu conceito, mencionando que de acordo com Convenção Internacional para a Eliminação do Financiamento do Terrorismo, os países devem criminalizar o financiamento de atos terroristas, organizações terroristas e terroristas individuais mesmo que não exista ligação a atos terroristas. Esta definição é a adotada pela maioria dos países.

Uma das grandes dificuldades do FT é envolver montantes de dinheiro relativamente baixos ou possuírem origem licita, o que torna a sua deteção mais difícil, pelo que deve exigir uma maior preocupação nas políticas de combate ao terrorismo implementadas pelos Estados.

Segundo a revista visão, atualmente fala-se da existência de um "Novo Terrorismo" que é o terrorismo que se tem verificado nos dias de hoje. Este "Novo Terrorismo" consiste na utilização de novas medidas

estratégicas, tais como ataques terroristas de baixo custo financeiro e com grande impacto de medo e terror, através de financiamento angariado localmente. Esta tendência não é exclusiva de grupos mais pequenos, pois os grupos transacionais como a Al-Qaeda e o Estado Islâmico (EI) realizaram ataques nas condições acima mencionadas, financiando-se através das fontes licitas como caridade, organizações sem fins lucrativos e empresas de fachada.

O combate ao FT assumiu maior peso desde o atentado terrorista de 11 de setembro de 2001, nos EUA, pelo que a comunidade internacional teve a necessidade de adotar medidas legislativas em articulação com o quadro normativo do BC, de forma a facilitar o seu combate e a sua prevenção através das dificultações de acesso ao sistema financeiro internacional pelos autores do terrorismo, organizações e grupos terroristas e pelos seus financiadores. Estas medidas legislativas incluem o congelamento e perda de bens pertencentes aos autores de atos terroristas, aos seus financiadores e apoiantes, obrigatoriedade de comunicação de transações suspeitas de ligação ao terrorismo e a criminalização do FT.

O FT é considerado um crime autónomo no ordenamento jurídico português de acordo com o artigo 5.º, da Lei nº 52/2003, de 22 de agosto, e posterior aditamento pela Lei nº 25/2008, de 5 de junho, sendo o mesmo punível com pena de prisão de 8 a 15 anos.

> "A recorrente utilização da Internet para a prossecução de atividades de apoio ao terrorismo tem proporcionado vantagens aos grupos extremistas e terroristas, permitindo-lhes contornar medidas de segurança e expandir a sua mensagem nas sociedades ocidentais a um alargado número de destinatários. Acresce que a divulgação maciça na Internet de propaganda do terrorismo tem elevado o risco de aparecimento dos fenómenos de autoradicalização e de atores solitários." (*Site* institucional do Serviço de Informações de Segurança[1])

2.3.1. Principais Grupos Organizados de Terrorismo

Segundo o Serviço de Informações de Segurança, a principal ameaça terrorista na Europa provém do terrorismo Internacional com origem no Al-Qaeda core (AQ) e seus filiados. O mais recente é o EI e a atuação dos grupos locais (*homegrown*) e isolados.

> "Pese embora a AQ core (e grupos afiliados) e o Estado Islâmico não atuarem primeiramente na Europa, é constante a ameaça de aqui perpetrarem atentados. Com efeito, esta ameaça está atualmente reforçada pelo recrudescimento da ameaça terrorista islamista nos países do Médio Oriente, em particular na Síria, e no Norte de África, bem como pela crescente presença

[1] *Site* institucional do Serviço de Informações de Segurança - https://www.sis.pt/ameacas/contra-terrorismo

em palcos de conflito jihadista de combatentes estrangeiros oriundos da Europa." (*Site* institucional do Serviço de Informações de Segurança[2])

2.3.1.1. Estado Islâmico do Iraque e do Levante

Este grupo terrorista é uma organização jihadista liderada por Abu Bakr Al Baghdadi, nasceu na segunda metade dos anos 2000 com uma divergência no grupo terrorista Al-Qaeda no Iraque. O objetivo inicial deste grupo era expulsar os soldados americanos do Iraque, matar xiitas apostatas[3] e traidores e criar um governo controlado por radicais sunitas[4].

O seu campo de atuação é maioritariamente regiões sunitas no Iraque e na Síria, apropriou-se de muitas cidades, campos de petróleo, armas e estruturas do exército.

Este grupo obteve uma receita de 2 mil milhões de dólares Norte Americanos no ano de 2015, no qual grande parte é proveniente do contrabando de petróleo, gerando em média 1,3 milhões de dólares por dia, no qual resultou aproximadamente 500 milhões de dólares de lucro. Outro fluxo de receita resulta da tributação dos indivíduos e das empresas afetas aos territórios controlados por eles, como os impostos de renda e de negócios, impostos sobre medicamentos e levantamento de dinheiro. Estima-se que se obteve cerca de 350 milhões de dólares. Outra fonte de financiamento é a venda de peças arqueológicas no mercado negro, estimando-se um lucro de 100 milhões de dólares por ano. Por fim uma parte minoritária do financiamento deve-se ao valor do resgate proveniente de sequestros no qual somou um total de 45 milhões de dólares no ano de 2014.

2.3.1.2. Al-Qaeda

Este grupo terrorista nasceu no ano de 1988 após a expulsão dos soldados da União Soviética do Afeganistão pelo exército civil do Afeganistão e estendeu-se à África do Norte, à África subsariana e sobretudo a Africa Ocidental, sendo que na Africa Ocidental "entre outras actividades ilícitas, foram detectados os tráficos de drogas, pessoas, armas, minerais, petróleo e a contrafacção e tráfico de medicamentos." (Costa, 2014: 68).

O objetivo principal deste grupo é destruir a presença ocidental nos países islâmicos, não havendo tolerância pelos muçulmanos.

[2] *Site* institucional do Serviço de Informações de Segurança - https://www.sis.pt/ameacas/contra-terrorismo

[3] Corrente islâmica

[4] Corrente islâmica

Ao longo dos tempos foi ganhando cada vez mais peso, e o exemplo disso foi o atendado do 11 de setembro de 2001. A quando do atentado, este grupo terrorista é liderado por Osama bin Laden, o homem mais procurado do mundo naquela altura.

O atentado contra os cartoonistas do *Charlie Hebdo* em janeiro de 2015 foi revindicado pela rede Al-Qaeda na Península Arábica.

Este grupo terrorista passou de um grupo financiado pela riqueza pessoal de Osama bin Laden e de doações por indivíduos do Estado do Golfo para uma organização global com uma carteira diversificada de negócios ilícitos. Contudo, as afiliadas deste grupo, como a Al-Qaeda in the Arabian Peninsula apresentam comportamentos criminosos mais banais, como roubar o Banco Central de Al Mukalla e extorquir companhias de petróleo e telecomunicações.

As receitas em 2015 ascenderam a 140 milhões de dólares e 50 milhões de dólares em 2016, resultando uma diminuição de 90 milhões de dólares em 2016.

Segundo Costa (2014: 68), na Africa Ocidental "O aumento do financiamento do terrorismo e de actos terroristas, as ligações entre grupos terroristas emergentes com diferentes origens e orientações, o uso de meios legítimos e ilegítimos para a angariação de fundos para o desenvolvimento de conflitos, a migração incontrolada de pessoas, aliam-se às vulnerabilidades que estes Estados apresentam".

2.3.1.3. Talibã

Este movimento radical político-religioso dominou o Afeganistão entre 1996 e 2001, ano da invasão dos EUA. Este movimento tem como objetivo impor a Sharia[5] no território Paquistanês. A educação é uma ameaça para eles, em especial para o sexo feminino pois vai contra os seus ideais de serviço para as mulheres. O ataque sofrido por Malala Yoursafzai foi um exemplo da manifestação deste movimento contra o direito de estudar.

Este grupo foi responsável por ataques em larga escala em Nova Iorque, Londres e Madrid, tendo sido o principal alvo pela Organização do Tratado do Atlântico Norte (OTAN ou NATO - *North Atlantic Treaty Organization)* após os ataques de 11 de setembro de 2001.

A maior parcela de receitas é proveniente da venda e tráfico de ópio, gerando pelo menos 200 milhões de dólares por ano, sendo o seu papel proteger o mercado, acompanhar os traficantes e auxiliar o transporte de ópio. O Afeganistão é o maior produtor deste estupefaciente no mundo.

O Conselho de Segurança da ONU informou que este grupo em 2012 arrecadou 400 milhões de dólares através de uma combinação de impostos, doações, extorsões e envolvimento no tráfico de narcóticos.

[5] Lei Islâmica

Entre 2012 e 2015 o ópio e o cultivo aumentaram 19 %, pelo que é expectável que este grupo tenha aumentado as suas receitas no comércio de ópio em 200 milhões de dólares.

A Arábia Saudita, Kuwait e os Emirados Árabes Unidos têm vindo a financiar este grupo através de instituições de caridade islâmicas e de outras índoles.

No Anexo B encontram-se 3 figuras que mostram os ataques terroristas ocorridos no Mundo entre 2000 e 2015, o número de ataques terroristas na Europa Ocidental entre 1970 e 2015 e o número de mortos e feridos nos ataques terroristas desse período.

2.4. Relação entre o Branqueamento de Capitais e o Financiamento do Terrorismo

O BC e o FT apresentam características operacionais semelhantes. A diferença é que os branqueadores de capitais enviam fundos ilícitos através de canais legais com o fim de ocultar a origem criminosa enquanto os financiadores do terrorismo transferem fundos ilícitos ou lícitos com o objetivo de ocultar as suas origens e o seu uso final (apoio ao terrorismo). Em ambas as ações o resultado é a recompensa.

Deste modo, a grande diferença entre ambos os conceitos prende-se na origem lícita ou ilícita dos fundos envolvidos. As fontes lícitas podem ser doações ou contribuições monetárias ou de bens a organizações como fundações ou instituições de caridade que as utilizam para apoiar organizações terroristas e consequentemente contribuem para o financiamento do mesmo. Quando os fundos utilizados no FT apresentam origem ilícita, estes podem estar incluídos num sistema de BC, dependendo do carater das infrações subjacentes ao BC.

A diferença entre estes conceitos exige a existência de legislação diferente consoante se trate de BC ou FT. Para efeitos sancionatórios no FT é irrelevante saber qual a origem dos fundos contrariamente do que se verifica no BC.

2.5. Métodos e tipologias do Branqueamento de Capitais/Financiamento do Terrorismo

No que se refere ao BC/FT, quando se fala em metodologia fala-se em tipologias, não havendo diferença entre estes dois conceitos. “As várias técnicas utilizadas para branquear capitais são geralmente denominadas *métodos* ou *tipologias*. Os termos “método” e “tipologia” podem ser utilizados indistintamente, sem qualquer diferença entre eles”. (Schott, 2005: I-10)

Os métodos podem variar de país para país estando sempre em contante mutação, consoante a sua economia, a política, os seus mercados financeiros, as autoridades policiais, o seu regime Anti-Branqueamento de Capitais (ABC) e do nível de cooperação internacional.

Como vimos anteriormente, o capital é o alvo mais branqueado, pelo que se separa as atividades financeiras das restantes atividades de forma a simplificar o seu estudo e compreensão.

Deste modo, é no sistema financeiro onde existem mais tipologias de branqueamento, pelo que o Banco de Portugal (BdP) identificou um conjunto de operações potencialmente suspeitas no qual emitiu vários avisos com caracter legislativo para as instituições de crédito e sociedades financeiras.

Existem indicadores que podem indiciar algumas tipologias utilizadas na ação de branquear e financiar o terrorismo, condicionando assim a recolha de informação. Deste modo destacam-se os seguintes indicadores: transações em numerário, em especial as efetuadas em instituições de pagamento, em moeda nacional e estrangeira, depósitos, transferências, transações comerciais, operações com recurso a crédito, operações relacionadas com a atividade *Offshore*, sector segurador, outras atividades económicas, utilização da banca eletrónica e em âmbito de fiscalidade e tributação.

O GAFI nos seus relatórios anuais e no seu relatório anual de tipologias, indica documentos relativos aos métodos utlizados pelos branqueadores nos últimos tempos, tal como acontece com os organismos regionais do GAFI que também publicam informações sobre as tipologias e métodos usados na região.

Deste modo, as organizações internacionais detetaram os seguintes métodos e técnicas de BC/FT: territórios *Offshore*, transporte físico de dinheiro, tráfico de tabaco ilícito, sectores dos valores mobiliários, sector dos jogos e casas de jogo, sector imobiliário, profissões jurídicas, corrupção, prestadores de serviços a *trusts* e sociedades, ouro, moeda virtual, *hawala*[6] e outros sistemas alternativos, futebol, tráfico de diamantes, contrafação de dinheiro, bens de elevado valor, EI, organizações sem fins lucrativos, proliferação e transferências de fundos e operações de câmbios.

2.6. Sectores de atividade mais expostos

Em países com sistemas financeiros frágeis, as ações de BC/FT têm consequências económicas e sociais bastante significativas, provocando fragilidades no mercado, colocando em risco a economia, a segurança e em último caso a sociedade. Estas ações levam por vezes a fenómenos de corrupção, levando a uma maior desconfiança no mercado e nas instituições, afetam os poderes estaduais e desprestigiam o mercado.

Como vimos anteriormente o grande aleado dos branqueadores é a exploração do sector económico-financeiro, fazendo com que o sector económico seja um sector de atividade mais sensível ao risco da sua utilização por parte dos branqueadores. Deste modo, criou-se um conjunto de normas legais para estes sectores de atividade, com vista a evitar a sua potencial utilização por estes.

[6] Corresponde ao termo dado para banca paralela ou sistema bancário não oficioso

2.7. Pessoas expostas politicamente

Este conceito refere-se a pessoas que se encontram mais expostas a uma possível prática de atos de BC/FT, trata-se de uma classificação atribuída a determinadas pessoas.

Segundo a definição do Parlamento Europeu, as Pessoas Expostas Politicamente (PEP) "podem representar um risco mais elevado de corrupção pelo facto de exercerem ou terem exercido funções públicas importantes". De acordo com os termos da alínea cc) do n.º 1, do artigo 2.º, da Lei n.º 83/2017, de 18 de agosto, como PEP destacam-se os chefes de Estado e do governo, ministros, membros da direção de partidos políticos, deputados, juízes de tribunais supremos, bem como cônjuge, pais, filhos e os cônjuges destes últimos.

A Diretiva nº 2015/849 de 20 de maio de 2015 do Parlamento Europeu e do Conselho veio atualizar a Diretiva Europeia original de 2005, permitindo o alargamento de quem tem acesso a informações relacionadas com as PEP. Esta diretiva veio estabelecer novas regras, nomeadamente os países da União Europeia são obrigados a manter um registo central com informações sobre os beneficiários efetivos de sociedades, fundações e outras estruturas, de forma a permitir identificar os indivíduos que estão por detrás dessas entidades. O sector bancário é também obrigado a intensificar a vigilância e a comunicar transações suspeitas dos clientes. Estas informações deverão estar armazenadas numa base dados central fora das sociedades.

2.8. Entidades envolvidas na prevenção

A prevenção do BC/FT está prevista na Lei nº 25/2008, de 5 de junho através da transposição da Diretiva nº 2005/60/CE, de 26 de outubro, do Parlamento Europeu e do Conselho e da Diretiva nº 2006/70/CE, de 1 de agosto, da Comissão Europeia. Esta legislação obriga as entidades sujeitas ao dever de cuidado e de informação a comunicarem formalmente as operações suspeitas detetadas à Unidade de Informação Financeira (UIF) e ao Ministério Público (MP), mais concretamente à Procuradoria-Geral da República.

A comunicação é feita à UIF porque esta tem caracter estritamente policial e trata-se de uma unidade de *intelligence* no qual são elaborados relatórios que auxiliam e originam relatório finais. Contudo, não é suficiente para aplicação de medidas de suspensão de operações, pelo que a comunicação ao MP completa o trabalho da UIF através de recolha de dados de prova, em sede de inquérito, de forma a permitir junto do juiz a aplicação de medidas de suspensão de operações ou de outra natureza. O MP tem a competência de elaborar uma decisão de medidas de suspensão provisória, mas só é efetivada com a aprovação de um juiz de instrução.

No procedimento de prevenção do BC/FT existe também a intervenção das autoridades de supervisão e de fiscalização.

2.8.1. Autoridades de Supervisão e de Fiscalização

De acordo com o artigo 38.º da Lei nº 25/2008, de 5 de junho, a prevenção do BC/FT envolve autoridades de supervisão do setor financeiro e de fiscalização do setor não financeiro. É da competência destas autoridades a verificação do cumprimento dos deveres previstos nos quadros normativos em vigor, por parte das entidades sujeitas, entidades financeiras e não financeiras.

No artigo 38º é expresso quais as autoridades competentes para a verificação do devido cumprimento pelas entidades sujeitas, no que respeita a entidades financeiras, destacam-se os seguintes supervisores financeiros: o BdP, a Comissão do Mercado de Valores Mobiliários (CMVM) e a Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) no âmbito das respetivas funções e o Ministério das Finanças relativamente ao instituto de Gestão da Tesouraria e do Crédito Publico (IGCP). No que respeita às entidades não financeiras engloba-se: SRIJ, relativamente a concessionários de exploração de jogo em casinos e a entidades pagadoras de prémios de apostas ou lotarias, o Instituto da Construção e do Imobiliário (InCI) no caso de atividades de mediação imobiliária e de compra e revenda de imóveis e das entidades construtoras que procedam à venda direta de imóveis, a Autoridade de Segurança Alimentar e Económica (ASAE) no caso de comerciantes que transacionem bens em que o seu pagamento é feito em numerário, em montante igual ou superior a €15.000,00, as respetivas Ordens Profissionais das respetiva atividade de Advogados, Revisores Oficiais de Contas e Técnicos Oficiais de Contas, Câmaras no caso de solicitadores, Instituto dos Registos e Notariado (IRN) para os notários e conservadores de registos.

Os supervisores financeiros e outras autoridades competentes cooperam, trocam e compartilham informações. O BdP trabalha em conjunto com outras autoridades competentes, como o Ministério Público, como parte de um quadro formal. No caso da revisão de bancos associados a jurisdições específicas de alto risco, são realizadas inspeções conjuntas. Em 2005 e 2008 foram estabelecidos memorandos de entendimento para formalizar a cooperação entre o BdP, a CMVM e a ASF.

2.8.2. Ministério Público

O Departamento Central de Investigação e Ação Penal (DCIAP) inserido na Procuradoria-Geral da República é o departamento competente na prevenção do BC/FT. O DCIAP após o recebimento de uma comunicação por parte das entidades sujeitas ao dever de prevenção do BC/FT procede á sua análise, registando a comunicação como um procedimento de prevenção e procede-se à solicitação de informação à UIF, podendo também ser necessário um pedido de esclarecimentos adicionais às entidades sujeitas.

Os procedimentos de prevenção instaurados podem resultar na abertura de um inquérito sem que tenha havido a suspensão de operações ou podem os documentos obtidos serem anexados a inquéritos já instaurados.

2.8.3. Unidade de Informação Financeira

A Unidade de Informação Financeira (UIF) foi incluída na estrutura orgânica da Policia Judiciária com o Decreto-Lei nº 304/2002, de 13 de dezembro, no qual foi aprovada uma nova estrutura orgânica na Lei nº 37/2008, de 6 de agosto, passando a ser um serviço da Direção Nacional. A estrutura orgânica encontra-se em detalhe na Instrução Permanente de Serviço nº 6/2010.

Em conformidade com o Decreto-Lei nº 42/2009, de 12 de fevereiro e com a Lei n.º 25/2008, de 5 de junho, a UIF tem como competências recolher, centralizar, analisar e difundir a nível nacional a informação relacionada com a prevenção e investigação dos crimes de BC/FT e tributários através da cooperação e articulação com as autoridades judiciárias, supervisão e fiscalização e com as entidades financeiras e não financeiras e em âmbito internacional, com as unidades de informação financeira ou estruturas similares.

A UIF no desempenho das suas competências de recolha, centralização e análise tem acesso em tempo útil a informação financeira, administrativa, judicial e policial. No que diz respeito a competência de difusão, é da sua responsabilidade preparar e atualizar a difusão de dados estatísticos referentes ao número de transações suspeitas comunicadas, ao seu encaminhamento e ao seu resultado.

Ver processo de difusão de atos ilícitos de BC/FT entre entidades, ver Anexo C.

2.9. Principais organismos de cooperação Internacional e Regional

O combate ao BC/FT é efetuado com a cooperação de organismos internacionais, os quais estão organizados por região e fins específicos.

Para efeito de supervisão do sector bancário, o BdP celebrou vários Memorandos de Entendimento com autoridades de supervisão estrangeiras, incluindo vários parceiros estratégicos chave, no qual se inclui, França, Reino Unido, Brasil, Angola, Macau e China. Estão previstos oito protocolos que estão a ser negociados com parceiros internacionais, incluindo a China e os EUA.

2.9.1.Grupo de Ação Financeira

O Grupo de Ação Financeira (GAFI) é um organismo intergovernamental criado em 1989 pelo Grupo dos Sete (G7), grupo internacional composto por: Alemanha, Canadá, Estados Unidos, França, Itália, Japão e Reino Unido.

Este organismo tem como função desenvolver e promover medidas políticas, nacionais e internacionais para o combate do BC/FT, além de outras ameaças à integridade do sistema financeiro internacional relacionadas com estes crimes. Tratam-se de medidas legais, regulamentares e operacionais necessárias para o seu combate.

Em cooperação com outros organismos internacionais, o GAFI colabora na identificação de vulnerabilidades nacionais de forma a proteger o sistema financeiro internacional de condutas incorretas.

Este organismo intergovernamental emite recomendações para prevenir e reprimir os crimes de BC/ FT, promove a avaliação mútua da observância dos mesmos, determina contramedidas relativas às jurisdições com deficiências avultadas e identifica novos riscos e metodologias para o combate destes atos.

As recomendações do GAFI estão disponíveis desde 2012 no seu *site* oficial e estão acessíveis a todas as pessoas, destacando-se as Quarenta Recomendações sobre o Branqueamento de Capitais de 1990 e revistas sucessivamente em 1996, 2003, 2004, 2011 e 2012 e as Nove recomendações especiais sobre o Financiamento do Terrorismo. Estas recomendações são os princípios aceites unanimemente para o combate ao BC/FT.

Atualmente são 35 os países ou territórios membros do GAFI: África do Sul, Alemanha, Argentina, Austrália, Áustria, Bélgica, Brasil, Canadá, China, Dinamarca, Espanha, E.U.A., Finlândia, França, Grécia, Hong Kong, Índia, Irlanda, Islândia, Itália, Japão, Luxemburgo, Malásia, México, Noruega, Nova Zelândia, Países Baixos, Portugal, Reino Unido, República da Coreia, Rússia, Singapura, Suécia, Suíça e Turquia e duas organizações regionais: Comissão Europeia e Conselho de Cooperação do Golfo. Portugal é membro do GAFI desde 1990.

2.9.2. Organismos Regionais do Tipo GAFI

Os organismos regionais do tipo GAFI (ORTGs) são organismos voluntários e cooperantes que funcionam em conformidade com as normas estabelecidas pelo GAFI mas aplicados regionalmente ao contrário do GAFI que é aplicado ao Mundo. Tanto o GAFI como os ORTGs têm um papel importante na promoção e aplicação das normas ABC e de Combate ao Financiamento do Terrorismo (CFT) nas respetivas regiões.

Estes organismos regem-se pelo modelo aplicado pelo GAFI para combate ao BC/FT. Os ORTGs aplicam as Quarenta Recomendações sobre o BC e as nove recomendações especiais sobre o FT do GAFI, avaliam os seus membros e identificam deficiências de forma a traçar um plano de medidas corretivas. Alguns destes ORTGs adotam convenções e instrumentos próprios de ABC/CFT, por exemplo, o GAFIC publicou as “Recomendações de Aruba” que consiste em 19 recomendações de combate ao BC/FT adaptadas ao contexto das caraíbas, sendo um complemento das quarenta recomendações do GAFI.

A adesão é aberta a qualquer país ou jurisdição da respetiva região geográfica que esteja de acordo e disposto a cumprir as regras e os objetivos do organismo. Existem membro dos ORTGs que são também membros do GAFI.

2.9.3.Grupo Wolfsberg de Bancos

O Grupo Wolfsberg é composto por 12 bancos globais que se concentra nas preocupações relacionadas com o *private banking* através da criação de 4 princípios. *O private banking* é constituído pelos departamentos das instituições financeiras que fazem identificação dos clientes, do beneficiário efetivo das contas e de situações que necessitam de grande vigilância, como operações suspeitas.

2.9.4.Grupo Egmont

O Grupo Egmont é composto por UIFs, tendo como missão a partilha de conhecimentos e informação para combater o BC/FT. Agrega valor ao trabalho efetuado pelas suas UIFs membros, permitindo melhorar o apoio dado aos seus *stakeholders*. Este apoio traduz-se na expansão e sistematização na troca de informações financeiras, aumento da especialização dos seus recursos humanos, melhorar a comunicação entre as UIFs com recurso à tecnologia e ajudar a criar UIFs no mundo.

O Grupo Egmont é composto por 94 jurisdições como membros.

Portugal faz parte deste grupo desde 28 de maio de 1999.

2.9.5.Organização dos Estados Americanos

Esta organização é o organismo regional de segurança e diplomacia do Hemisfério Ocidental tendo sido ratificada a carta por 35 países do continente Americano, no qual deu origem à criação da Comissão Interamericana para o Controlo do Abuso de Drogas em 1986, para combater o tráfico de drogas neste hemisfério. Anos mais tarde, passou a incluir-se também o ABC nas suas funções.

Esta comissão elaborou estratégias regionais abrangentes e modelos de regulamentos para o combate ao tráfico de drogas, à proliferação de substâncias químicas e ao tráfico de armas, bem como para o combate do BC.

2.9.6.Secretariado da Commonwealth

O Secretariado da Commonwealth é uma associação voluntária composta por 53 Estados soberanos que cooperam entre si com intuito de promover a compreensão internacional e a paz mundial e interesses comuns dos Estados. Esta associação coopera juntamente com organizações nacionais e internacionais para ajudar na implementação e aplicação das Quarenta Recomendações e das Recomendações Especiais do GAFI pelos governos. Publicou *A Manual of Best Practices for*

Combating Money Laundering in the Financial Sector destinado às autoridades governamentais, aos reguladores e às instituições financeiras.

2.10. Banco de Portugal

O Banco de Portugal (BdP) é o banco central da República Portuguesa fundado a 19 de novembro de 1846. Na sua Lei orgânica, Lei nº 5/98, de 31 de janeiro e nas suas sucessivas alterações, estão presentes a natureza e as atribuições do BdP. O Banco é composto pelos seguintes órgãos: Governador, Conselho de Administração, Conselho de Auditoria e Conselho Consultivo (artigo 26.º, capitulo I, secção I). Desde 1998 que o BdP integra o Sistema Europeu de Bancos Centrais (SEBC) que é constituído pelo Banco Central Europeu (BCE) e os bancos centrais nacionais da União Europeia (ponto 1, artigo 3.º do capítulo I). Segundo o ponto 2 deste mesmo artigo, o BdP: "prossegue os objetivos e participa no desempenho das atribuições cometidas ao SEBC e está sujeito ao disposto nos Estatutos do Sistema Europeu de Bancos Centrais e do Banco Central Europeu, adiante designados por Estatutos do SEBC/BCE, atuando em conformidade com as orientações e instruções que o Banco Central Europeu, adiante abreviadamente designado por BCE, lhe dirija ao abrigo dos mesmos Estatutos ".

De acordo com o Tratado da UE "o objetivo primordial do SEBC é a manutenção da estabilidade dos preços", ou seja, a manutenção do poder de compra da moeda, que constitui o principal objetivo da política monetária.

O BdP faz parte do Eurosistema desde o seu início a 1 de janeiro de 1999, constituído pelo BCE e pelos bancos centrais nacionais participantes no euro. De acordo com o disposto no Tratado da UE e nos Estatutos do SEBC/BCE, é da responsabilidade do Governador exercer as funções de membro do Conselho e do Conselho-Geral do BCE.

O BdP tem a seu cargo duas missões principais: manutenção da estabilidade dos preços e a promoção da estabilidade do sistema financeiro.

Desempenha as seguintes funções: Politica Monetária; Gestão de ativos e reservas; Supervisão prudencial; Resolução; Política macroprudencial; Supervisão comportamental; Sistemas de pagamentos; Regulação e fiscalização do mercado cambial; Emissão de moeda; Compilação e elaboração de estatísticas; Produção de estudos e análises económicos; Atividade internacional; Relações com o Estado;

O BdP está organizado em 19 departamentos que são geridos por uma direção, a qual reporta a um membro do Conselho de Administração, designado por Administrador do Pelouro, conforme organograma do Anexo D.

2.10.1. Departamento de Averiguação e Ação Sancionatória

Em 2011 com a reorganização da estrutura de supervisão do BdP, com o objetivo de reforçar e autonomizar as suas diversas funções supervisivas, foi criado o Departamento de Averiguação e Ação Sancionatória (DAS), o qual inclui uma unidade de estrutura dedicada à prevenção do BC/FT - o Núcleo de Prevenção do Branqueamento.

Em 2017, o BdP contava com 23 funcionários em tempo integral a trabalhar em inspeções, políticas e questões institucionais relacionadas com ABC/CFT. Segundo o Relatório de Avaliação Mútua de Portugal 2017, este núcleo parece ter bons recursos e corresponde bem ao tamanho do setor, parece estar bem equipado para assumir obrigações de supervisão de ABC/CFT e realizar inspeções específicas e mais focalizadas, ao contrário de se concentrar em inspeções abrangentes concentradas apenas em instituições maiores, que tem sido a abordagem dos últimos cinco anos.

Esta unidade de estrutura é composta por técnicos: juristas, economistas e informáticos que asseguram as seguintes atividades:

- Executar ações e procedimentos de supervisão *on-site* e *off-site*;
- Assegurar a representação institucional do BdP junto de várias instâncias nacionais e internacionais relacionadas com o combate ao BC/FT, destacando-se o GAFI;
- Participar em processos de produção ou alteração normativa referentes à prevenção do BC/FT;
- Cooperar com as autoridades judiciárias e policiais.

2.10.2. Competências do BdP em matéria de Branqueamento de Capitais/Financiamento do Terrorismo

- Verificar se as instituições identificam, avaliam, acompanham e controlam o risco de BC/FT inerente à sua atividade;
- Avaliar se as instituições possuem sistemas de controlo adequados à mitigação do risco de BC/FT e o cumprimento das disposições legais e regulamentares presentes respetivamente na Lei nº 25/2008, de 5 de junho e o Aviso do Banco de Portugal n.º 2/2018, de 26 de setembro em vigor;
- Adotar as medidas de supervisão necessárias para a correção das falhas detetadas nos sistemas de controlo interno das instituições e à prevenção da ocorrência futura de situações idênticas, através da emissão de recomendações ou determinações específicas.

2.11. Abordagem Baseada no Risco

O BdP no seu exercício da supervisão ABC/CFT utiliza uma abordagem baseada no risco (ABR), abordagem essa que tem como objetivos principais: priorização das áreas de intervenção em função do grau de risco associado a cada instituição ou tipo institucional e gestão racional dos recursos afetos à prevenção do BC/FT. Esta abordagem permite direcionar a ação dos supervisores para as situações de maior risco e alocar de forma mais eficiente os recursos disponíveis.

O princípio geral desta abordagem é o seguinte: onde os riscos forem mais altos, os países devem exigir que as instituições financeiras e Atividades, Profissões e Negócios Não Financeiros (APNFDs) adotem medidas reforçadas para administrar e mitigar tais riscos, e onde os riscos forem menores, sejam permitidas medidas simplificadas.

2.11.1. Modelo efetivo de supervisão ABC/CFT baseada no risco

A supervisão baseada no risco (SBR) em matéria de ABC/CFT estabelece a frequência e a intensidade da supervisão das instituições em matéria de ABC/CFT tendo por base a avaliação dos riscos de BC/FT das instituições, de acordo com nº 6 do artigo 48.º, da Diretiva (UE) nº 2015/849. A supervisão efetuada pelas autoridades competentes não é um exercício pontual, mas um processo contínuo, dinâmico e cíclico.

Este Modelo de SBR estabelece um conjunto de procedimentos, processos, mecanismos e aspetos práticos de modo a que as autoridades competentes possam exercer os seus poderes de supervisão de ABC/CFT de forma lógica com os riscos de BC/FT identificados.

Segundo as Orientações Conjuntas ESAs 2016 72 de 07/04/2017, as autoridades competentes devem adotar o modelo efetivo de supervisão ABC/CFT baseada no risco, que se caracteriza pela adoção do seguinte procedimento baseado nas 4 fases seguintes:

- Fase 1 – Identificação de fatores de risco de BC/FT;
- Fase 2 – Avaliação do risco;
- Fase 3 – Supervisão;
- Fase 4 – Monitorização, revisão e ações de seguimento.

2.11.1.1. Fase 1 – Identificação de fatores de risco de BC/FT

O Risco de BC/FT consiste na *"probabilidade e no impacto da ocorrência de BC/FT. O termo «risco» refere-se ao risco intrínseco"*. (Orientações Conjuntas ESAs 2016 72 de 07/04/2017:5)

Antes de se aplicar o modelo SBR começa-se por se proceder à identificação dos fatores de risco intrínsecos de BC/FT a que o objeto de avaliação está exposto.

As autoridades competentes podem optar por agrupar instituições com características semelhantes (dimensão, natureza da atividade, tipo de clientes, áreas geográficas ou atividade e/ou canais de

distribuição) e considerá-las como um único objeto de avaliação. A quando do agrupamento deve-se ter o cuidado de verificar se as condições e os aspetos práticos do grupo são adequados aos riscos de BC/FT associados às instituições desse grupo. A dimensão ou a importância sistémica de uma instituição podem não ser indicativas do grau de exposição a um risco de BC/FT, até as pequenas instituições sem importância sistémica podem apresentar um risco elevado de BC/FT.

Entende-se como fatores de risco de BC/FT as "variáveis que, isoladas ou em combinação, podem aumentar ou reduzir o risco de BC/FT" (Orientações Conjuntas ESAs 2016 72 de 07/04/2017:5).

2.11.1.2. Fase 2 – Avaliação do risco

Os fatores de risco identificados anteriormente servem de base para se efetuar a avaliação do risco do objeto de avaliação das entidades supervisionadas.

É necessário avaliar de que modo é que os fatores de risco intrínsecos afetam o objeto de avaliação, e se os sistemas e controlos ABC/CFT aplicados ao objeto de avaliação são adequados para mitigar eficazmente os riscos intrínsecos de BC/FT a que este está exposto. Incluem-se como sistemas e controlos ABC/CFT o enumerado no nº 4, do artigo 8.º, da Diretiva (UE) nº 2015/849[7].

As autoridades competentes podem ponderar os fatores de risco e os mecanismos de controlo mitigadores, contudo tal ponderação carece de fundamentação. As autoridades competentes devem utilizar fatores semelhantes para objetos de avaliação semelhantes. "Deve ser atribuída maior ponderação a deficiências substanciais que possam afetar significativamente a eficácia das medidas preventivas ABC/CFT do que a deficiências médias ou menores. " (Orientações Conjuntas ESAs 2016 72 de 07/04/2017:13)

2.11.1.3. Fase 3 – Supervisão

A base da estratégia de supervisão de cada objeto de avaliação e do seu sector é a avaliação que foi feita do risco do objeto de avaliação. Os recursos de supervisão alocados pelas autoridades

[7] 4. As políticas, os controlos e os procedimentos a que se refere o nº 3 incluem: a) O desenvolvimento de políticas, controlos e procedimentos internos, nomeadamente relativamente aos modelos de práticas de gestão do risco, a diligência quanto à clientela, a comunicação de informações, a conservação de registos, ao controlo interno, a gestão da conformidade, incluindo, quando adequado à dimensão e natureza da atividade, a designação de um responsável pela conformidade ao nível da direção, e o controlo dos funcionários; b) Quando adequado, em função da dimensão e natureza da atividade, uma função de auditoria independente para testar as políticas, controlos e procedimentos internos a que se refere a alínea a).

competentes para cada objeto de avaliação devem ser coerentes com o perfil de risco do objeto de avaliação.

As autoridades competentes podem adotar as seguintes estratégias de supervisão:

- Ajustamento da natureza da supervisão, ou seja, um ajustamento do rácio entre as ações de supervisão *off-site* e *on-site*.
- Ajustamento do âmbito da supervisão, ou seja, centrar a supervisão nos riscos subjacentes a determinados produtos ou serviços, identificação dos clientes, avaliação do risco, ou as atividades de monitorização contínua e de comunicação de informações;
- Ajustamento da frequência da supervisão, ou seja, quando os riscos são reduzidos a monitorização dos "indicadores-chave*"* ser menos frequente;
- Ajustamento da intensidade e intervenção da supervisão, ou seja, a intensidade e intervenção da supervisão deve variar consoante o risco, a extensão da revisão dos ficheiros de clientes, das amostras de transações e da comunicação de transações suspeitas realizadas *on-site.*

2.11.1.3.1. Supervisão *off-site* - inspeções diretas

A Supervisão *off-site* consiste na análise do relatório anual obrigatório que as Instituições Financeiras (IFs) submetem aos supervisores financeiros. Nestes relatórios constam informações sobre a implementação dos requisitos de ABC/CFT e medidas de mitigação.

Anualmente, o BdP recebe relatórios de risco de BC/FT e questionários de autoavaliação (Anexo E) de ABC/CFT de todas as entidades supervisionadas. Os relatórios de risco de BC/FT incluem uma descrição do modelo de gestão de risco BC/FT pelas IFs, incluindo fatores de risco relevantes e uma explicação do controlo dos mecanismos implementados para mitigar esses fatores de risco. Estes relatórios são analisados manualmente de acordo com uma abordagem baseada no risco. Em contrapartida, os questionários de autoavaliação de ABC/CFT consideram e avaliam os controlos implementados pelas IFs, mas automaticamente.

Estes relatórios servem também para o BdP fazer análises transversais do setor, por exemplo, os investimentos de certas jurisdições de alto risco, o capital envolvido, se canalizado dentro ou fora do sistema bancário português. Os relatórios de notícias ou indicadores podem desencadear ad hoc[8] e atividades de supervisão *off-site* pelo BdP.

2.11.1.3.2. Supervisão *on-site*

As atividades de supervisão *on-site* são muito minuciosas e podem durar dois meses ou mais, envolvendo uma equipa de múltiplos supervisores. Tanto para o BdP como a CMVM, a base das

[8] Proveniente do latim, em português e aplicado a este contexto, significa "desencadear algo específico"

inspeções *on-site* envolve revisão dos relatórios de risco de BC/FT e/ou controlos interno, medidas de supervisão anteriormente aplicadas e informações solicitadas às IFs. É obrigatório desde 2015 que as inspeções *on-site* estejam de acordo com o cumprimento de todas as obrigações de ABC/CFT. O número de inspeções ABC/CFT *on-site* no setor financeiro é relativamente baixo. Estas inspeções permitem verificar o funcionamento dos mecanismos de deteção e alerta de operações suspeitas de configurarem atos de BC/FT. A avaliação recai sobre os sistemas informáticos (ou mecanismos alternativos), os procedimentos adotados e a suficiência de recursos humanos alocados a esta missão, podendo incidir sobre a totalidade dos procedimentos preventivos ou sobre aspetos específicos criteriosamente selecionados.

Durante o processo *on-site*, o BdP fornece informações abrangentes aos avaliadores da metodologia aplicada e demonstra como é que os diferentes parâmetros foram combinados para a análise do risco e classificação das IFs.

O BdP realizou em 2015 uma revisão temática de bancos provenientes de jurisdições de alto risco, e em 2017 uma revisão nos sistemas informáticos relacionados com o ABC/CFT das IFs. Esta revisão teve por base deficiências identificadas durante inspeções *on-site* e *off-site*. O ABC feito pelo BdP está a mudar para uma abordagem de inspeção mais temática, com base em riscos sectoriais identificados, novos ou emergentes. Outra ferramenta de supervisão que fortalece ainda mais o programa de supervisão baseada no risco do BdP é a realização de inspeções antes do início dos negócios das IFs.

De acordo com o Relatório de Avaliação Mútua de Portugal 2017, o alvo das atividades de supervisão financeira do BdP até agora tem sido a implementação de obrigações específicas de ABC/CFT, como: manutenção de registos, obrigações de CDD[9], entre outros. Contudo, o BdP demonstrou que o seu foco está a mudar para a compreensão dos riscos e a implementação da abordagem baseada no risco pelas IFs. O BdP destaca como a frequência, o alvo e a profundidade das inspeções *on-site* correspondem às categorias de risco identificadas de cada instituição. Segundo este mesmo relatório, os avaliadores registaram progressos pelo BdP nos últimos anos na supervisão do sector de prestação de serviços de transferência de dinheiro ou valor, que é considerado um sector de alto risco em Portugal.

2.11.1.3.3. Avaliação do ABC/CFT feito pelo Banco de Portugal

Os supervisores do BdP utilizam uma amostra representativa de clientes, que pode incluir PEP e titulares originários de jurisdições consideradas de risco, e testam o funcionamento dos mecanismos de prevenção de BC/FT.

[9] *Customer Due Diligence* – Dever de diligência relativo à clientela

Procedimento da avaliação:

- Analise do histórico destes clientes para verificar se a respetiva *due diligence*[10] cumpriu todos os requisitos;
- Caso tenham sido detetadas operações suspeitas, verificar se estas transações foram reportadas à UIF e ao MP - DCIAP, de acordo com a lei;
- São também efetuados testes aos sistemas, para averiguar se detetam e bloqueiam as transações em tempo real.
- Após ocorridos os procedimentos indicados anteriormente, o BdP elabora um relatório de inspeção que inclui: determinações específicas vinculativas e recomendações para alterar os procedimentos de prevenção do BC/FT em causa de acordo com o quadro normativo aplicável e com as melhores práticas nacionais e internacionais. Caso tenham sido detetadas infrações, os relatórios incluem propostas de instauração de procedimentos sancionatórios.

No Anexo F constam 2 quadros que mostram a Atividade Sancionatória do Banco de Portugal nos anos 2017 e 2018.

2.11.1.4. Fase 4 – Monitorização, revisão e ações de seguimento

Na revisão do plano de avaliação do risco e de supervisão, deve-se rever as informações periodicamente que estão na base da avaliação do risco, e se necessário atualizá-las, pois a supervisão é um processo dinâmico. Na revisão do modelo de supervisão ABC/CFT baseada no risco, as revisões periódicas devem ser feitas para avaliar se os resultados obtidos através do modelo de supervisão ABC/CFT adotado e se alocação de recursos é coerente com os riscos de BC/FT identificados; As revisões extraordinárias devem ser efetuadas com periocidade fixa, e rever, atualizar ou alterar o seu modelo de supervisão ABC/CFT baseada no risco se a sua adequação ou eficácia for questionável.

Segundo avaliação o Relatório de Avaliação Mútua de Portugal 2017, no geral, as instituições financeiras parecem adotar as injunções e recomendações emitidas pelo supervisor. O tempo decorrido entre uma inspeção e ações subsequentes de acompanhamento, incluindo ações de supervisão, quando as deficiências identificadas não forem bem atendidas, pode ser reduzido. Com base nos resultados iniciais e na análise transversal dos relatórios de inspeção externa do BdP, a tendência inicial foi um aumento na compreensão e no nível de conformidade das IFs. Estas estão cientes das atividades de supervisão que ocorrem dentro de outras instituições financeiras, especialmente no setor de seguros. Acredita-se que as ações de supervisão tenham efeito em cascata noutras IFs. O número de Relatórios de transações suspeitas (RTS) arquivados está de acordo com as expectativas de

[10] Termo que em português significa “Diligência prévia”

supervisão e tem aumentado nos últimos anos, o que poderia ser atribuído às ações de supervisão efetuadas no setor.

Os supervisores financeiros utilizam uma variedade de meios para promover a compreensão das obrigações ABC/CFT entre as IFs. Segundo o Relatório de Avaliação Mútua de Portugal 2017, entre os supervisores financeiros, o BdP é o mais proactivo na utilização de canais formais para promover a compreensão das IFs, dados os recursos disponíveis do BdP e os níveis de risco identificados. Os supervisores financeiros emitiram regulamentos ABC/CFT, no qual o BdP emitiu orientações adicionais por escrito. A orientação é fornecida através dos *sites* institucionais dos supervisores financeiros e através da emissão de circulares, que são enviadas a todas as IFs. O BdP organizou sessões de formação e seminários para o setor, tendo também um endereço de correio eletrónico dedicado ao ABC/CFT, usado frequentemente por IFs, com questões específicas sobre obrigações de ABC/CFT.

2.12. Ferramentas Tecnológicas

Neste capítulo aborda-se a temática das ferramentas tecnológicas utilizadas pelo BdP para supervisão das IFs bem como um protótipo de um Sistema Inteligente Anti-Branqueamento de Capitais.

2.12.1. Ferramentas Tecnológicas utilizadas pelo Banco de Portugal

O Banco de Portugal entre os supervisores financeiros é o que possui uma avaliação/supervisão do BC/FT mais abrangente. Para auxílio do seu exercício utiliza as seguintes ferramentas:

2.12.1.1. Índice de Atenção Supervisiva

O Índice de Atenção Supervisiva (IAS) interage com os dados obtidos da Avaliação Nacional de Riscos e na Avaliação de Risco Setorial e extrai informações provenientes de inspeções *on-site* e *off-site*.

Deste modo, este índice permite ao BdP atribuir e aplicar uma classificação de risco a cada instituição supervisionada. Esta classificação atribuída é baseada em vários parâmetros quantitativos e qualitativos, incluindo o risco de atividade da instituição, análise de risco baseada em inspeções gerais e específicas de ABC/CFT, informações de supervisão *off-site* e a avaliação supervisora.

O IAS é atualizado todos os meses de modo a refletir as informações coletadas e analisadas durante as inspeções. O BdP usa a classificação das instituições para determinar atividades de supervisão específicas para essas instituições. Esta atualização mensal fornece ao BdP uma eficaz ferramenta para implementar e ajustar a SBR.

2.12.1.2. Base de Informação de Inspeções e Averiguações

Segundo o Relatório de Avaliação Mútua de Portugal 2017, o modelo ABC/CFT de abordagem baseada no risco é o mais desenvolvido no BdP, e como tal o BdP criou um Banco de Dados de Inspeção e Investigação, a Base de Informação de Inspeções e Averiguações (BIIA). O BIIA é uma aplicação informática desenvolvida pelo DAS e pelo Departamento de Sistemas de Informação (DSI) que constitui uma ferramenta multifuncional, que tem servido como base para o desenvolvimento de outras aplicações para outros departamentos. Esta aplicação não só assegura a definição do IAS e a hierarquização das instituições em função do seu IAS, como também adiciona fontes externas e internas de informação a todas as instituições.

2.12.2. Sistemas ABC utilizados pelas IFs

Como foi referido anteriormente o BdP efetua supervisão *off-site* onde avalia relatórios de risco de BC/FT que incluem uma descrição do modelo de gestão de risco BC/FT pelas IFs e supervisões *on-site* onde se avalia os sistemas informáticos (ou mecanismos alternativos) utilizados pelas entidades supervisionadas por este, averiguando se os sistemas informáticos detetam e bloqueiam as transações em tempo real.

Segundo o artigo 9.º do Aviso do Banco de Portugal n.º 2/2018, o BdP tem o dever de controlar se as IFs adotam as ferramentas/sistemas de informação instrumentais ou auxiliares, do cumprimento das obrigações e deveres previstos na Lei n.º 83/2017, de 18 de agosto e no presente Aviso.

As ferramentas/sistemas de informação utilizados pelas IFs devem:

- Consolidar os registos relativos a relações de negócio, transações ocasionais ou operações em geral, próprias ou por conta de clientes, incluindo os suportes documentais recolhidos em cumprimento do dever de identificação e diligencia;
- Tratar a informação em bases de dados de acesso restrito, atribuindo diferentes classificações e perfis de acesso, para que previna a sua partilha ou divulgação indevidas, dentro da própria IF ou perante terceiros;
- Manter as bases de dados atualizadas e integralmente acessíveis, de forma a assegurar o cumprimento do disposto na alínea j) do nº 2 do artigo 18.º da Lei n.º 83/2017, de 18 de agosto.

As IFs devem garantir o acesso integral e imediato às ferramentas ou sistemas de informação sempre que solicitado pelo BdP.

2.12.2.1. Sistema Inteligente Anti-Branqueamento de Capitais

O sistema seguinte é um Sistema Inteligente Anti-Branqueamento de Capitais[11], trata-se de um protótipo elaborado pela Universidade de Hong Kong.

Um Sistema Inteligente ABC possui a capacidade de monitorizar todas as transações financeiras, descobrir comportamentos fora do comum e separar as transações que representem um risco real para as instituições financeiras. É capaz de aprender e adaptar-se, aprendendo novos esquemas de BC à medida que eles surgem. Baseia-se numa abordagem corporativa, determinando todas as transações que são pouco comuns, em vez de procurar padrões ou comportamentos específicos ao analisar o perfil do cliente e as transações realizadas pela IF.

2.12.2.1.1. Agentes Inteligentes

O desenvolvimento de agentes inteligentes (AIs) e de sistemas multi-agentes (SMAs) tem vindo a ganhar popularidade. Um AI é aquele que possui uma ação autónoma flexível para atingir os objetivos do projeto, através de autonomia, capacidade social, reatividade e proatividade. Um agente genérico possui um conjunto de objetivos, capacidades de executar inúmeras tarefas e possui conhecimentos sobre o seu ambiente em redor.

Para atingir os seus objetivos, um agente utiliza o seu conhecimento racional sobre o seu ambiente e os comportamentos de outros agentes, para gerar planos e executar esses planos.

O SMA consiste num grupo de agentes, que interagem uns com os outros para atingirem coletivamente os seus objetivos. Os agentes absorvem os conhecimentos e capacidades de outros agentes, superando assim os seus limites inerentes de inteligência. Um dos fatores atuais que fomentam o desenvolvimento de SMA é o aumento da popularidade da Internet, que fornece bases para um ambiente aberto, onde os agentes interagem uns com os outros para alcançar os seus objetivos individuais ou compartilhados.

Agentes inteligentes:

- *Data Collecting Agent* (Agente “Coletor” de Dados)
- *User Agent* (Agente Utilizador)
- *Monitoring Agent* (Agente Monitor)
- *Behavior Diagnosing Agent* (Agente que faz Diagnóstico Comportamental)
- *Reporting Agent* (Agente que Reporta)
- *Internal Data Collecting Agent (Agente* “Coletor” de Dados Internos)
- *External Data Collecting Agent (Agente* “Coletor” de Dados Externos)

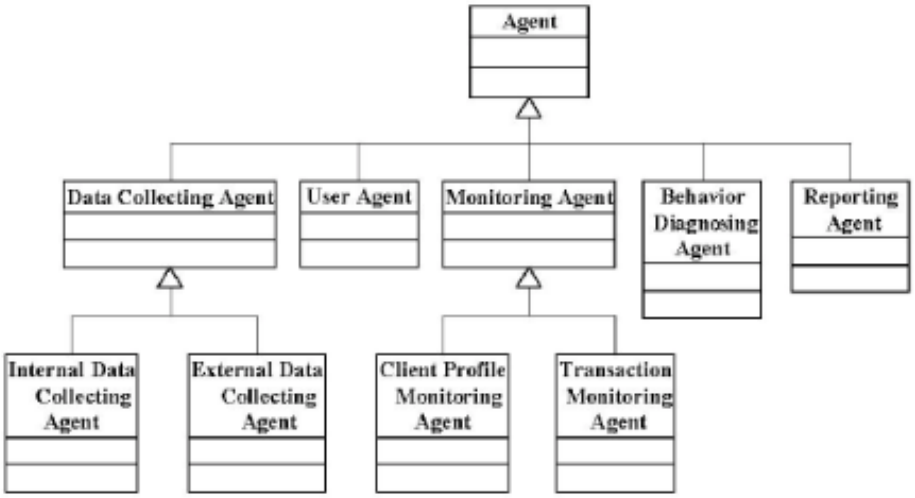
[11] Gao S, Xu D, Wang H, Wang Y. Intelligent anti-money laundering system. (2006: 851-856)

- *Client Profile Monitoring Agent* (Agente Monitor de Perfis de Clientes)
- *Transaction Monitoring Agent (*Agente Monitor de Transações)

2.12.2.1.2. Desenvolvimento de Agentes Inteligentes

Para projetar a arquitetura de um SMA de ABC, decompomos o processo de ABC em várias fases autónomas, nas quais cada agente possui uma tarefa específica cujo comportamento é reativo e orientado com base em metas, cooperando com outros agentes para perseguir os seus objetivos.

Figura 1 - Fases do Processo ABC



Fonte: Gao S, Xu D, Wang H e Wang Y. (2006: 853)

2.12.2.1.3. Arquitetura do Sistema

Qualquer solução de ABC deve ser baseada na capacidade de descobrir atividades financeiras suspeitas, identificando os indivíduos ou organizações específicas que podem estar envolvidos.

Dada a complexidade do ABC, um sistema automatizado não define se uma atividade detetada é suspeita, apenas deteta atividades que necessitam de interpretação de um analista.

A intervenção humana é necessária para determinar se uma atividade é suspeita e necessita de ser reportada. Deste modo, a melhor forma de implementar o controlo e a prevenção do BC é a existência de uma simbiose entre a perícia humana e a inteligência artificial.

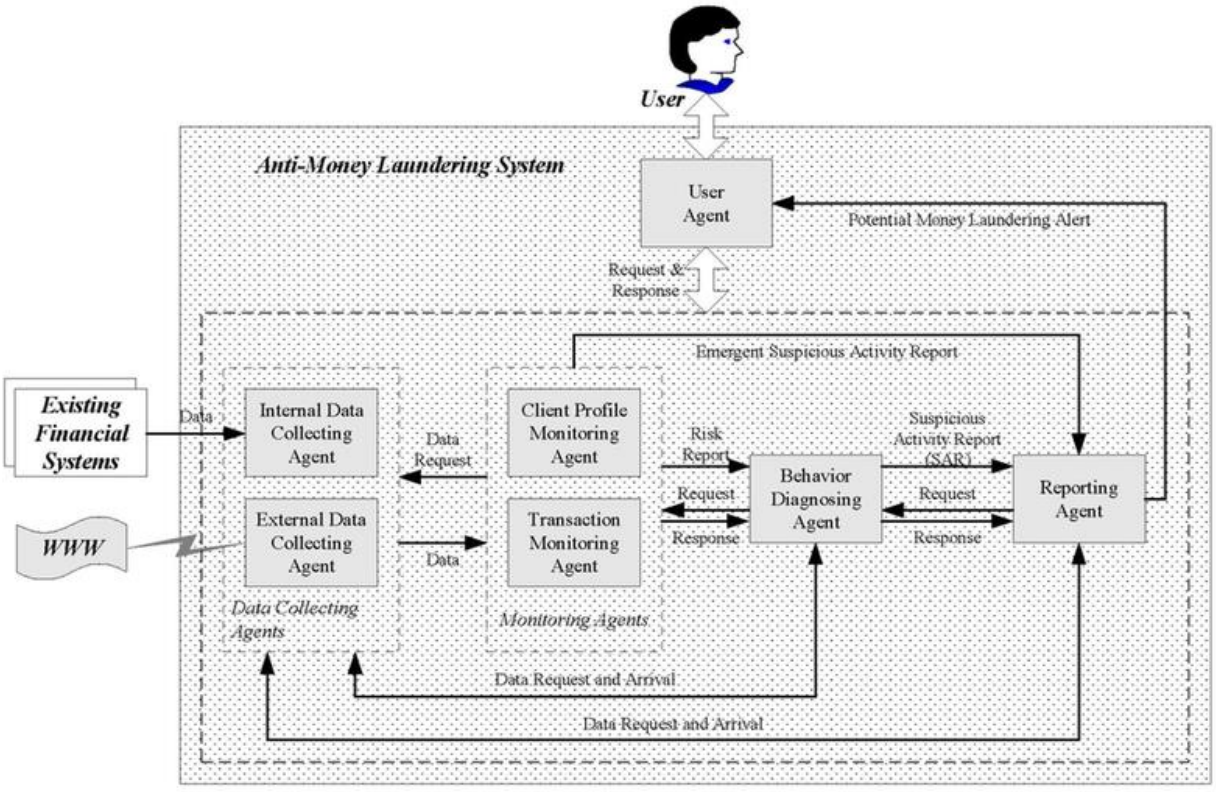
Nesta pesquisa, o sistema automatizado realiza o trabalho de deteção, enviando alertas relativas a transações consideradas suspeitas, enquanto os analistas humanos realizam investigações sobre os casos que são detetados.

Existem duas formas de desenvolver uma solução ABC inteligente:

- Reengenharia dos sistemas financeiros existentes para apoiar funções ABC;
- Desenvolver um sistema independente interligado com as aplicações existentes, através das quais todos os clientes e dados de transações passariam durante o seu ciclo de vida;

Os sistemas financeiros existentes são distribuídos em várias instituições, (como bancos, seguradoras, fundos imobiliários, entre outros.), sendo fundamental usar recursos internos para construir *softwares* com capacidade de interagir entre sistemas.

Figura 2 - Arquitetura de um Sistema Inteligente ABC e a interação entre agentes



Fonte: Gao S, Xu D, Wang H e Wang Y. (2006: 854)

O *User Agent* fornece a interface para o usuário que, por norma, é um analista de BC e permite que os utilizadores visualizem o estado atual das transações financeiras e os processos de monitorização, diagnóstico e relatórios de BC. Este agente comunica e coopera com outros agentes, executando automaticamente as suas operações e dando respostas diferentes consoante eventuais mudanças ambientais.

Os *Data Collecting Agents* permitem que o sistema colete dados internamente e externamente.

Em particular, o *Internal Data Collecting Agent* é responsável pela aquisição de dados em tempo real de sistemas financeiros existentes para a avaliação do perfil do cliente, a mensuração do risco da transação, o diagnóstico e o relatório de comportamento adicional.

Coleta dados associados a possíveis esquemas de BC como por exemplo: perfis de clientes, detalhes de transações financeiras, dados de referência de contas, dados de referência de clientes, estatísticas históricas, entre outros.

Por outro lado, o *External Data Collecting Agent* coleta dados das outras entidades de combate ao BC, do governo e de outras autoridades. Os dados incluem padrões internacionais, regulamentos oficiais, listas de observação, legislações, entre outros.

Os *Monitoring Agents*, *Diagnosing Agent* e *Reporting Agent,* podem solicitar dados relacionados com as suas tarefas aos *Data Collecting Agents*, se necessário.

Os *Monitoring Agents* incluem:

- *Client Profile Monitoring Agent*;
- *Transaction Monitoring Agent*;

Estes agentes são colocados no sistema para monitorizar possíveis esquemas de BC numa base de "cliente-para-cliente" e de "transação-para-transação", seguindo a política central globalmente aceite para controlos efetivos de BC – *Know your Consumer (*KYC).

O *Client Profile Monitoring Agent* avalia uma ampla variedade de informações detalhadas relacionadas com a conta do cliente, normalmente coletadas no momento em que a conta é aberta. O agente fornece uma visão única do perfil do cliente, incorporando todos as relações financeiras com as quais a conta tem uma afiliação.

Cada cliente é classificado em diferentes perfis de risco, e com base na classificação de risco do cliente, o agente determina a frequência e a intensidade da monitorização.

O *Transaction Monitoring Agent* serve para identificar transações que apresentam maior risco de possíveis atividades de BC. As transações classificadas de maior risco podem variar de organização para organização com base nas suas linhas e tipos de negócios. Por exemplo, o risco associado às transações de um banco seria diferente do risco associado a uma agência de seguros ou a uma empresa de valores mobiliários.

No geral, o comportamento de risco de transações inclui (mas não é limitado a):

- Movimentação rápida de fundos para dentro ou fora da conta;
- Atividade repentina numa conta anteriormente inativa;
- Alterações frequentes numa conta;
- Transações recorrentes;

- Relações de conta ocultas;
- Compensação, negociações, liquidação e/ou instruções permanentes de uma conta;
- O movimento de fundos sem um comércio correspondente e o depósito do excesso de garantia numa conta.

Por norma, se um perfil de cliente for questionável ou se for detetada uma transação fora do comum pelos *Monitoring Agents*, é emitido e enviado um relatório de risco para o *Behavior Diagnosing Agent,* para se proceder a uma investigação mais aprofundada.

Contudo, um relatório de atividades suspeitas (RAS) pode ser emitido e enviado ao utilizador, para ação instantânea.

O *Behavior Diagnosing Agent* ao receber os relatórios de risco dos *Monitoring Agents* inicia o seu processo de diagnóstico para investigar o comportamento complexo que é usualmente associado a esquemas de BC. Este agente pode realizar análises sobre relatórios de risco dos *Monitoring Agents* e solicitar qualquer informação adicional, se necessário, para examinar os casos.

Este agente permite que as instituições financeiras detetem irregularidades, encontrando padrões suspeitos de comportamento que possam estar ocultos por trás de grandes volumes de dados financeiros. É também capaz de identificar eventos suspeitos e entidades que são construídos ao longo do tempo, separando-os de eventos e transações do dia-a-dia.

Quando o *Behavior Diagnosing Agent* identifica um comportamento fora do comum ou suspeito, é automaticamente produzido e enviado um RAS para o *Reporting Agent*.

Em seguida, o *Reporting Agent* apresenta e comunica um alerta de possível BC ao pessoal apropriado, por meio do *User Agent*, para investigação e ação imediata.

O *Reporting Agent* irá automatizar ou tomar conta da situação, por exemplo, interferindo com operações padrão de modo a bloquear uma transação suspeita em particular.

Os casos para investigação são filtrados e priorizados com base na gravidade do alerta. O *Reporting Agent* fornece evidências da atividade e das informações do cliente, garantindo que o responsável pelo caso tenha todas as informações relevantes do cliente disponíveis. Se necessário, são solicitadas informações adicionais ao *Behavior Diagnosing Agent.*

Isto permite que se tomem decisões baseadas em factos e demonstra uma *due diligence* regulatória no processo. O *Reporting Agent* também simplifica o combinar dos alertas gerados automaticamente com relatórios manuais, para construir o caso para investigação.

Os relatórios do *Reporting Agent* fornecem um sistema de rastreamento completo e caminho de auditoria, para gerir ações em resposta a eventos detetados ou comportamentos suspeitos. Esses

relatórios extensos permitem que as instituições financeiras demonstrem conformidade com as regras de ABC e a adotação dos requisitos regulatórios.

2.12.2.1.4. Operacionalização do Sistema

Para avaliar a arquitetura do sistema referido anteriormente foi elaborado um protótipo que realiza a análise, monitorização e diagnóstico, gerando relatórios com base no perfil de cliente simulado e nos dados de transações financeiras, utilizando para isso um pequeno número de AIs.

Dentro deste protótipo, os *Data Collecting Agents* coletam continuamente dados relevantes de clientes e de transações simuladas em tempo real, respondendo automaticamente a qualquer solicitação de dados de outros agentes, em tempo útil.

O *Monitoring Agent* e o *Behavior Diagnosing Agent* são pré-configurados com cenários detalhados de BC. Esses cenários são padrões de comportamento do interesse da organização e baseados nas regras de conformidade do Regulador, como por exemplo, as 40 Recomendações do GAFI. Estes cenários são adaptáveis e facilmente estendidos.

Os agentes possuem flexibilidade para permitir que as organizações incorporem os seus próprios cenários específicos de negócio, refletindo as suas práticas de segurança.

As várias técnicas avançadas são combinadas com uma abordagem holística baseada em riscos.

Ao avaliar outros fatores de risco, os alertas mais relevantes são assinalados, com uma abordagem baseada numa combinação do risco, de regras, deteção de anomalias, rede neutra, lógica difusa e programação linear. Tudo isto resulta numa ponderação de risco.

Para cada cenário, são atribuídas pontuações a cada fator de risco e, em seguida, multiplicadas pela ponderação de risco para obter as pontuações gerais. Deste modo, a instituição financeira é capaz de avaliar com mais eficiência os padrões de BC no contexto de outros fatores de risco existentes.

Ao lidar com padrões inéditos, esses agentes são capazes de “aprender” esses padrões, para referência futura. Desta forma, eles podem adaptar-se a diferentes cenários e ter bons resultados tanto em padrões vistos anteriormente como inéditos.

Por exemplo: Foram detetados os seguintes acontecimentos, três meses simulados de dados de transações bancárias mostram depósitos que foram feitos diariamente para uma conta em moeda estrangeira totalizando cerca de 350.000 dólares.

No mesmo período de tempo, existem 10 transferências eletrónicas no total de 2,7 milhões de dólares para um banco nos Emirados Árabes Unidos.

Estas atividades fora do comum são capturadas pelo *Transaction Monitoring Agent* e são encaminhados para o *Behavior Diagnosing Agent* no formato de um relatório de risco.

Para investigar, o *Behavior Diagnosing Agent* efetua uma análise do perfil do cliente através do *Client Profile Monitoring Agent* e da origem e informações da conta de destino e detalhes da transação através do *Transaction Monitoring Agent* e de dados adicionais através do *External Data Collecting Agent*.

Após a análise baseada no risco, são emitidos três alertas pelo protótipo:

- O primeiro é "Relacionamento com o terrorismo **",** já que o perfil da empresa mostra que a maior parte das transações desta empresa foram realizadas por países associados a atividades terroristas (como por exemplo, Emirados Árabes Unidos, que é identificado como um país de alto risco);
- O segundo alerta é "A empresa estava envolvida em várias transações com drogas que ocorreram na Colômbia", pois foi baseado nas conclusões da *Drug Enforcement Administration* e nos registros do banco, a empresa estava sempre a receber dinheiro de contas de organizações da Columbia;
- O terceiro é "fonte pouco clara de uma grande quantidade de dinheiro", uma vez que nenhuma informação mostrou como é que dinheiro foi ganho com seus negócios, existindo apenas registos que indicavam que a empresa recebia dinheiro de contas individuais de outros países ou de empresas colombianas ou bancos.

2.12.2.1.5. Conclusão do Sistema Inteligente Anti-Branqueamento de Capitais

Este artigo explora a abordagem de aplicação de agentes inteligentes para o ABC, de forma a ultrapassar as limitações das soluções existentes. É um sistema ABC baseado em agentes múltiplos projetado e implementado e onde vários tipos de AIs são utilizados para fornecer um conjunto de funcionalidades.

Em suma, a abordagem deste estudo tem várias vantagens para o ABC:

- Inteligência - esquemas BC complexos e distribuídos podem ser identificados e diagnosticados por um número de agentes inteligentes através das suas propriedades, tais como autonomia, reatividade, proatividade e habilidade social;
- Adaptabilidade – o sistema realiza não só um trabalho autónomo de monitoramento e diagnóstico, mas também é capaz de aprender com o seu ambiente, adaptar-se a mudanças no ambiente e tomar decisões que podem ser entregues e interpretadas pelos olhos humanos;
- Integração de sistemas - Através do *User Agent*, que corresponde ao Sistema Inteligente de ABC, é capaz de integrar facilmente com aplicativos financeiros;

- Escalabilidade - É fácil adicionar mais funcionalidades de negócios ao sistema adicionando mais agentes. Também é simples modificar, inserir ou excluir regras de negócios ou cenários de BC no sistema;
- Valores de negócios – pode oferecer benefícios significativos para os negócios em termos de redução de custos, eficiência do negócio, aumento de produtividade e novo estilo de operação.

2.12.3. Sistemas inteligentes ABC existentes no mercado

Realizou-se uma pesquisa a fim de descobrir *softwares* ABC existentes no mercado, e observou-se que grande parte dos softwares existentes apenas detetam padrões/ameaças/transações suspeitas com base nos dados da empresa, não havendo qualquer interface com outras bases dados ou sistemas.

Ao investigar as várias opções existentes no mercado atualmente inferiu-se que existem várias empresas a desenvolver sistemas para suporte ao combate de BC (ou seja, sistemas de deteção de padrões e ameaças). No entanto, seis destacam-se claramente como sendo as melhores/mais utilizadas: BAE Systems, Clear View KYC, Thompson Reuters, FICO TONBELLER, SAS e Feedzai AML.

Estas soluções focam-se todas em análise comportamental, *compliance*, verificação de identidades (KYC e PEPs), análise de risco, *know your transactions* (KYT) e gestão de risco.

A maioria destes sistemas são baseadas na *Cloud* (Azure e AWS por exemplo) funcionando, portanto, como IaaS (*Infrastructure as a Service*) e todos utilizam base de dados com padrões, regras e limites pré-definidos, que usam para comparar as potenciais ameaças que detetam.

Estas soluções apresentam algumas lacunas como por exemplo:

- Dificuldade em detetar esquemas de BC de baixos montantes (Por exemplo, nos atentados do 11 de setembro, os terroristas efetuavam transações com um baixo somatório de valores, estando dentro dos limites estabelecidos. Como tal não foram detetados);
- Existem transações que ultrapassam o limite estabelecido, pelo que estão marcadas como suspeitas, mas não representam nenhum caso de BC;
- Dificuldade em detetar esquemas de BC delineando um perfil com base em informações da indústria ou de determinados padrões associados a atividades suspeitas de BC;
- Os sistemas baseados em regras têm a capacidade de reconhecer comportamentos padrão, contudo não possuem a capacidade de aprendizagem, reconhecendo apenas padrões que já estão presentes na sua base de dados. Assim, muitos destes sistemas não têm capacidade de fazer face ao desenvolvimento do BC;
- As instituições financeiras apresentam um grande volume de transações, que estão constantemente a aumentar. Os sistemas existentes não possuem capacidade para verificar

todas as transações de forma abrangente e consistente. A verificação de transações suspeitas de BC acarretam custos elevados;

Algumas, como é o caso do sistema da Thompson Reuters, utilizam uma base de dados global que pode ser consultada e que vai sendo atualizada. No entanto, tanto este tipo de base de dados, como as dos sistemas que utilizam uma base de dados interna que pode ser atualizada, são atualizadas no máximo apenas uma vez por dia (com a exceção da solução da BAE *Systems*), o que no combate a este tipo de crime pode não ser suficiente.

Com exceção da solução da Feedzai, que utiliza Inteligência Artificial, nenhuma das soluções disponíveis é especialmente "inteligente", na medida em que dependem das bases de dados para comparação de padrões, não sendo capazes de detetar novos tipos de ameaças.

Conclusão, as soluções atualmente disponíveis são de uma maneira geral, pouco "inteligentes", quase na totalidade baseadas em sistemas *cloud* (o que, apesar de aumentar a versatilidade, para instituições financeiras pode não ser a melhor solução sob o ponto de vista de segurança e controlo, uma vez que a solução não está na infraestrutura própria, sendo também bastante mais caro a longo prazo manter infraestrutura na *cloud*) e recebem informação atualizada com pouca frequência, não existindo neste momento nenhuma solução que combine soluções para estas três questões.

3. Metodologia de Investigação

Este capítulo apresenta as metodologias adotadas na presente dissertação, como metodologia de estudo utilizou-se como técnicas de recolha de dados: a análise documental e a realização de uma entrevista.

A metodologia de investigação consiste num "processo de seleção da estratégia de investigação, que condiciona, por si só, a escolha das técnicas de recolha de dados, que devem ser adequadas aos objetivos que se pretendem atingir." (Sousa & Baptista, 2011: 52)

Tendo em conta os objetivos propostos para a presente investigação, o método de investigação qualitativa apresentou-se como o mais adequado e lógico.

3.1. Método de Investigação Qualitativa

Como o objetivo desta investigação é conhecer as ferramentas tecnológicas utilizadas no combate do BC/FT e a função do BdP enquanto supervisor, utilizou-se o método de investigação qualitativa.

A investigação qualitativa ao contrário da investigação quantitativa não se preocupa com a dimensão da amostra nem com a generalização dos resultados, com a validade e finalidades dos instrumentos. Foca-se em compreender os problemas, analisar comportamentos, atitudes ou valores. (Sousa & Baptista, 2011: 52).

Esta investigação através dos dados recolhidos permite ao investigador desenvolver conceitos, ideias e entendimentos a partir de padrões encontrados nos dados recolhidos. (Sousa & Baptista, 2011: 52).

O estudo incidirá em estudar uma realidade bastante recente e pouco estudada, como é o caso das ferramentas tecnológicas para combate do BC/FT. Deste modo, este estudo classifica-se como exploratório. (Marshal e Rossman,1995:40-41)

3.1.1. Análise Documental

A análise documental consiste em "identificar, verificar e apreciar os documentos com uma finalidade específica e, nesse caso, preconiza-se a utilização de uma fonte paralela e simultânea de informação para complementar os dados e permitir a contextualização das informações contidas nos documentos. A análise documental deve extrair um reflexo objetivo da fonte original, permitir a localização, identificação, organização e avaliação das informações contidas no documento, além da contextualização dos factos em determinados momentos." (Souza et al., 2011: 223)

Tendo em conta o tema da presente dissertação, a análise documental justifica-se pela utilização de documentos dos organismos internacionais de combate ao BC/FT e legislação como parte da fonte de informação utilizada.

3.1.2.Entrevista

A entrevista é um método de recolha de informações que consiste em conversas orais individuais ou em grupo, cujo entrevistado possui pertinência, validade e fiabilidade em relação aos objetivos proposto pela tese. (Ketele & Roegiers, 1999)

Uma entrevista é uma "análise do sentido que os atores dão às suas práticas e aos seus acontecimentos com os quais se veem confrontados: os seus sistemas de valores, as suas referências normativas, as suas interpretações de situações conflituosas ou não, as leituras que fazem das próprias experiencias, etc." (Quivy & Campenhoudt, 1998:193)

Segundo o autor Sousa & Baptista, as entrevistas dividem-se em 3 tipos: entrevistas não-estruturadas, entrevistas semiestruturadas e entrevistas estruturadas.

As entrevistas semiestruturadas possuem um guião, com um conjunto de tópicos ou perguntas para abordar na entrevista. Neste tipo de entrevista, o entrevistado possui liberdade para se expandir mas com alguma rigidez. Optou-se por utilizar este tipo de entrevista pois o tema da presente investigação é bastante amplo e incide em vários extensões, pelo que uma entrevista semiestruturada permite que seja seguida uma linha de pensamento ao longo da entrevista, mas que permita ao entrevistador expandir-se sobre o tema, mas dentro do contexto da entrevista.

Segundo Sousa & Baptista uma entrevista pode possuir questões abertas e fechadas. As questões abertas permitem o entrevistado expor e justificar a sua opinião, enquanto nas questões fechadas, o entrevistado não tem a possibilidade de desenvolver a sua resposta. Tendo em conta que o tema da presente investigação é bastante amplo e incide em várias extensões, é mais vantajoso para o estudo que se façam entrevistas com questões abertas pois permite que haja um maior detalhe na informação partilhada.

3.1.2.1. Caracterização do entrevistado

O entrevistado foi o Senhor Professor Doutor Miguel Pardal. O Prof. Dr. Miguel Pardal fez a sua Licenciatura, Mestrado e Doutoramento no Instituto Superior Técnico (1995-2014), na área de *Computer Science and Engineering e Information Systems*.

Trabalhou como consultor na empresa Unisys Portugal entre 2000-2002.

É professor assistente no Instituto Superior Técnico desde Setembro de 2002 e a sua área de ensino é principalmente Segurança de Redes e Computadores e Sistemas Distribuídos.

É também investigador no INESC-ID, sendo o foco da sua investigação a Cibersegurança para Internet *of Things and Cloud*, tendo já apresentado vários *papers* e publicações desde 2004.

3.1.2.2. Guião da Entrevista

O guião (Anexo G) é composto por duas categorias:

1. Conhecimento sobre aplicações financeiras de combate ao BC/FT;
2. Metodologia para proteção de aplicações financeiras.

A Primeira Categoria tem como objetivo perceber se o entrevistado, tendo em conta a sua experiência, se conhece aplicações financeiras de combate ao BC/FT, com enfoque nas utilizadas pelo BdP e nos Sistemas Inteligentes ABC/CFT.

A Segunda Categoria tem como objetivo perceber como é feita a proteção de uma aplicação financeira olhando para o caso em concreto do sector bancário, perceber se no caso dos ataques do *NotPetya* e do *WannaCry* se o indicado anteriormente teria sido suficiente para impedir esses ataques, se as formas de proteção atuais podem manter-se aptas no futuro e qual o envolvimento do Centro Nacional de Cibersegurança neste tipo de aplicações financeiras.

3.1.2.3. Realização da entrevista

Numa entrevista é importante que o entrevistador possua todos os conhecimentos a respeito do tema, para que depois possa ser ele próprio a conduzir a mesma. (Rosa e Arnoldi, 2007), Deste modo, a entrevista foi realizada após se proceder à revisão da literatura, permitindo assim adquirir um conhecimento teórico sobre a temática abordar.

A entrevista foi marcada via correio eletrónico e realizada no ambiente de trabalho do entrevistado, Instituto Superior Técnico. Antes de se realizar a entrevista, o entrevistado preencheu uma Declaração de Consentimento elaborada e entregue por mim (Anexo H) e solicitou-se autorização para se proceder à gravação da entrevista através de áudio, pois permitiu uma maior atenção ao discurso do entrevistado, reduzindo-se assim a perda de informação relevante durante a entrevista.

A entrevista foi realizada no dia 11 de outubro de 2018 às 17h00, tendo tido uma duração de aproximada de 25 minutos.

4. Análise e discussão dos resultados

4.1. Categorias da entrevista

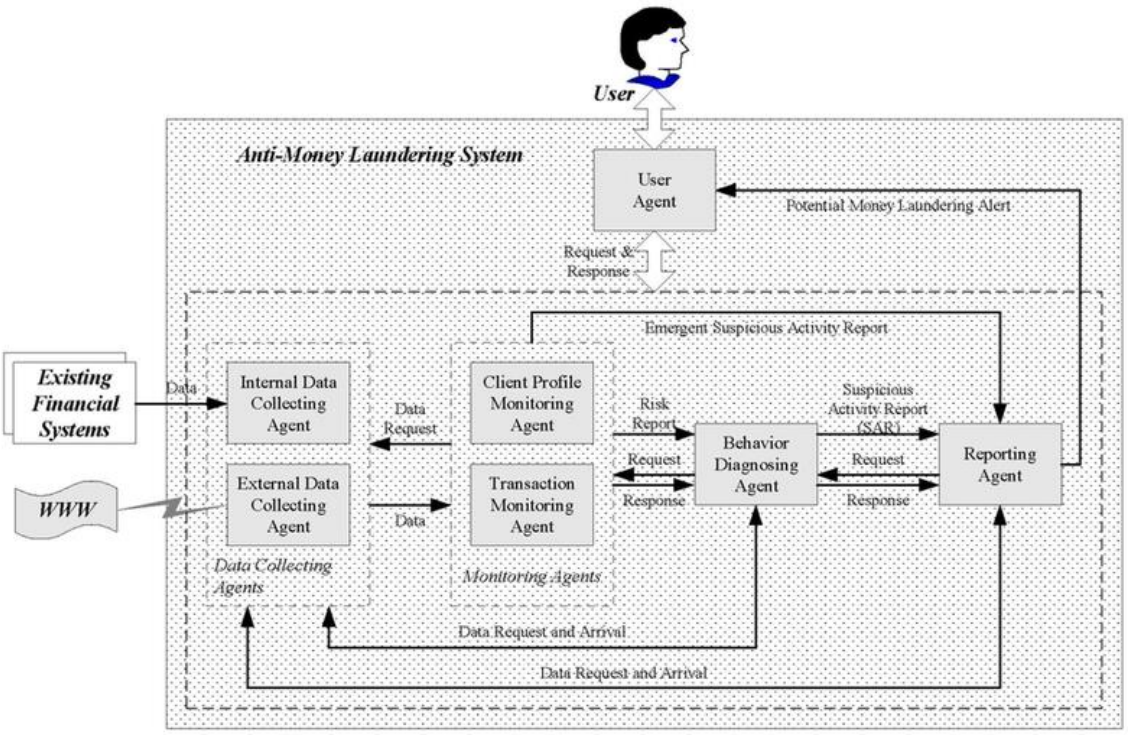
4.1.1. Categoria I - Conhecimento sobre Aplicações Financeiras de Combate ao BC/FT

Esta categoria tem como objetivo perceber se o entrevistado, tendo em conta a sua experiência, se conhece aplicações financeiras de combate ao BC/FT, com enfoque nas utilizadas pelo BdP e nos Sistemas Inteligentes Anti-Branqueamento de Capitais/Financiamento do Terrorismo.

Para se alcançar estas informações, elaboraram-se as seguintes questões:

1. O BdP utiliza uma aplicação informática, o BIIAS - Base de Informação de Inspeções e Averiguações, que assegura a definição do Índice de Atenção Supervisiva (IAS) e a hierarquização das instituições em função desse índice. O IAS é atribuído a cada instituição e calculado com base em informação interna e externa de natureza e proveniência diversa. Face ao exposto, gostaria de lhe perguntar se tem conhecimento sobre este tipo de aplicações utilizadas no combate ao BC e ao FT? Se sim, qual/quais? Na sua opinião, como acha que estes sistemas podem ser melhorados?
2.

Figura 3 - Arquitetura de um Sistema Inteligente ABC e a interação entre agentes



Fonte: Gao S, Xu D, Wang H e Wang Y. (2006: 854)

O diagrama apresentado explica em alto nível o funcionamento da aplicação “padrão” que é um protótipo para combate do Branqueamento de Capitais e do Financiamento do Terrorismo, extraído de um artigo publicado pela Universidade de Hong Kong, pelo que esta informação é pública e está disponível *online*. Como poderá constatar a informação é recolhida em tempo real por *Collecting agents* e é posteriormente analisada de forma a detetar padrões e criar perfis levando a um diagnóstico que é então enviado ao operador. A informação recolhida é proveniente de duas fontes: interna - outros sistemas financeiros) e externa - informação que está disponível *online*.

Estes sistemas usam padrões previamente carregados para utilizarem como termo de comparação e quando detetam um novo podem adicionar o mesmo à sua base de dados.

Ao estudar o funcionamento destes sistemas concluí que poderiam ser melhorados de forma relativamente simples:

- À semelhança do que já é feito, por exemplo, com diversas *appliances* de segurança (como *firewalls*, UTMs, etc) estes sistemas poderiam comunicar constantemente com uma base de dados geral (do fabricante?) e eventualmente uns com os outros. Desta forma, seria possível a partilha rápida e fácil de informação. Por exemplo, sempre que um sistema detetasse uma nova “ameaça” (leia-se tentativa de BC) enviava o padrão/ perfil criado, de imediato para todos os outros sistemas e para a base de dados geral. Assim, numa questão de alguns minutos/ horas, todos os outros sistemas estariam já “informados” da existência do problema e preparados para o resolver. Exemplos: Sophos UTM, HP Aruba, Checkpoint, etc

Até que ponto acha que isto poderia ter implicações a nível de segurança? Como seria possível proteger um sistema destes, tendo em conta a implementação desta funcionalidade (que implicaria comunicação com outros sistemas, externos à rede da instituição, e com a referida “base de dados geral”)?

4.1.1.1. Conhecimento sobre as Aplicações Financeiras do Banco de Portugal para combater o Branqueamento de Capitais e Financiamento do Terrorismo

O entrevistado não conhece as aplicações financeiras usadas pelo BdP, mas sabe que o BdP faz o controlo do combate do BC/FT e que o fazem através de meios informáticos, contudo o entrevistado não tem conhecimento sobre estes tipos de ferramentas.

Segundo o entrevistado, as análises do BC/FT podem ser melhoradas de 2 maneiras:

- Reconhecer um padrão de transação financeira malicioso, em que sabemos que uma pessoa faz uma transferência uma para um lado outra para outra, se virmos este padrão de mensagens, então isto pode levantar um alarme, e alguém tem que olhar isto e ver se aquilo

realmente tem justificação. Isto só permite detetar padrões de fraude já conhecidos antes;

- Outra abordagem, mais contemporânea, está relacionada com a aprendizagem, que consiste em tentar aprender o que é o normal e depois por desvio estatístico perceber o que são anomalias. Perceber o que é que é normal acontecer, e quando há alguma coisa que está fora do padrão da normalidade é necessário defini-lo matematicamente. Sendo possível dizer que existe qualquer coisa diferente do habitual que pode ser justificada por qualquer coisa que aconteceu para justificar aquilo, podendo ser um falso alarme, como outra coisa que merece ser investigada. Tratam-se de duas abordagens genericamente expostas.

O entrevistado acrescentou ainda que não sabe em concreto que abordagem é que o BdP segue.

4.1.1.2. Funcionamento de Sistema Inteligente de BC

Este ponto vai ao encontro do anterior, pois trata-se de um sistema de combate ao BC/FT. Segundo o entrevistado, o diagrama apresentado trata-se da arquitetura do sistema e observa-se a interação entre os módulos, acrescenta ainda que estes esquemas são muito importantes para perceber o fluxo de informação, qual a sua origem e como é que é processada.

Estas duas fontes de informação são relevantes, temos os sistemas financeiros, por exemplo o sistema bancário, e o *www* representa outros dados públicos.

Vamos supor que existiam estes sistemas a funcionar e que havia entre as agências que os estão a utilizar a partilha de informações entre elas. Esta ideia existe já em algumas áreas, e é definida como *threats sharing*, que é a partilha das ameaças, é a partilha da forma de detetar o problema.

Uma melhoria a estes sistemas e de acordo com a ideia do Sistema Nacional de Cibersegurança é criar um sistema cooperativo e receber a informação que estas coisas estão a acontecer, funcionaria como um facilitador de informação, não ao nível de um padrão técnico, mas de modo a pôr as entidades a falarem umas com as outras, por exemplo o Banco de Portugal com o Banco de Espanha.

Na visão do entrevistado é muito otimista achar que a deteção permite logo criar um padrão e que esse padrão pode ser instalado noutro sem uma validação mais demorosa. Neste tipo de sistemas as pessoas são cautelosas, estão sempre disponíveis para receber informação do exterior, mas partilhar só quando estão seguros que não estão a partilhar erros ou outras coisas, receber informações de fora é fácil, partilhar coisas internas é mais difícil. Estas partilhas podem gerar muito ruido na comunicação: muitos falsos padrões e não terem disponibilidade de pessoal para verificarem todos os padrões.

O entrevistado acha que como principio, é para lá que estão a convergir muito dos sistemas de partilha de informação de segurança, contudo há um custo de comunidade e beneficio também em detetar os problemas, saber descreve-los de forma rigorosa, saber como podem ser reproduzidos, e vistos em ação, e partilhar essa informação com os nossos congéneres, e esperar que eles façam alguma coisa

com isso. É na direção deste tipo de processos que se deve caminhar, não sabe se será muito imediato lá chegar, mas é uma proposta perfeitamente válida e útil. Contudo, vai ter que haver sempre uma relação pessoal, o entrevistado não acredita para breve num sistema automático em que isto aconteça, definição de regras automáticas vindas do exterior é sempre algo de desconfiar, pode ser um ataque, alguém pode pôr uma regra: “isto não tem problema nenhum”.

Segundo o entrevistado, a tendência é descrever os problemas de maneira a que qualquer pessoa consiga entender, e deverá ser de forma logica, num formato pré-definido, com um determinado formulário, preenchido o que se observa, qual o padrão, quem participa, e que essa descrição depois possa mais facilmente ser entendida sem ambiguidade pelos congéneres, e que eles depois possam dentro do seu ciclo de decisão incorporar essas regras. No futuro podem existir maquinas que façam isto, mas é sempre necessária uma supervisão humana de validação que aquilo está a fazer sentido. Na opinião do entrevistado, neste caso, seria mais benéfico existir formato de dados comuns, um entendimento comum de como se descrem as coisas, e depois procedimentos internos de cada organização, como pega nessa informação que recebem que é fresca e como é que a podem aplicar no seu próprio sistema, passando pelos vários níveis de aprovação.

4.1.2. Categoria II - Metodologia para proteção de aplicações financeira

Esta categoria tem como objetivo perceber como é feita a proteção de uma aplicação financeira olhando para o caso em concreto do sector bancário, no caso dos ataques do *NotPetya* e do *WannaCry* se o indicado anteriormente teria sido suficiente para impedir esses ataques, se as formas de proteção atuais podem manter-se aptas no futuro, qual a posição a “tomar” entre Estabilidade Vs Atualizações/Segurança dos Sistemas Operativos, qual o envolvimento do Centro Nacional de Cibersegurança neste tipo de aplicações financeiras.

Para se alcançar estas informações, elaboraram-se as seguintes questões:

1. Tendo em conta a sua área de estudo em segurança informática em redes e sistemas, na sua opinião como se deve proteger uma aplicação financeira deste género, de ataques exogéneos?
2. No caso dos ataques *NotPetya* e do *WannaCry*, que causaram danos a nível mundial e de forma transversal, afetando setores como a banca, a saúde, os operadores de serviços de comunicações, entre outros. Acha que o que me indicou anteriormente teria sido suficiente para prevenir a situação? O que falhou?
3. Por norma, os sistemas operativos do setor bancário estão desatualizados em relação às inovações tecnológicas existentes no mercado e adotadas por diversas empresas. O motivo por trás disto é a manutenção da estabilidade dos sistemas utilizados. Assim, na sua opinião qual deveria ser a decisão a tomar? Dar prioridade à estabilidade em detrimento de atualizações dos sistemas operativos (que podem eventualmente implementar mais

mecanismos de segurança e *patches*, entre outros)? Ou vice-versa? Impasse: Estabilidade VS Atualizações/ Segurança; Será possível haver a simbiose entre estes dois termos?

4. Tendo em conta as soluções oferecidas pelo mercado para proteger as aplicações financeiras, acha que estas podem continuar a estar adequadas/atualizadas no futuro tendo em conta a velocidade da evolução constante dos sistemas e redes?
5. Tem conhecimento se os órgãos como o centro nacional de cibersegurança estão envolvidos neste tipo de aplicações financeiras? Se sim, como?

4.1.2.1. Mecanismo de proteção de aplicações financeiras de ataques exogéneos

O entrevistado afirma que a componente de rede é muito importante, os sistemas não devem ser acessíveis diretamente do exterior a partir da internet da rede pública, não devia ser possível eu estar aqui no IST e conseguir ligar-me à rede do BdP e conseguir chegar à máquina ou maquinas onde estão a correr esses sistemas. Se isto for sequer possível, é uma fonte de preocupação ainda que esses sistemas tenham palavra-passe e controlo de acessos. A melhor maneira de impedir o acesso a esses sistemas é através da segmentação da rede: rede do banco e a rede pública que é a rede internet. Não tem de haver só uma defesa, podem haver várias muralhas que dificultam muito o acesso.

Portanto a principalmente preocupação deve ser a proteção das redes informáticas, impedir o acesso ou dificulta-lo bastante. Normalmente isto é feito através das chamadas f*irewalls*, são as defesas, portas corta-fogo, que é algo que separa o fora do dentro, impede que tentativas de acesso do exterior não possam passar. Na visão do entrevistado, esta é a principal forma de proteção de aplicações, neste caso de aplicações financeiras.

4.1.2.2. Aplicabilidade do indicado anteriormente na prevenção do caso dos ataques *NotPetya* e *Wanna Cry*

Segundo o entrevistado, se tivesse sido impossível chegar às máquinas o indicado anteriormente sim teria sido suficiente para impedir os ataques, pois mesmo que viesse um vírus contaminar, se não chegar à máquina não a vai contaminar. Muitas vezes estes vírus exploram canais legítimos, entram, contaminam uma máquina e essa outra máquina contamina outras, não é uma contaminação direta do exterior, mas sim uma contaminação em epidemia, que vai passando de umas máquinas para as outras.

O entrevistado acrescentou ainda que no ataque *WannaCry,* o sistema operativo Windows tinha uma vulnerabilidade, um erro na programação, e alguém usou esse erro para conseguir escrever nos ficheiros da máquina de modo a cifrar esses ficheiros e fazendo chantagem de pagamento em troca de desbloquear os ficheiros. Os atacantes bloqueiam os ficheiros para impedir o acesso das pessoas, o Reino Unido foi especialmente afetado em especial o seu sistema de saúde, por exemplo: não era

possível dar entrada no sistema do hospital utentes porque as máquinas estavam todas paradas. Os computadores não eram atualizados à muitos anos e tinham a vulnerabilidade e ninguém corrigiu e aquilo foi passando de uns para os outros.

Ambos os ataques são *ransomware*, ou seja, são um *software* nocivo que impede o acesso ao sistema infetado e pede um resgate para que o acesso seja restabelecido, caso o mesmo não ocorra, os arquivos podem ser perdidos ou publicados. Este *software* é considerado o *malware* mais rentável da história.

4.1.2.3. Estabilidade VS Atualizações/ Segurança dos sistemas operativos

Segundo a visão do entrevistado, podemos ter problemas de duas abordagens:

- Temos um computador a funcionar e o seu sistema também, que é o desejável. Podemos ter a tentação de não fazer nada, ou seja, manter como está, de acordo com o princípio, se funciona não se mexe. Qualquer alteração na área da informática num pormenor pode causar o efeito cascata porque bloqueia o programa, pode não parecer nada, mas pode ser o suficiente para parar o programa todo. Deste modo, para aplicação continuar como estava a funcionar, deve-se manter a estabilidade. Contudo todos os sistemas operativos comerciais são enormes e possuem milhões de linhas de código, pelo que a probabilidade desse código ter erros é de 1%. Existem defeitos que não se manifestam, porque ninguém tenta fazer uma coisa errada, os atacantes testam por coisas que as pessoas não tentam ou experimentam, por exemplo: uma pessoa quando escreve um *urser name* com 100 letras, o programa não está preparado para este excesso de letras pelo que pode provocar uma corrupção do sistema e ele deixa o atacante entrar sem haver conhecimento sobre a *password*. Quem souber que existe um erro no código pode usar isto para explorar a vulnerabilidade e entrar no sistema, quem está a tentar entrar só tem que tentar entrar por uma maneira e quem está a defender tem que tapar os buracos todos que surjam. Conclusão: a probabilidade de qualquer sistema operativos ter defeitos é probabilisticamente certa, todos os sistemas têm defeitos. Quer os defensores quer os atacantes não sabem onde eles estão, os defensores assim que souberem têm que tapar os ataques todos, os atacantes se encontrarem um que ninguém sabe podem usar para fazer o seu ataque, e um ataque muito dirigido pode ser difícil parar, podendo se ter vulnerabilidades de zero dias, defeito que existe, que é pouco conhecido ou conhecido por poucas pessoas e que é usado para atacar o sistema.
- Deixar parado o sistema operativo parado é uma má solução, com o passar do tempo vão se descobrindo vulnerabilidades e o atacante tem mais pontos de ataque. Ao estarmos sempre atualizar, estamos a estragar o nosso programa, corro o risco de estar a tapar uma coisa que estava a contar que esteja lá.

  Nestes casos, aconselha-se a ter um ambiente de produção do sistema, um ambiente de pré-produção, com uma máquina virtualmente idêntica da produção mas que está a trabalhar com

dados simulados. Ou seja, eu tenho um computador principal e eu tenho uma cópia desse computador, que em vez de estar a trabalhar com dados reais, está a trabalhar com dados de há 2 anos por exemplo, mas que está a testar o meu *software* com as mesmas versões. Noutro ambiente de testes, um ambiente de desenvolvimento onde os programadores mexem, quando o código passa, o código passa para o ambiente de testes, caso passe estes testes, se passar passa para pré-produção e para produção, se não passar volta para trás.
Sempre que existirem *updates* deve-se seguir um caminho idêntico, devo seguir o caminho até aos sistemas de pré-produção, vou verificando se o sistema não deixa de funcionar, 1/2/3 dias, ou talvez um dia, caso o processamento seja diário, pode ser suficientes para perceber que não ocorreu nenhum problema.

Para os fabricantes é um grande custo ter de suportar as versões antigas do Windows, a 1ª versão do Windows XP saiu em 2001, 17 anos depois não têm interesse nenhum em manter isto ativo, pois precisam de alocar os seus recursos noutras versões, pelo que eles tentam que as pessoas avancem para as versões seguintes.

Segundo o entrevistado, deve existir um equilíbrio, nem estar na crista da onda a apanhar as últimas versões dos erros que todas a gente vai ter e nem estar na década passada com os buracos todos que já toda a gente conhece.

4.1.2.4. Adaptabilidade no futuro dos mecanismos de proteção de aplicações financeiras de ataques exogéneos existente atualmente no mercado

Segundo o entrevistado, as proteções de rede vão se manter, têm é que sofrer atualizações. O princípio é o mesmo e é estável, existem *firewalls* à 20/30 anos e o que se está a fazer agora é o mesmo, a diferença é que agora se está a fazer de maneira mais rápida, porque a internet também passa mais informação, existe maior largura de banda, processa mais dados, mas o principio das redes e do isolamento mantem-se, podemos ter que acompanhar a evolução dos sistemas operativos e das redes e ir atualizando o *hardware* que está a fazer isso para que ele tenha o desempenho que estamos à espera. Esta abordagem é independente do sistema que estamos a atualizar, e mantem-se adequada.

Uma coisa que mudou isto nos últimos anos, são as redes internas que só eram acedidas por máquinas internas, mas hoje cada vez mais as pessoas utilizam o seu telemóvel ou *Tablet* que tem uma ligação à internet que não passa pela *firewall* da organização. Esta utilização é insegura, e o ataque pode vir não da rede, pela porta principal, mas pelo dispositivo móvel. Como os dispositivos são cada vez mais pequenos, merecem uma revista melhor e é necessário ter em atenção isto.

4.1.2.5. Envolvimento do Centro Nacional de Cibersegurança em aplicações financeiras

O entrevistador não tem conhecimento sobre o envolvimento do Centro Nacional de Cibersegurança em aplicações financeiras, mas sabe que existem requisitos a nível europeu dos setores críticos da economia, como o tráfico aéreo, os transportes, a eletricidade, a água, e talvez o sector financeiro, que têm que reportar problemas ao Centro Nacional de Cibersegurança. O entrevistador acha que eles devem ter o mínimo conhecimento, mas não sabe se eles participam na questão de normas, entre outros assuntos relacionados.

4.2. Proposta de Sistema Inteligente Anti-Branqueamento de Capitais

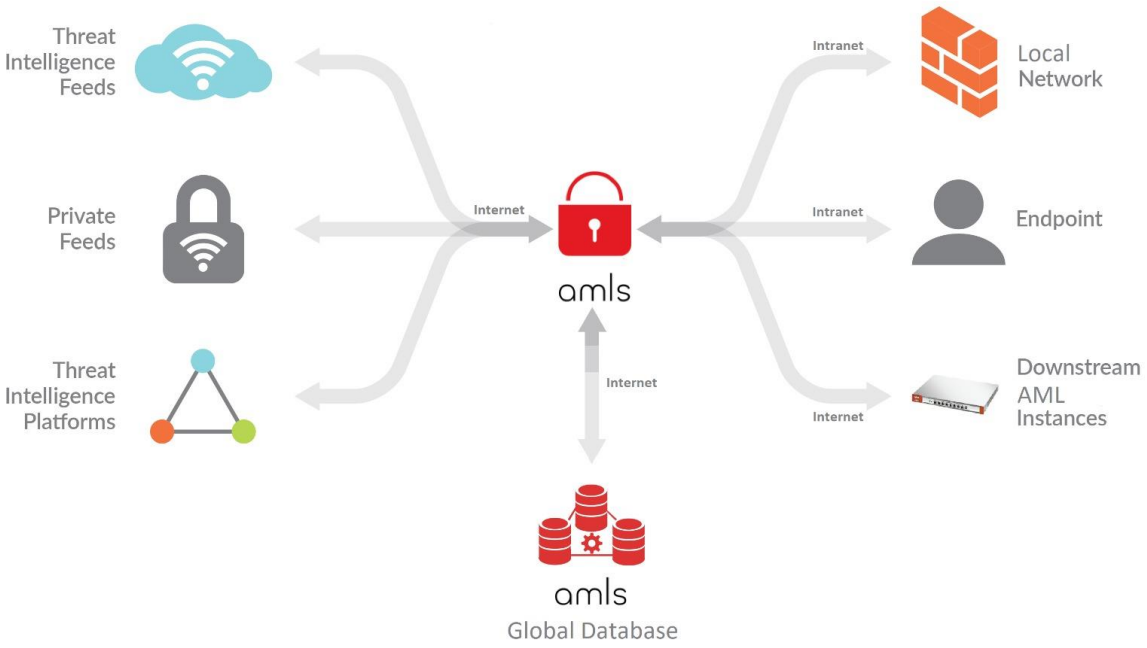
Neste ponto apresenta-se uma proposta de um Sistema Inteligente Anti-Branqueamento de Capitais, baseado num protótipo feito pela Universidade de Hong Kong e nos dados obtidos na entrevista realizada ao Prof. Dr. Miguel Pardal, que já foram descritos no ponto 4.1. do presente capítulo.

O Prof. Dr. Miguel Pardal afirmou que em algumas áreas existem sistemas que partilham informações entre si, chamados *threat sharing systems*, que partilham ameaças e formas de as detetar. Tendo em conta essa informação, proponho um modelo que acredito ser mais fiável na deteção de tentativas de BC.

4.2.1. Estrutura e componentes do Sistema Inteligente

Tendo em conta a estrutura do Sistema Inteligente Anti-Branqueamento de Capitais e Financiamento do Terrorismo apresentado no ponto 2.12.2.1. - Sistema Inteligente Anti-Branqueamento de Capitais, é apresentado na Figura 4 um diagrama de alto nível do sistema que proponho: *Anti-Money Laundering System* (daqui em diante designado apenas por *amls*), em português “sistema anti-branqueamento de capitais”.

Figura 4 - Diagrama de alto nível do Sistema amls



Fonte: Elaboração Própria

O *amls* é uma *appliance*, ou seja, é um dispositivo de *hardware* com *software* integrado e projetado especificamente para fornecer um recurso de computação específico, neste caso, deteção e comunicação de padrões associados a atos de BC/FT.

Este sistema troca informação, via internet, com os seguintes:

- *Threat Intelligence Feeds* – Fontes/fluxos de informação de ameaças
- *Private Feeds* – Fontes/fluxos de informação privados
- *Threat Intelligence Platforms* – Plataformas com informação de ameaças
- *Local Network* – Rede local
- *Downstream AML Instances* - Outras instâncias de *AMLS*
- *Endpoint* - Operador/Utilizador Humano
- *Amls Global Database* – Base de Dados Global da Empresa *AMLS*

O *amls* tem por base o protótipo apresentado no 2.12.2.1 do Capitulo 2, onde foram referidos os seguintes “agentes inteligentes”:

- *Data Collecting Agent* (Agente “Coletor” de dados)
    - *Internal Data Collecting Agent* (Agente “Coletor” de Dados Internos)
    - *External Data Collecting Agent* (Agente “Coletor” de Dados Externos)

- *Monitoring Agent* (Agente Monitor)
    - *Client Profile Monitoring Agent* (Agente Monitor de Perfis de Clientes)
    - *Transaction Monitoring Agent* (Agente Monitor de Transações)
- *Behavior Diagnosing Agent* (Agente que faz Diagnóstico Comportamental)
- *Reporting Agent* (Agente que Reporta)
- *User Agent* (Agente Utilizador)

4.2.2. Funcionamento do Sistema Inteligente

No caso do *amls*, o *Internal Data Collecting Agent* adquire/agrega dados provenientes da *Local Network* (rede local/interna) e do *endpoint* (operador/utilizador), enquanto os *External Data Collecting Agent* adquirem dados provenientes das restantes fontes representadas na figura 4, nomeadamente *Threat Intelligence Feeds*, *Private Feeds*, *Threat Intelligence Platforms*, *amls Global Database* e *Downstream amls Instances* (ou seja, outras Instâncias de *amls*).

Os dados agregados pelos *Data Collecting Agents* vão ser analisados pelos *Monitoring Agents*.

O *Client Profile Monitoring Agent* e o *Transaction Monitoring Agent* têm a função de monitorizar possíveis esquemas de BC numa base de "cliente-para-cliente" (KYC) e de "transação-para-transação" (KYT).

O *Client Profile Monitoring Agent* avalia um conjunto de informações detalhadas relacionadas com a conta do cliente, fornecendo uma visão única do perfil do cliente, incorporando todos as relações financeiras com as quais a conta tem uma afiliação.

O *Transaction Monitoring Agent* identifica transações que apresentam maior risco de possíveis atividades de BC, sendo que as transação classificadas como de maior risco podem variar de organização para organização com base nas suas linhas e tipos de negócios.

Quando um perfil de cliente for questionável ou for detetada uma transação fora do comum pelos *Monitoring Agents*, é emitido e enviado um relatório de risco para o *Behavior Diagnosing Agent,* para se proceder a uma investigação mais aprofundada. O *Behavior Diagnosing Agent* ao receber os relatórios de risco dos *Monitoring Agents* inicia o seu processo de diagnóstico para investigar o comportamento complexo que é usualmente associado a esquemas de BC. Analisa os relatórios de risco dos *Monitoring Agents* e solicita qualquer informação adicional, se necessário, para examinar os casos.

Quando o *Behavior Diagnosing Agent* identifica um comportamento fora do comum ou suspeito, é automaticamente produzido e enviado um Relatório de Atividades Suspeitas (RAS) para o *Reporting Agent*.

O Reporting Agent apresenta e comunica possível alerta de BC ao operador/utilizador, por meio do *User Agent.* Este agente é responsável por garantir que o responsável do possível caso de BC tem todas as informações relevantes do cliente disponíveis.

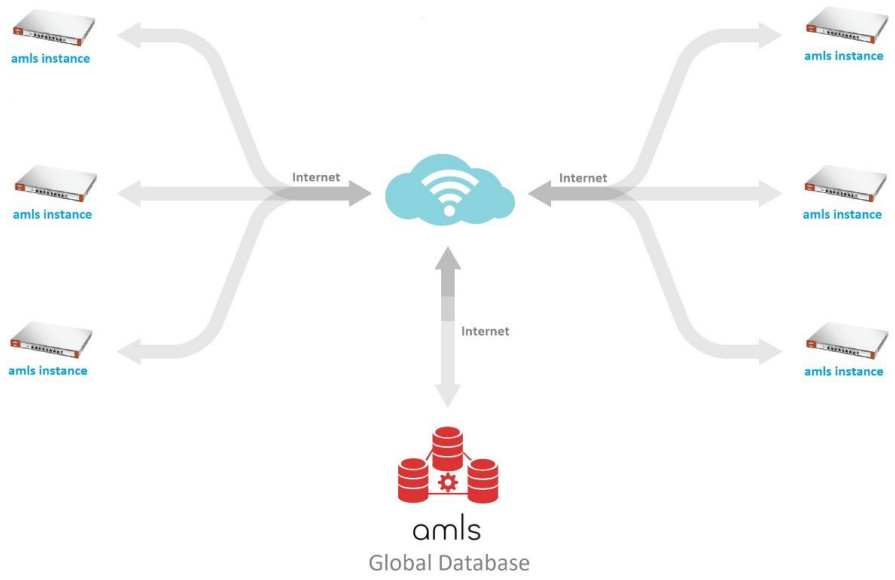
Simultaneamente ao envio do RAS, o *amls* envia também o padrão detetado para a *Global Database* e para todas as outras Instâncias de *amls* (noutras instituições financeiras), a que está conectado, via internet. Desta forma, para além da informação que cada *appliance* tem à partida na sua base de dados interna, está constantemente a receber atualizações, o que permite ao sistema detetar ameaças mais rapidamente.

Em pouco tempo (numa questão de minutos ou horas) todos os *amls* conseguem ter a mesma informação relativa a novas ameaças que foram detetadas noutro continente (por exemplo), seja através da ligação a outras instâncias ou através da *Global Database*. Na Figura 5 é apresentado um diagrama mais detalhado destas interações.

Para além disso, conseguem também receber informação de *Feeds* e plataformas *online* dedicadas a este tipo de atividade, bem como da sua rede interna e inputs manuais dos operadores do sistema.

Este tipo de partilha de informação que proponho (principalmente no que diz respeito à comunicação constante com outras instâncias do sistema e com uma base de dados global) já é feita em vários sistemas UTM (*Unified Threat Manager*), *Firewalls*, *softwares* de gestão de infraestruturas (de *Bladecenters* como o HP OneView), entre outros.

Figura 5 - Diagrama de Comunicação que ilustra os Downstream AML Instances, que se decompõem em várias amls Instances, em que cada uma delas pertence a uma empresa/entidade que se dedica ao combate do BC e FT

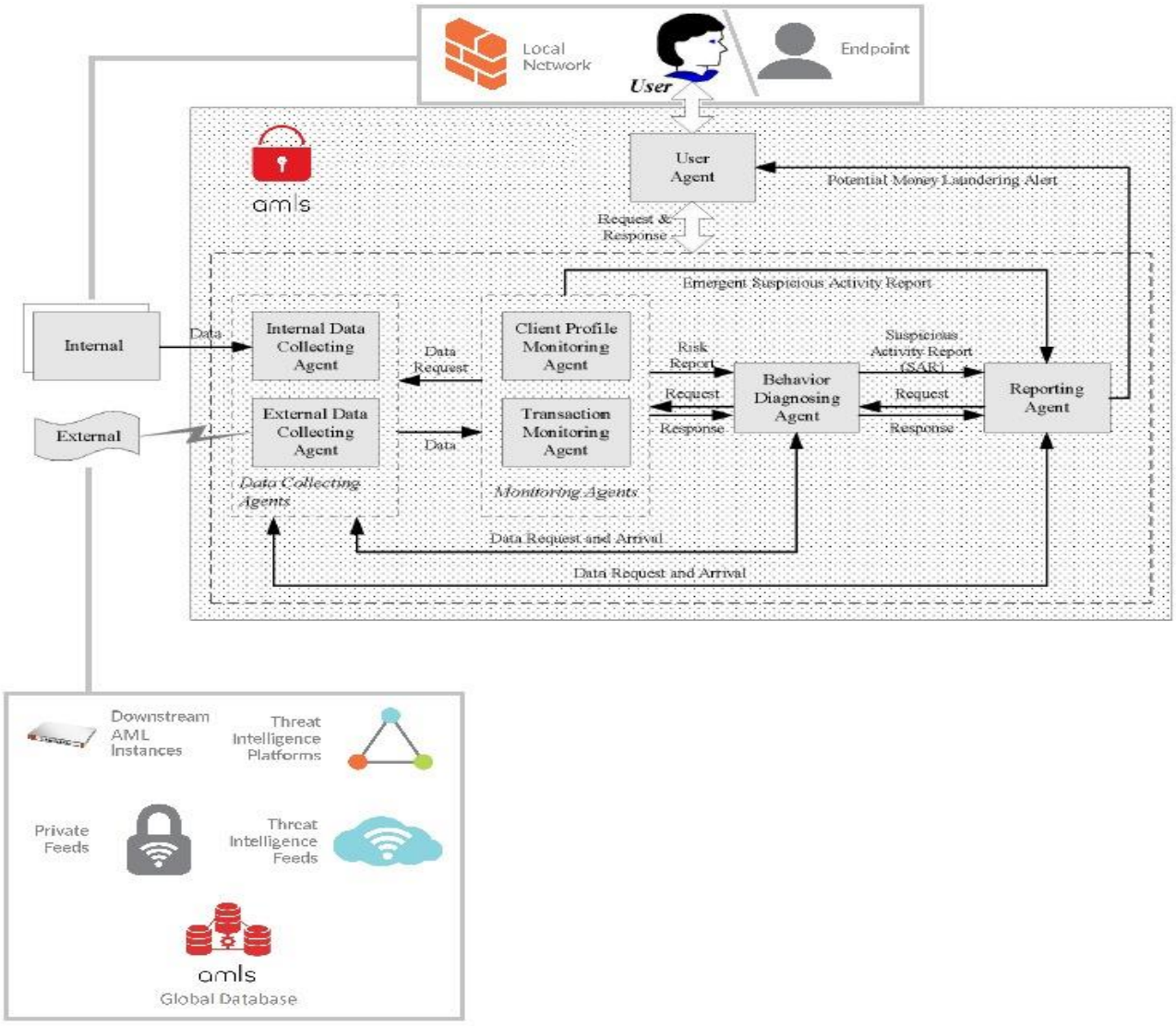


Fonte: Elaboração Própria

A visão geral do *amls*, integrada com o protótipo da Universidade Hong Kong - Sistema Inteligente Anti-Branqueamento de Capitais do ponto 2.12.2.1., que lhe serve de base, está representada no diagrama da Figura 6.

Segundo o Prof. Dr. Miguel Pardal, estes tipo de diagrama é muito importante, para se perceber o fluxo de informação, qual a sua origem e como é que é processada.

Figura 6 - Visão geral do amls



Fonte: Elaboração Própria

4.2.3. Proteção de uma *appliance amls*

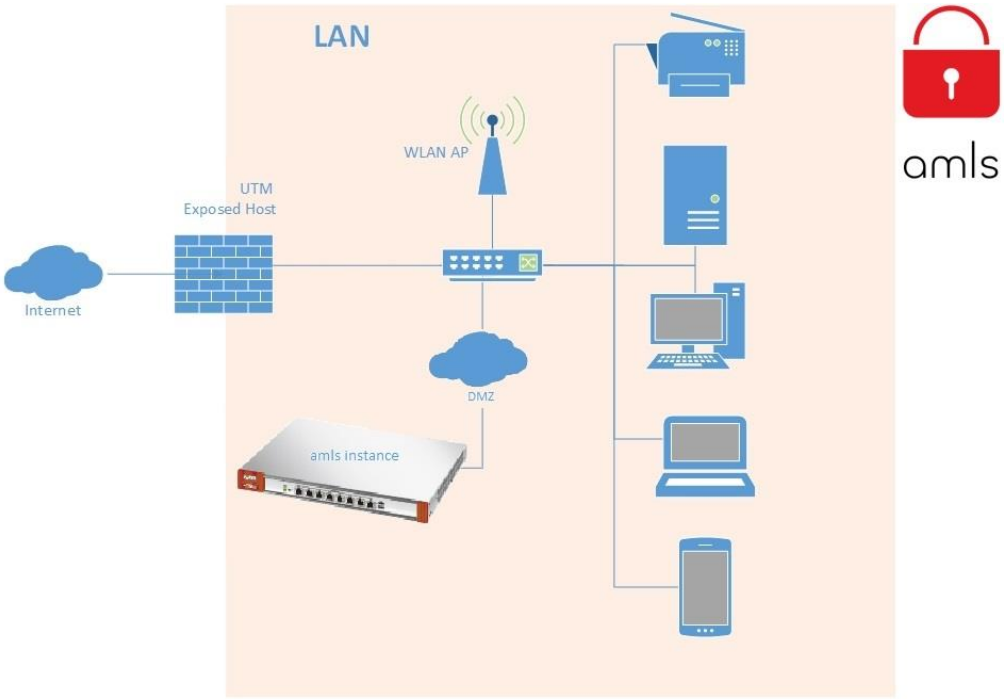
De acordo com o Prof. Dr. Miguel Pardal, a proteção deste tipo de sistemas é de máxima importância, e, obviamente, não devem estar acessíveis diretamente do exterior (da internet), ainda que tenham palavra-passe e controlo de acessos.

Para controlar/prevenir acessos do exterior, protegendo assim o sistema, é comum recorrer-se a *Firewalls*. *Firewalls* são sistemas de segurança de rede, que monitorizam e controlam o tráfego da rede tanto de fora para dentro como de dentro para fora. São baseadas sobretudo na aplicação de regras pré-determinadas e são, na visão do entrevistado, a principal forma de proteção de aplicações financeiras.

Segundo o Prof. Dr. Miguel Pardal, as *Firewalls* irão manter-se como sistemas primários de proteção de redes, tendo, no entanto, que sofrer atualizações regulares, de modo a acompanhar a evolução das ameaças.

Na figura 7, é apresentado um diagrama de rede, que ilustra a proteção de uma *appliance amls*:

Figura 7 - Diagrama de proteção de uma appliance amls



Fonte: Elaboração Própria

De modo a controlar acessos externos (da Internet) ao sistema, é utilizada uma UTM. Uma UTM é também uma *appliance* que inclui *Firewall* e que opcionalmente poderá também incluir uma série de outros sistemas como antivírus, *web proxy*, entre outros. Há vários fabricantes que vendem este tipo de equipamentos, como por exemplo (Sophos, Palo Alto e Checkpoint).

A *Firewall* na UTM controla o acesso à rede, através de regras pré-definidas que por sua vez vão reencaminhar os pedidos (vindos do exterior) de acesso à instância local de *amls* para uma DMZ (*Demilitarized Zone*), passando antes por um *switch* que por sua vez "distribui rede" pelos recursos necessários (impressoras, computadores, APs, etc).

Uma DMZ é uma sub-rede que contem e expõe recursos que devem ter contacto com o exterior, como é o caso da *appliance* do *amls*.

À parte do que está representado no diagrama seria também conveniente a utilização de *backup* em dois tipos de media diferentes e a utilização de sistemas geo-redundantes do tipo ativo-ativo.

Finalmente, de forma a garantir maior proteção dos sistemas, as comunicações entre as várias instâncias de *amls* e entre cada instância e a *Global Database*, deveriam ser efetuadas através de VPNs IPSec, configuradas ponto-a-ponto.

4.2.4. Desvantagens e Vantagens do *amls*, face aos sistemas atualmente existentes

Desvantagens:

- Resistência inicial à mudança por parte de algumas instituições financeiras (uma vez que o *amls* estaria constantemente a comunicar com o exterior);
- Necessidade de maior proteção do sistema que pode eventualmente levar a maior custo de implementação;

Vantagens:

- Sistemas melhor preparados para resolver tentativas de ameaça de BC, pois a informação difunde-se mais rapidamente e os sistemas numa questão de alguns minutos/horas tem acesso a dados extremamente relevantes.

A inovação é uma grande tendência que "veio para ficar" quer a nível setorial quer em termos globais. "O fato de se estar perante um fenômeno de globalização é indiscutível e esse fator tem consequências diretas nas economias nacionais e regionais também. A questão centra-se nas consequências dessa globalização e em como responder a esse desafio." (Costa, 2014: 31). Sabemos ainda que, em algumas geografias do Mundo a pressão na dinâmica da inovação vai aumentar. Por exemplo na América Latina onde os conflitos e a informalidade económica estão a aumentar essa pressão de dinâmica é cada vez maior.

É necessário que a sociedade se envolva e que percecione os resultados obtidos no âmbito da tecnologia de forma a dar sustento e apoio à mesma. Para que a tecnologia faça parte da vida das pessoas, é necessário que esteja presente no seu dia-a-dia/quotidiano por meio de bens ou serviços melhorados e diversificados e que sejam testados pela sociedade. Após a aceitação por parte da sociedade é necessário que se direcione o investimento, que este responda às expectativas e que aposte na internacionalização. (Costa, 2014: 31 e 32) "A internacionalização por meio de parcerias talvez seja o modo mais flexível e com menos custos para a sociedade em geral de adquirir e projetar conhecimentos, acedendo sem barreiras a mercados que lhe estariam vedados por convenções internacionais." (Costa, 2014: 33). No caso das empresas, existe uma tendência para desempenhar as atividades de trabalho e negócios com base numa racionalidade "bounded" (Simon, 1959 e 1965), ou seja, é a capacidade limitada de usar informações e fazer escolhas económicas e tecnológicas."

(Castellaci et al., 2005: 5), e como tal, a inovação no nível organizacional requer que se desenvolva uma teoria microeconómica evolutiva da inovação com uma estreita interação e conexão com outras disciplinas fora do domínio económico, como psicologia cognitiva, negócios e estudos organizacionais (Castellaci et al., 2005: 39), sendo os setores das finanças e da distribuição apontados como pioneiros e usuários criativos no desenvolvimento de tecnologias.

Tendo em conta os fatores referidos nos dois parágrafos anteriores, juntamente com o facto da "resistência à mudança" ser uma condição praticamente universal no aparecimento de qualquer "nova tecnologia" e que, rapidamente é ultrapassada, começando as empresas e particulares a usar a dita "nova tecnologia", (A aprendizagem é uma atividade social que torna o processo inovador incerto, cumulativo e coletivo (Lazonick, 2004)), e o facto de se ter que olhar obrigatoriamente para os eventuais custos adicionais como um investimento (tendo em conta os benefícios de um sistema destes e a obrigatoriedade de ter em consideração os custos de manutenção de uma infraestrutura em *cloud*) acredito que o *amls* poderia trazer ao mercado uma vantagem enorme relativamente às soluções apresentadas atualmente pelos outros *players* no mercado.

Quanto mais promissora for uma determinada tecnologia em termos utilitários, mais considerada será pela sociedade. Esta noção prende-se com a ideia de que o conhecimento e técnicas tecnológicas permitem que a sociedade conceda valor público a essa mesma tecnologia (Costa, 2014: 29) e a prova de que este será o caminho a seguir, mais tarde ou mais cedo, é que este tipo de funcionalidades adicionais de comunicação e atualização em tempo real já está neste momento a ser adotada globalmente pelos maiores fabricantes de *hardware* e *software* na área de segurança e não só. É também esta a visão do Prof. Dr. Miguel Pardal, que acredita que é neste sentido que estão a convergir este tipo de sistemas.

5. Conclusão

O Banco de Portugal possui um papel importante na supervisão de Instituições Financeiras. Esse papel traduz-se em ser, de entre os supervisores financeiros, o mais proactivo na utilização de canais formais para promover a necessidade das IFs terem um modelo de supervisão ABC/CFT baseado no risco ajustado à realidade, utilizando para isso a emissão por escrito de orientações adicionais aos regulamentos de ABC/CFT, a organização de sessões de formação e seminários para o setor e a disponibilização de um endereço de correio eletrónico dedicado ao ABC/CFT.

O papel de supervisão abrange também as ferramentas/sistemas de informação utilizados pelas IFs. O BdP certifica-se de que as ferramentas consolidam registos relativos a relações de negócio, transações ocasionais, operações em geral, se tratam a informação em bases de dados de forma a atribuem diferentes classificações e perfis de acesso e se as bases de dados são atualizadas e integralmente acessíveis (artigo 9.º do Aviso do Banco de Portugal n.º 2/2018, de 26 de setembro).

Após análise das ferramentas mais utilizadas pelas IFs, conclui que se tratavam de sistemas pouco "inteligentes" e com várias lacunas, não existindo nenhum que reúna todas as características necessárias para colmatar as falhas encontradas.

Assim, propus nesta dissertação um sistema que, tendo por base a arquitetura e protótipo contruídos pela Universidade do Hong Kong e adicionando as funcionalidades que detalhei no ponto 4.2. do capítulo 4, me parece dar resposta às necessidades das IFs na sua ação de combate ao BC/FT.

No processo de investigação que efetuei para elaborar esta dissertação, deparei-me com algumas limitações que se devem ter em conta na elaboração de trabalhos futuros.

Destaco como limitações: a sensibilidade do tema Branqueamento de Capitais e Financiamento do Terrorismo, uma vez que as organizações não divulgam as suas técnicas e metodologias no combate a estes atos ilícitos, para além daquelas que são obrigas a comunicar, especificamente no que toca às ferramentas tecnológicas. Outra limitação encontrada foi o domínio e conhecimento do entrevistado sobre o tema, porque apesar do entrevistado ter correspondido ao perfil de amostra desejado, a metodologia qualitativa possui um caracter subjetivo, o que pode pôr em causa as conclusões alcançadas.

A presente investigação pode ser o ponto de partida para investigações futuras, sendo eventualmente necessário o aumento da dimensão da amostra e alarga-la a outras entidades envolvidas no combate no BC/FT. Outra possível abordagem para investigações futuras, seria a implementação do Sistema Inteligente proposto na presente dissertação.

Com a realização desta dissertação, em particular através da proposta efetuada para um novo Sistema Inteligente, faculta-se um *input* para repensar e redesenhar os Sistemas Inteligentes Anti-Branqueamento de capitais/Financiamento do Terrorismo, permitindo abrir horizontes para um novo caminho no sentido da sua prevenção.

Referencias Bibliográficas

Bae Systems. 2018. AML Regulatory Compliance. Disponível em: https://www.baesystems.com/en/capability/aml-compliance

Banco de Portugal. 2015. *Newsletter* Biblioteca. *O Banco de Portugal e a prevenção do branqueamento de capitais e do financiamento do terrorismo.* Disponível em: https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/2015_2_newsletter_abril2015_internet.pdf.

Banco de Portugal. 2018. Grupo de Acção Financeira (GAFI). Disponível em: https://www.bportugal.pt/page/grupo-de-accao-financeira-gafi?mlid=861

Banco de Portugal. 2015. Avaliação nacional de riscos de branqueamento de capitais e de financiamento do terrorismo. Disponível em: https://www.bportugal.pt/sites/default/files/anexos/gafi_doc_avaliacao_pt_0.pdf

Banco de Portugal. Lei nº 25/2008 de 5 de junho. Disponível em: https://www.bportugal.pt/sites/default/files/anexos/legislacoes/252808039_1.doc.pdf

BCFT. Pessoa Politicamente Exposta. Disponível em: http://portalbcft.pt/pt-pt/content/pessoa-politicamente-exposta

BCFT. Documentos Orientadores. Disponível em: http://www.portalbcft.pt/pt-pt/content/documentos-orientadores.

BIS. 2017. Sound management of risks related to money laundering and financing of terrorism. Disponível em: https://www.bis.org/bcbs/publ/d405.pdf

Braguês JL. *O Processo de Branqueamento de Capitais*. Vol 2009.; 2009.

Castellaci, F., Grodal, S., Mendonca, S., Wibe, M. (2005) “Advances and Challenges in Innovation Studies”, *Journal of Economic Issues*, 39 (1), pp. 91–121

Checkpoint. Cyber Security Management. Disponível em: https://www.checkpoint.com/products/cyber-security-management/.

Clear view kyc. 2018. Banks & Financial Institutions. Disponível em: http://www.clearkyc.net/Banking-Finance-Industry.html

Costa, C. M. (2014) “Internacionalização como contexto para novas políticas de ciência e tecnologia”, *Parcerias Estratégicas*, pp. 27 – 34

Costa, C.M. (2014), "A erosão do Estado na África Ocidental", Janus, pp. 68-69.

Costa, C.M. e L.A. Fretes (2018), “Different perspectives on changes and conflict in the transatlantic world”, *Portuguese Journal of Social Science*, Vol. 17, No. 2., pp. 125-129

Costa, C.M. e L.A. Fretes (2018), “Different perspectives on changes and conflict in the transatlantic world”, *Portuguese Journal of Social Science*, Vol. 17, No. 2., pp. 125-129

Demetis, D. S. 2010. *Technology and Anti-money Laundering: A Systems Theory and Risk-based Approach*. Cheltenham: Edward Elgar Publishing.

Diário da República, Decreto-Lei Nº 49/2009 de 12 de fevereiro

Diário da República, Lei Nº 25/2008 de 5 de junho

Diário da República, Portaria Nº 150/2004 de 13 de fevereiro

Diário da República, Decreto-Lei Nº 15/93 de 22 janeiro

Diário da República, Lei Nº 52/2003 de 22 de agosto

EBA. Orientações Conjuntas. Disponível em: https://esas-joint-committee.europa.eu/Publications/Guidelines/Joint%20Guidelines%20on%20risk-based%20supervision_EN%20%28ESAs%202016%2072%29.pdf.

Edição S, Schott PA. Guia de Referência Anti-Branqueamento de Capitais e de Combate ao Financiamento do Terrorismo.

ESMA. 2017. Esas warn on money laundering and terrorist financing risks affecting the eu financial sector. Disponível em: https://www.esma.europa.eu/press-news/esma-news/esas-warn-money-laundering-and-terrorist-financing-risks-affecting-eu-financial

EUR-Lex. Diretiva (UE) 2015/849 do parlamento europeu e do conselho de 20 de maio de 2015

Fachesf. 2012. O que você precisa saber sobre Pessoa Politicamente Exposta (PPE). Disponível em: http://www.fachesf.com.br/pdf/notafachesf/nota_fachesf_22_05_12_tira_duvidas_ppe.pdf

FATF (2012-2018), International Standards on Combating Money Laundering and the Financing of

Terrorism & Proliferation, FATF, Paris. Disponível em: www.fatf-gafi.org/recommendations.html

FATF. Money Laudering. Disponível em: http://www.fatf-gafi.org/faq/moneylaundering/.

FATF. What do we do. Disponível em: http://www.fatf-gafi.org/about/whatwedo/

FATF. Find a Country. Disponível em: http://www.fatf-gafi.org/countries/

FATF (2013), *FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22*), FATF, Paris. Disponível em: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

FATF (2015), *Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL),* FATF, Paris. Disponível em: http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf

FATF (2015), *Emerging Terrorist Financing Risks*, FATF, Paris. Disponível em: http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

FATF (2010), *Money Laundering through Money Remittance and Currency Exchange Providers.* FATF, Paris. Disponível em: http://www.fatf-gafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf

FATF (2017), *Anti-money laundering and counter-terrorist financing measures – Portugal*, Fourth Round Mutual Evaluation Report, FATF, Paris. Disponível em: http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Portugal-2017.pdf

Feedzai. Feedzai Anti-money Laundering System. Disponível em: https://feedzai.com/products/aml/.

Gao S, Xu D, Wang H, Wang Y. Intelligent anti-money laundering system. In: *2006 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI 2006*. ; 2006:851-856. doi:10.1109/SOLI.2006.235721.

Heidarinia N, Harounabadi A, Sadeghzadeh M. An Intelligent Anti-Money Laundering Method for Detecting Risky Users in the Banking Systems. *Int J Comput Appl*. 2014;97(22):975-8887.

HP aruba. Aruba Switches. Disponível em: https://www.arubanetworks.com/products/networking/switches/.

HP Enterprise. HP BladeSystem. Disponível em: https://www.hpe.com/us/en/integrated-systems/bladesystem.html.

HP Entreprise. HPE OneView. Disponível em: https://www.hpe.com/us/en/integrated-systems/software.html.

Institute for Economics and Peace (2015), *Global Terrorism Index 2015.* Disponível em: http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf.

Institute for Economics and Peace (2016), *Global Terrorism Index 2016.* Disponível em: http://economicsandpeace.org/wp-content/uploads/2016/11/Global-Terrorism-Index-2016.2.pdf.

Institute for Economics and Peace (2017), Global Terrorism Index 2017. Disponível em:

http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf.

Mendonça, S. (2010), "Mercúrio e Marte, SA: Serviços de segurança e defesa", *Janus*, pp. 42-43.

Mendonça, S. (2013), “O negócio da força em África: o nexo estabilidade-segurança”, *Janus,* pp. 78-79.

Mendonça, S. (2014), "O complexo industrial-militar", *Janus*, pp. 112-113.

Notre Dame Law School.1995. e Money Laundering Control Act of 1986: Creating a New Federal O ense or Merely A ording Federal Prosecutors an Alternative Means of Punishing Speci ed Unlawful Activity? Disponível em: https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1014&context=law_faculty_scholarship

Palo Alto. Next-Generation Firewalls. Disponível em: https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall.html.

Quivy, R. and Campenhoudt, L. (2008). *Manual de investigação em ciências sociais*. Lisboa: Gradiva.

Revista Visão. 2015. Baixo custo do financiamento do terrorismo. Disponível em: http://visao.sapo.pt/opiniao/silnciodafraude/2015-11-12-Baixo-custo-do-financiamento-do-terrorismo

SAS. SAS ANTI-MONEY LAUNDERING. Disponível em: https://www.sas.com/en_us/software/anti-money-laundering.html

Shu M, Rui L, Dancheng L, Shuaizhen Z. Anti-money-laundering system based on mainframe and SOA. In: *Proceedings - 5th International Conference on Computational Intelligence and Communication Networks, CICN 2013*. ; 2013:613-616. doi:10.1109/CICN.2013.134.

Serviço de Informação de Segurança. Contraterrorismo. Disponível em: https://www.sis.pt/ameacas/contra-terrorismo

Sophos. Sophos SG UMT. Disponível em: https://www.sophos.com/en-us/products/unified-threat-management.aspx.

Sousa, M. J. e Baptista C.S. 2011. *Como fazer investigação, dissertações, teses e relatórios*. Lisboa: Pactor.

Thomsonreuters. 2018. Anti-Money Laundering. Disponível em: https://risk.thomsonreuters.com/en/risk-solutions/aml-anti-money-laundering.html;

Tonbeller. 2018. The Leading Software for Money-Laundering Research and Monitoring. Disponível em: http://www.tonbeller.com/en/solutions/anti-money-laundering/anti-money-laundering-for-banks/

United Nations. 1999. International Convention for the Suppression of the Financing of Terrorism. Disponível em: http://www.un.org/law/cod/finterr.htm.

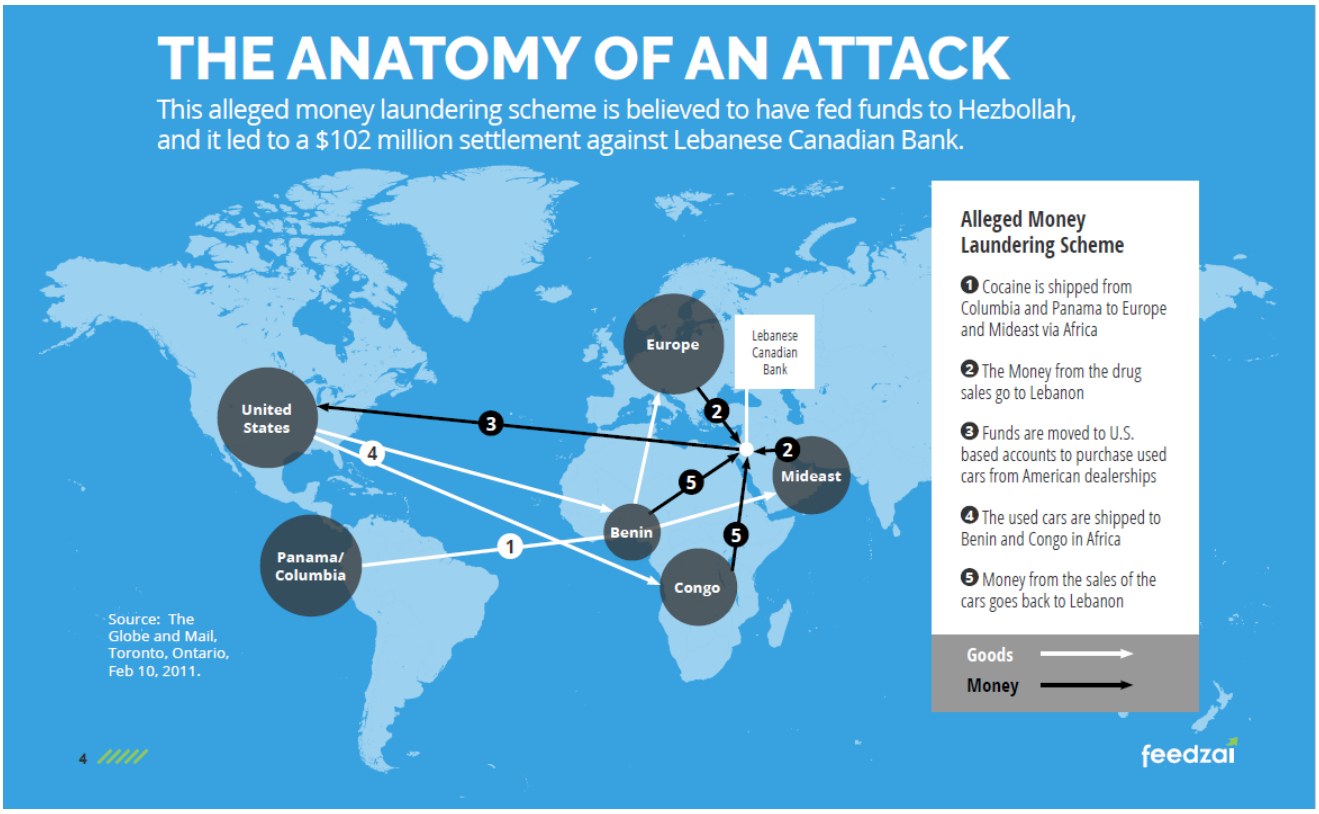
UNODC. 2018. goAML – UNODC's Software for Financial Intelligence Units. Disponível em: http://goaml.unodc.org.

Winn, J. (2000). *Catalytic impact of information technology on the new international financial architecture*.

Anexos

Anexo A – Anatomia de um ataque de BC

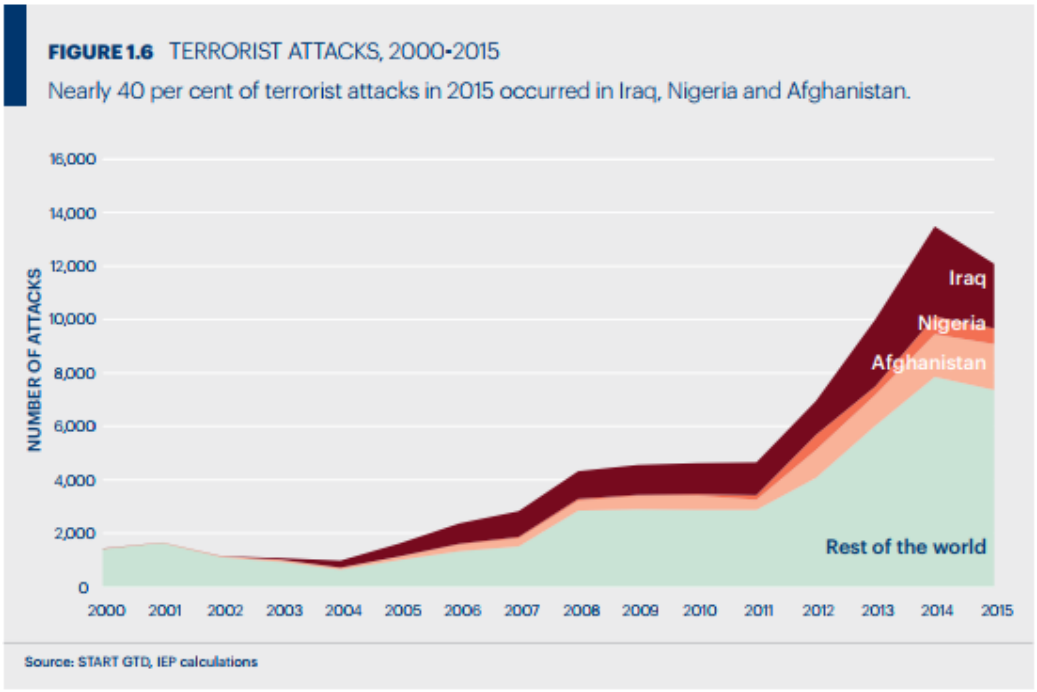
Figura 8 - Anatomia de um ataque de BC



Fonte: Site *institucional da* Feedzai – https://feedzai.com/resources/wp/augmenting-your-aml-with-ai/

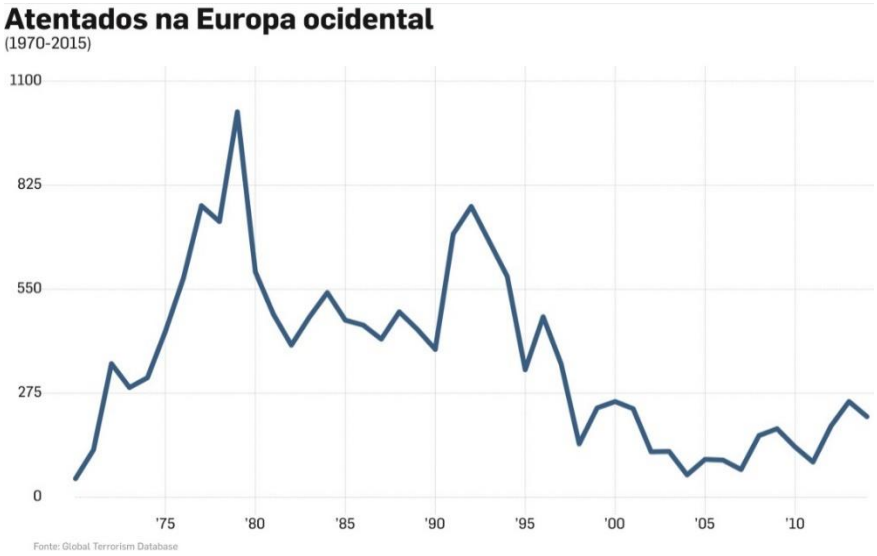
Anexo B – Ataques Terroristas no Mundo

Figura 9 - Ataques terroristas no Mundo entre 2000 e 2015



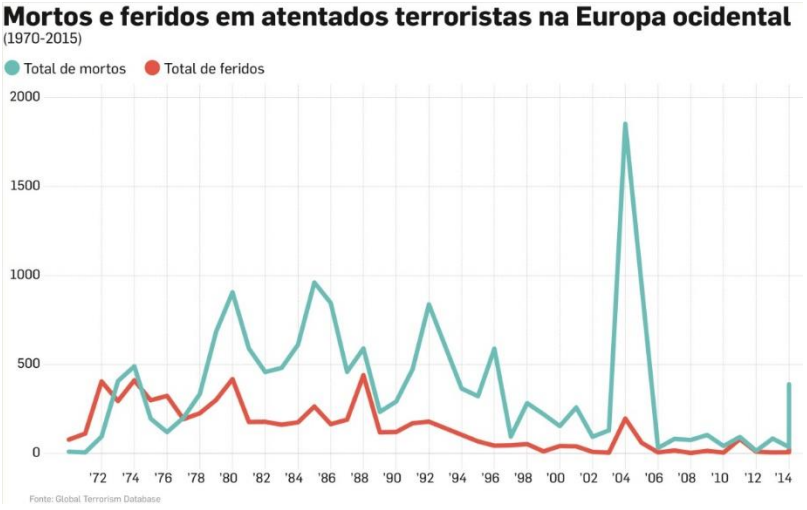
Fonte*: Global Terrorism Index 2016*

Figura 10 - Nº de ataques terroristas na Europa Ocidental entre 1970 e 2015



Fonte: *Global Terrorism Database*

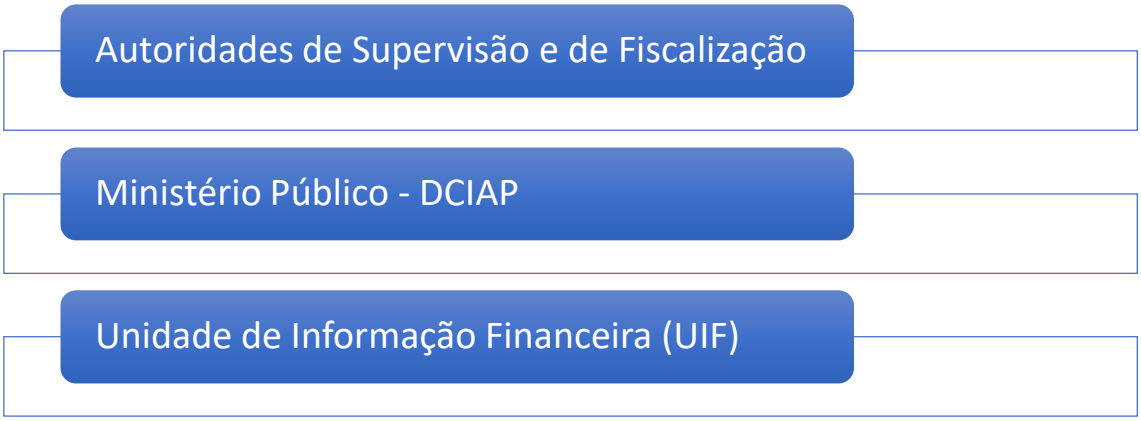
Figura 11 - Nº de mortos e feridos nos ataques terroristas na Europa Ocidental entre 1970 e 2015



Fonte: *Global Terrorism Database*

Anexo C – Processo de difusão de atos ilícitos de BC/FT entre entidades

Figura 12 - Processo de difusão de atos ilícitos de BC/FT entre entidades



Fonte: Elaboração Própria

Anexo D – Organograma do Banco de Portugal

Figura 13 - Organograma do Banco de Portugal

Fonte: *Site* Institucional do Banco de Portugal

Anexo E – Questionário de autoavaliação

ANEXO À INSTRUÇÃO N.º 46/2012 - (BO N.º 12, 17.12.2012)

SUPERVISÃO

Temas

Branqueamento de Capitais

ANEXO

(a que se refere o nº 3.)

QUESTIONÁRIO DE AUTO-AVALIAÇÃO

A. PERÍODO DE REFERÊNCIA	
INÍCIO	
TERMO	
B. INFORMAÇÃO INSTITUCIONAL	
CÓDIGO DE AGENTE FINANCEIRO	
DENOMINAÇÃO SOCIAL	
NÚMERO DE IDENTIFICAÇÃO DE PESSOA COLETIVA	
TIPO DE INSTITUIÇÃO	

INSTITUIÇÕES DE CRÉDITO **SOCIEDADES FINANCEIRAS** **INSTITUIÇÕES DE PAGAMENTO** **INSTITUIÇÕES DE MOEDA ELETRÓNICA**	Morada da Sede ou do Estabelecimento Principal: Países ou jurisdições das Filiais: Países ou jurisdições das Sucursais: Países ou jurisdições dos Agentes:
SUCURSAIS ESTABELECIDAS EM PORTUGAL	Morada da Sucursal em Portugal: País ou jurisdição da Sede:
OUTRAS ENTIDADES QUE PRESTEM SERVIÇOS FINANCEIROS	Morada da Sede ou do Estabelecimento Principal:

NÚMERO TOTAL DE EMPREGADOS	
NÚMERO DE COLABORADORES RELEVANTES INTERNOS	
NÚMERO DE COLABORADORES RELEVANTES INTERNOS AFETOS À FUNÇÃO DE *COMPLIANCE* E ESPECIFICAMENTE DEDICADOS À PREVENÇÃO DO BC/FT	
PRINCIPAIS ÁREAS DE NEGÓCIO DA INSTITUIÇÃO (DEFINIDAS NO PLANO ESTRATÉGICO OU EM DOCUMENTO EQUIVALENTE)	
PAÍSES OU JURISDIÇÕES ONDE A INSTITUIÇÃO DESENVOLVE AS ATIVIDADES CORRESPONDENTES ÀS SUAS PRINCIPAIS ÁREAS DE NEGÓCIO	
CENTROS *OFFSHORE* ONDE A INSTITUIÇÃO TENHA FILIAIS	

CENTROS *OFFSHORE* ONDE A INSTITUIÇÃO TENHA SUCURSAIS	
ELEMENTO DA ÁREA DE *COMPLIANCE* RESPONSÁVEL PELA PREVENÇÃO DO BC/FT (RCBCFT)	Nome:
	Data de início de funções:
	Contato telefónico direto:
	Endereço de correio eletrónico:

C. ELEMENTOS INFORMATIVOS			
C.1 AVALIAÇÃO DE RISCOS E POLÍTICAS BC/FT	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1.1 A instituição identificou os fatores de risco de BC/FT existentes no contexto da sua realidade operativa específica, tendo em atenção o seu modelo de negócio e os perfis dos seus clientes?			
1.2 A instituição definiu e implementou uma política de prevenção do BC/FT, tendo em vista a identificação, gestão e mitigação dos riscos associados à sua realidade operativa específica?			
1.2.1 Os princípios orientadores e procedimentos previstos na política de prevenção do BC/FT:			
a) São objeto de apreciação e aprovação pelo órgão de administração da instituição (ou equivalente) e/ou por comité competente?			
b) São reduzidos a escrito?			
c) São objeto de revisão periódica, por forma a assegurar a sua eficácia e permanente atualidade?			
1.3 Os procedimentos preventivos do BC/FT existentes na instituição são objeto de alguma avaliação periódica efetuada no âmbito da função de auditoria interna?			
1.4 Os procedimentos preventivos do BC/FT existentes na instituição são objeto de algum tipo de auditoria externa periódica?			

1.5 A instituição desenvolve atividade em zonas geográficas de risco?			
C.2 SISTEMA INFORMÁTICO	**SIM**	**NÃO**	**NÃO APLICÁVEL**
2.1 Existe, nos quadros da instituição, entidade/pessoa responsável pelos sistemas de informação?			
2.2 As bases de dados e servidores da instituição estão localizados em território nacional?			
C.3 DEVER DE IDENTIFICAÇÃO	**SIM**	**NÃO**	**NÃO APLICÁVEL**
3.1 A instituição dá cumprimento ao dever de identificação:			
3.1.1 Sempre que estabelece uma relação de negócio?			
3.1.2 Quando efetua transações ocasionais cujo valor unitário seja igual ou superior a € 15.000,00?			
3.1.3 Quando efetua transações ocasionais que aparentem estar relacionadas entre si e cujo valor agregado seja igual ou superior a € 15.000,00?			
3.1.4 Quando efetua transações ocasionais de qualquer valor e das quais suspeite poderem estar relacionadas com o BC/FT?			
3.1.5 Sempre que tem dúvidas quanto à veracidade ou adequação dos dados de identificação anteriormente obtidos?			
3.2 O processo de identificação:			
3.2.1 Abrange os representantes/titulares de poderes de movimentação de contas de depósito bancário?			
3.2.2 Abrange os beneficiários efetivos?			
3.2.3 Compreende o registo dos elementos identificativos e a comprovação da veracidade dos mesmos, nos termos previstos no quadro normativo vigente?			
3.2.4 Pressupõe sempre a apresentação de um documento de identificação válido emitido, por autoridade pública competente, com a fotografia e assinatura do respetivo titular			

(ressalvada a abertura de contas de depósito bancário em nome de menores que, em razão da sua idade, não sejam titulares deste documento)?			
3.2.5 Pressupõe sempre a apresentação de documentos originais/cópias certificadas:			
a) No caso das relações de negócio/transações ocasionais estabelecidas/realizadas de forma presencial?			
b) No caso das relações de negócio/transações ocasionais estabelecidas/realizadas de forma não presencial?			
3.2.6 Compreende a verificação da idoneidade e da suficiência dos instrumentos que outorgam os poderes de representação/poderes de movimentação de contas?			
3.2.7 Compreende sempre a aposição, nos registos internos de suporte, da data e da identificação do colaborador da instituição que executou os procedimentos de identificação?			
3.2.8 Tem sempre lugar antes do estabelecimento de qualquer relação de negócio ou da realização de qualquer transação ocasional?			
3.3 No caso de contas de depósito bancário e enquanto não se mostrar completo o processo de identificação:			
3.3.1 A instituição procede à abertura da conta?			
a) É permitida a realização de quaisquer movimentos a débito ou a crédito na conta subsequentes ao depósito inicial?			
b) São disponibilizados instrumentos de pagamento sobre a conta?			
c) É permitida a realização de alterações na titularidade da conta?			
3.4 Quando a instituição adota procedimentos de identificação simplificada, recolhe sempre os elementos identificativos suficientes para verificar se se mostram preenchidas as condições previstas nos números 1 e 2 do artigo 11.º da Lei?			
3.5 Quando a instituição adota procedimentos de identificação simplificada relativamente aos beneficiários efetivos de contas-clientes tituladas por advogados ou solicitadores estabelecidos em Portugal, exige sempre a declaração prevista no nº 2 do artigo 11.º da Lei?			
3.6 A instituição recorre à execução do dever de identificação por terceiros previsto no artigo 24.º da Lei?			

3.7 A instituição dispõe de procedimentos regulares de confirmação da atualidade dos elementos identificativos, dos meios comprovativos e dos demais elementos de informação relacionados com os clientes, os representantes/titulares de poderes de movimentação de contas de depósito bancário e os beneficiários efetivos?			
3.8 A instituição, antes de estabelecer uma relação de negócio ou efetuar uma transação ocasional, procede à verificação e filtragem de nomes constantes de listas publicadas pela União Europeia, Organização das Nações Unidas ou outros organismos?			
3.9 Relativamente às transações ocasionais em geral:			
3.9.1 A instituição dispõe de um registo centralizado:			
a) Que contenha informação sobre todos os seus clientes?			
b) Que contenha informação sobre todas as operações efetuadas?			
c) Que permita associar a um cliente todas as operações por este efetuadas?			
3.9.2 No caso de a instituição dispor de um registo centralizado, as informações constantes do mesmo estão permanentemente acessíveis em todos os espaços físicos, sitos no território nacional, onde aquela desenvolve a sua atividade (incluindo nas instalações dos seus agentes e terceiros com funções operacionais, a que alude o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, aprovado pelo Decreto-Lei nº 317/2009, de 30 de Outubro)?			
3.10 Relativamente a transferências de fundos para o exterior ou do exterior (quando dissociadas de qualquer conta e quando não abrangidas pelas exclusões previstas nos números 2, 4, 5 e 7 do artigo 3.º do Regulamento (CE) nº 1781/2006, do Parlamento Europeu e do Conselho, de 15 de Novembro de 2006):			
3.10.1 A instituição dá cumprimento ao processo de identificação dos seus clientes, sempre que as transferências sejam de montante superior a € 1.000, independentemente de este valor resultar de uma única operação ou da agregação de várias operações que aparentem estar relacionadas entre si?			
3.11 GRAU DE CONFORMIDADE NORMATIVA | Dever de Identificação			

C.4 DEVER DE DILIGÊNCIA	**SIM**	**NÃO**	**NÃO APLICÁVEL**
4.1. Para além da identificação dos clientes, dos representantes/titulares de poderes de movimentação de contas de depósito bancário e dos beneficiários efetivos, a instituição:			

4.1.1 Obtém informação sobre a estrutura de propriedade e de controlo do cliente, quando este é uma pessoa coletiva ou um centro de interesses coletivos sem personalidade jurídica?			
4.1.2 Obtém informação sobre a finalidade e a natureza pretendida da relação de negócio?			
4.1.3 Obtém informação sobre a origem e o destino dos fundos, quando o perfil de risco do cliente ou as características da operação o justifiquem?			
4.1.4 Mantém um acompanhamento contínuo da relação de negócio, a fim de assegurar que tais transações são consentâneas com o conhecimento que a entidade tem das atividades e do perfil de risco do cliente?			
4.2 Quando a instituição adota procedimentos de diligência simplificada, recolhe sempre os elementos identificativos suficientes para verificar se se mostram preenchidas as condições previstas nos números 1 e 2 do artigo 11.º da Lei?			
4.3 Quando a instituição adota procedimentos de diligência simplificada relativamente aos beneficiários efetivos de contas-clientes tituladas por advogados ou solicitadores estabelecidos em Portugal, exige sempre a declaração prevista no nº 2 do artigo 11.º da Lei?			
4.4 Relativamente às relações de negócio/transações ocasionais estabelecidas/realizadas de forma não presencial, a instituição complementa o processo de identificação através de algum dos meios previstos no nº 3 do artigo 12.º da Lei?			
4.5 Relativamente a "Pessoas Politicamente Expostas" (PEP):			
4.5.1 A instituição dispõe de mecanismos ou procedimentos específicos que lhe permitam detetar – entre os seus clientes, os representantes/titulares de poderes de movimentação de contas de depósito bancário e os beneficiários efetivos – PEP residentes fora do território nacional?			
4.5.2 A instituição dispõe de mecanismos ou procedimentos específicos que lhe permitam detetar – entre os seus clientes, os representantes/titulares de poderes de movimentação de contas de depósito bancário e os beneficiários efetivos – PEP residentes em território nacional?			
4.5.3 É assegurada a intervenção do nível hierárquico imediato para a autorização do estabelecimento/realização de relações de negócio/transações ocasionais com PEP residentes fora do território nacional?			

C.6 DEVER DE CONSERVAÇÃO	**SIM**	**NÃO**	**NÃO APLICÁVEL**

4.5.4 A instituição toma as medidas necessárias para determinar a origem do património e dos fundos envolvidos nas relações de negócio e transações ocasionais com PEP residentes fora do território nacional?			
4.5.5 A instituição efetua um acompanhamento contínuo acrescido no caso das relações de negócio estabelecidas com PEP residentes fora do território nacional?			
4.6 Relativamente às operações de correspondência bancária:			
4.6.1 A instituição possui relações de correspondência bancária com instituições de crédito de países terceiros?			
4.6.2 Em caso afirmativo, a instituição obtém informação sobre o banco cliente que lhe permita:			
a) Compreender a natureza da respetiva atividade?			
b) Avaliar as respetivas políticas e procedimentos internos destinados a prevenir o BC/FT?			
c) Aferir a respetiva reputação e a qualidade da supervisão a que a mesma está sujeita?			
4.6.3 A relação de correspondência bancária é autorizada por um nível hierárquico superior?			
4.6.4 As responsabilidades assumidas por cada instituição no âmbito da relação de correspondência bancária constam sempre de documento escrito?			
4.6.5 No caso de contas correspondentes de transferência, a instituição:			
a) Confirma que foi verificada a identidade dos clientes que dispõem de acesso direto à conta?			
b) Confirma que o banco cliente observa o dever de diligência relativamente aos clientes que dispõem de acesso direto à conta?			
c) Assegura-se de que os elementos de informação referentes aos clientes que dispõem de acesso direto à conta lhe são fornecidos quando solicitados ao banco cliente?			
4.7 A instituição recorre à execução do dever de diligência por terceiros previsto no artigo 24.º da Lei?			
4.8 GRAU DE CONFORMIDADE NORMATIVA | Dever de Diligência			

C.5 DEVER DE RECUSA	SIM	NÃO	NÃO APLICÁVEL
5.1 Durante o período de referência, a instituição recusou efetuar operações, iniciar relações de negócio ou realizar transações ocasionais?			
5.1.1 Existe evidência escrita da análise às circunstâncias que determinaram a recusa?			
5.1.2 Qual o número de recusas motivadas pela não disponibilização de elementos de identificação do cliente, do seu representante ou do beneficiário efetivo?			
5.1.3 Qual o número de recusas motivadas pela não disponibilização de elementos sobre a estrutura de propriedade e controlo do cliente, a natureza e a finalidade da relação de negócio ou a origem e destino dos fundos?			
5.1.4 Qual o número de recusas que deram origem a comunicações à UIF e à PGR.			
5.1.5 Qual o número de recusas que levaram ao termo da relação de negócio por decisão da instituição.			
5.2 GRAU DE CONFORMIDADE NORMATIVA | Dever de Recusa			

6.1 São conservadas cópias ou referências dos/aos documentos recolhidos pela instituição no âmbito do cumprimento do dever de identificação e de diligência, por um período de sete anos (i) após o momento em que a identificação se processou ou (ii) no caso das relações de negócio, após o termo das mesmas?			
6.2 São conservados os originais, as cópias, as referências ou quaisquer suportes duradouros, com idêntica força probatória, dos documentos comprovativos e dos registos das operações por um período de sete anos a contar da execução daquelas (mesmo nos casos em que a respetiva relação de negócio já tenha terminado)?			
6.3 Os elementos referidos em 6.1.e 6.2 são conservados pela instituição em condições que permitam o imediato acesso aos mesmos, sempre que a informação seja solicitada pelos responsáveis pela função de *compliance* ou de auditoria, pelos auditores externos, pelas entidades policiais ou pelas autoridades judiciárias ou de supervisão?			
6.4 GRAU DE CONFORMIDADE NORMATIVA | Dever de Conservação			

C.7 DEVER DE EXAME	SIM	NÃO	NÃO APLICÁVEL

7.1 A instituição examina com especial cuidado e atenção qualquer conduta, atividade ou operação cujos elementos caracterizadores a tornem particularmente suscetível de poder estar relacionada com o BC/FT?			
7.2 A instituição dispõe de algum sistema informático que permita, cumulativamente, a monitorização e a pesquisa de operações e clientes, com o objetivo de identificar condutas, atividades ou operações suspeitas ou não usuais?			
7.3 Os resultados do exame de condutas, atividades ou operações suspeitas constam de documento escrito?			
7.3.1 O documento em apreço é conservado durante 5 anos?			
7.4 O processo de exame de condutas, atividades ou operações suspeitas tem sempre a participação de colaboradores da área de *compliance* da instituição afetos à prevenção do BC/FT?			
7.5 Qual o número de operações examinadas durante o período de referência?			
7.6 Qual o montante agregado das operações examinadas durante o período de referência?			
7.7 Qual o número de operações examinadas durante o período de referência em relação às quais foi decidida a comunicação às autoridades competentes?			
7.8 GRAU DE CONFORMIDADE NORMATIVA | Dever de Exame			
C.8 DEVER DE COMUNICAÇÃO	**SIM**	**NÃO**	**NÃO APLICÁVEL**
8.1 Durante o período de referência, a instituição efetuou comunicações de operações suspeitas à PGR e à UIF?			
8.2 As comunicações de operações suspeitas à PGR e à UIF:			
8.2.1 São efetuadas no âmbito da função de *compliance* da instituição?			
8.2.2 São efetuadas através dos canais de comunicação externos definidos pela PGR e/ou pela UIF, nos termos por elas estabelecidos?			
8.2.3 São efetuadas logo que a instituição financeira conclui pela natureza suspeita da operação?			

8.2.4 Incluem informação sobre a identidade das pessoas direta ou indiretamente envolvidas nas operações?			
8.2.5 Incluem informação sobre a atividade conhecida das pessoas direta ou indiretamente envolvidas nas operações?			
8.2.6 Incluem informação sobre os elementos caracterizadores das operações?			
8.2.7 Incluem informação sobre os fatores de suspeita concretamente identificados pela instituição?			
8.3 Nos casos em que a instituição decide não comunicar às autoridades competentes uma operação que tenha sido objeto de exame, os fundamentos dessa decisão são reduzidos a escrito?			
8.3.1 Esse documento é conservado durante 5 anos?			
8.4 Qual o número total de comunicações de operações suspeitas à PGR e à UIF efetuadas pela instituição, durante o período de referência, ao abrigo do artigo 16.º da Lei?			
8.5 Qual o montante agregado das operações suspeitas comunicadas à PGR e à UIF efetuadas pela instituição, durante o período de referência, ao abrigo do artigo 16.º da Lei?			
8.6 Qual o número total de comunicações à PGR e à UIF efetuadas pela instituição, durante o período de referência, ao abrigo do artigo 27.º da Lei?			
8.7 Qual o montante agregado das operações comunicadas à PGR e à UIF, durante o período de referência, ao abrigo do artigo 27.º da Lei?			
8.8 GRAU DE CONFORMIDADE NORMATIVA | Dever de Comunicação			
C.9 DEVER DE ABSTENÇÃO	**SIM**	**NÃO**	**NÃO APLICÁVEL**
9.1 Durante o período de referência, a instituição absteve-se de executar operações suspeitas de estarem relacionadas com a prática do BC/FT?			
9.1.1 A instituição informou de imediato a PGR e a UIF da abstenção de execução das operações?			

9.2 Durante o período de referência, ocorreram situações em que a instituição tenha executado uma operação suspeita por considerar não ser possível a abstenção da respetiva realização?			
9.2.1 Qual o número total de operações em que tal se verificou?			
9.2.2 Qual o montante agregado das operações em que tal se verificou?			
9.2.3 As informações respeitantes às operações foram fornecidas de imediato à PGR e à UIF?			
9.3 Durante o período de referência, ocorreram situações em que a instituição tenha executado uma operação suspeita por considerar que a abstenção da respetiva realização poderia prejudicar a prevenção ou a futura investigação do BC/FT?			
9.3.1 Qual o número total de operações em que tal se verificou?			
9.3.2 Qual o montante agregado das operações em que tal se verificou?			
9.3.3 A decisão da instituição foi precedida de consulta à PGR e à UIF?			
9.4 GRAU DE CONFORMIDADE NORMATIVA | Dever de Abstenção			

C.10 DEVER DE COLABORAÇÃO	**SIM**	**NÃO**	**NÃO APLICÁVEL**
10.1 A estrutura organizativa da instituição está preparada para dar uma resposta atempada aos pedidos de informação que lhe são endereçados pelas entidades referidas nos artigos 18.º e 28.º da Lei?			
10.2 Durante o período de referência, foram recebidos pedidos de informação por parte das autoridades judiciárias, PGR ou UIF ao abrigo do dever de colaboração previsto na Lei?			

C.11 DEVER DE SEGREDO	**SIM**	**NÃO**	**NÃO APLICÁVEL**
11.1 A instituição dispõe de normas ou procedimentos internos destinados a prevenir a ocorrência das situações previstas no nº 1 do artigo 19.º da Lei?			
11.2 GRAU DE CONFORMIDADE NORMATIVA | Dever de Segredo			

C.12 DEVER DE CONTROLO	SIM	NÃO	NÃO APLICÁVEL
12.1 A instituição define e implementa um sistema de controlo interno que integre estratégias, políticas, processos e procedimentos destinados a garantir o cumprimento das normas legais e regulamentares em matéria de prevenção do BC/FT e a evitar o seu envolvimento em operações relacionadas com aqueles tipos de crimes?			
12.2 A instituição reduz a escrito as estratégias, políticas, processos e procedimentos que, em matéria de BC/FT, integram o seu sistema de controlo interno?			
12.3 A instituição assegura a suficiência e adequação dos recursos humanos, financeiros, materiais e técnicos afetos à prevenção do BC/FT?			
12.4 A instituição divulga, junto dos seus colaboradores relevantes, informação escrita atualizada e permanentemente acessível aos mesmos sobre os princípios fundamentais do sistema de controlo interno em matéria de prevenção de BC/FT, bem como sobre as normas e procedimentos instrumentais para a sua execução?			
12.5 A instituição assegura a monitorização das operações, com vista à deteção daquelas que comportem maior risco e à emissão dos correspondentes indicadores de alerta?			
12.6 A instituição assegura a monitorização contínua da qualidade do sistema de controlo interno e procede a testes regulares da sua adequação e eficácia?			
12.7 A instituição mantém uma função de *compliance* independente, permanente e efetiva, para controlo do cumprimento do quadro legal e regulamentar preventivo do BC/FT?			
12.8 O RCBCFT integra os quadros da instituição?			
12.9 O RCBCFT dispõe dos poderes, meios e recursos necessários para o desempenho objetivo e independente das respetivas competências funcionais?			
12.10 O RCBCFT tem acesso irrestrito e atempado a toda a informação interna relevante para o exercício da sua função?			
12.11 GRAU DE CONFORMIDADE NORMATIVA | Dever de Controlo			
C.13 DEVER DE FORMAÇÃO	**SIM**	**NÃO**	**NÃO APLICÁVEL**
13.1 A instituição dispõe de uma política de formação regular sobre prevenção do BC/FT dirigida:			

13.1.1 Aos seus colaboradores relevantes internos?			
13.1.2 Aos seus colaboradores relevantes externos?			

13.2 Durante o período de referência, quantas ações de formação sobre prevenção de BC/FT foram ministradas a colaboradores relevantes da instituição?			
13.3 Durante o período de referência, qual a percentagem de colaboradores relevantes internos que frequentaram, pelo menos, uma ação de formação sobre esta temática específica?			
13.4 Existe um registo atualizado sobre as ações de formação frequentadas pelos colaboradores relevantes da instituição?			
13.5 A instituição conserva o suporte documental relativo às ações de formação frequentadas pelos colaboradores relevantes da instituição?			
13.6 GRAU DE CONFORMIDADE NORMATIVA | Dever de Formação			
C.14 OUTROS ASPETOS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
14.1 Sucursais e filiais em países terceiros			
14.1.1 A instituição tem sucursais em países terceiros (incluindo centros *offshore*)?			
14.1.2 A instituição tem filiais em países terceiros (incluindo centros *offshore*), nos quais detenha participação maioritária no capital social e/ou que confira a maioria dos direitos de voto?			
14.1.3 A instituição aplica, em todas as suas sucursais e filiais em países terceiros (incluindo as domiciliadas em centros *offshore*), medidas equivalentes às previstas na Lei em matéria de deveres de identificação, diligência, conservação e formação?			
14.1.4 A instituição comunica as suas políticas e procedimentos internos em matéria de prevenção de BC/FT a todas as suas sucursais e filiais em países terceiros (incluindo as domiciliadas em centros *offshore*)?			
14.1.5 A instituição dispõe de mecanismos de controlo que lhe permitam verificar se as medidas equivalentes às previstas na Lei são efetivamente aplicadas, em permanência, nas suas sucursais e filiais em países terceiros (incluindo as domiciliadas em centros *offshore*)?			

14.1.6 A instituição tem alguma sucursal ou filial em país terceiro (incluindo os centros *offshore*) cuja legislação não permita a aplicação de medidas equivalentes às previstas na Lei em matéria de deveres de identificação, diligência, conservação e formação?			
14.1.6.1 Em caso afirmativo:			
a) A instituição comunicou tal impedimento ao Banco de Portugal?			
b) A instituição adotou medidas suplementares destinadas a prevenir o risco de BC/FT?			
14.1.7 GRAU DE CONFORMIDADE NORMATIVA | Sucursais e Filiais em Países Terceiros			
14.2 Bancos de fachada			
14.2.1 A instituição dispõe de procedimentos específicos destinados a evitar o estabelecimento de relações de correspondência com instituições que permitam a utilização das respetivas contas por bancos de fachada?			
14.2.2 Durante o período de referência, foi detetada alguma relação de correspondência com instituições que permitam a utilização das respetivas contas por bancos de fachada?			
14.2.2.1 Nesses casos, a instituição pôs termo à relação de correspondência existente?			
14.2.3 GRAU DE CONFORMIDADE NORMATIVA | Bancos de Fachada			
14.3 Instituições de Pagamento e Instituições de Moeda Eletrónica			
14.3.1 A instituição presta, em território nacional, serviços de pagamento através de agentes ou terceiros com funções operacionais?			
14.3.2 Em caso afirmativo, qual o número total desses agentes e terceiros com funções operacionais?			
14.3.3 A instituição presta, fora do território nacional, serviços de pagamento através de agentes ou terceiros com funções operacionais?			
14.3.4 Em caso afirmativo, qual o número total desses agentes e terceiros com funções operacionais?			
14.3.5 A instituição de moeda eletrónica procede à emissão, distribuição e/ou reembolso de moeda eletrónica com recurso a terceiros com funções operacionais?			

14.3.6 Em caso afirmativo, qual o número total desses terceiros com funções operacionais?			
14.3.7 A instituição, monitoriza o cumprimento da legislação preventiva do BC/FT por parte dos seus agentes /terceiros com funções operacionais domiciliados em território nacional?			
14.3.8 A instituição, monitoriza o cumprimento da legislação preventiva do BC/FT por parte dos seus agentes /terceiros com funções operacionais domiciliados fora do território nacional?			
14.3.9 No caso de operações de transferência de fundos para o exterior:			
14.3.9.1 A instituição acompanha diretamente todo o circuito dos fundos, desde o momento em que os mesmos lhe são entregues pelo ordenante da operação até ao momento em que são disponibilizados, no país ou jurisdição de destino, ao beneficiário final da mesma?			
a) Em caso afirmativo, a instituição conserva nos seus arquivos a documentação de suporte do circuito integral dos fundos transferidos, ilustrando todo o percurso dos mesmos entre o ordenante e o beneficiário da operação?			
14.3.9.2 No decurso do processo de transferência e durante todo o circuito dos fundos, a instituição recorre exclusivamente a entidades ou pessoas devidamente autorizadas – pelas entidades competentes dos países ou jurisdições envolvidos – para processar as operações, em especial no país ou jurisdição que corresponde ao destino final dos fundos transferidos?			
14.4 Língua portuguesa			
14.4.1 Existe uma versão em língua portuguesa, permanentemente atualizada, dos manuais de procedimentos, e de outra documentação interna relevante, em matéria de prevenção do BC/FT?			
14.5 Ilícitos criminais e contra-ordenacionais			
14.5.1 Durante os últimos cinco anos, a instituição foi objeto de alguma condenação criminal ou contra-ordenacional – em Portugal ou em qualquer outro país e ainda que não transitada em julgado – pela prática de ilícitos relacionados com o BC/FT ou pelo incumprimento de procedimentos destinados à sua prevenção?			

D. DECLARAÇÃO DO ÓRGÃO DE GESTÃO

O órgão de administração (ou equivalente) da instituição declara que:

A) Todas as informações prestadas no presente QAA são verdadeiras;

B) As avaliações feitas no presente QAA quanto ao grau de conformidade normativa correspondem à efetiva perceção da instituição.

Anexo F – Atividade Sancionatória do Banco de Portugal

- 2017

Tabela 1 - Atividade Sancionatória do Banco de Portugal em 2017

Trimestre	Processos Instaurados	Processos de Contraordenação	Quantidade e Natureza da Contraordenação	Admoestações (Advertências)	Coimas	Coimas suspensas na Execução
1º T	54	84	55 - Infrações de natureza comportamental 17 - Infrações de natureza prudencial 11 - Infrações a deveres relativos à prevenção do branqueamento de capitais e do financiamento do terrorismo 1 - Infrações às regras em matéria de recirculação de	**18**	**230 000,00 €**	**- €**
2º T	46	37	27 - Infrações de natureza comportamental 6 - Infrações de natureza prudencial 3 - Infrações a deveres relativos à prevenção do branqueamento de capitais e do financiamento do terrorismo 1 - Atividade financeira ilícita	**3**	**1 455 500,00 €**	**400 000,00 €**
3º T	31	55	38- Infrações de natureza comportamental 15 - Infrações de natureza prudencial 1- Infrações a deveres relativos à prevenção do branqueamento de capitais e do financiamento do terrorismo 1 - Infrações às regras em matéria de recirculação de	**4**	**317 000,00 €**	**10 000,00 €**
4º T	23	108	77- Infrações de natureza comportamental 23 - Infrações de natureza prudencial 5 - Infrações a deveres relativos à prevenção do branqueamento de capitais e do financiamento do terrorismo 2 - Atividade financeira ilícita 1 - Infrações às regras em matéria de recirculação de numerário.	**11**	**911 000,00 €**	**336 500,00 €** •

Fonte: Elaboração Própria com base em dados do *site* institucional do Banco de Portugal

- 2018

Tabela 2 - Atividade Sancionatória do Banco de Portugal em 2018

Trimestre	Processos Instaurados	Processos de Contraordenação	Quantidade e Natureza da Contraordenação	Admoestações (Advertências)	Coimas	Coimas suspensas na Execução
1º T	34	30	11 - Infrações de natureza comportamental 9 - Infrações de natureza prudencial 10 - Infrações a deveres relativos à prevenção do branqueamento de capitais e do financiamento do terrorismo	**8**	**694 500,00 €**	**566 000,00 €**
2º T	34	39	25 - Infrações de natureza comportamental 10 - Infrações de natureza prudencial 2- Infrações a deveres relativos à prevenção do branqueamento de capitais e do financiamento do terrorismo 1 - Atividade financeira ilícita 1 - Infrações às regras em matéria de recirculação de numerário.	**18**	**273 250,00 €**	**20 000,00 €**

Fonte: Elaboração Própria com base em dados do *site* institucional do Banco de Portugal

Anexo G – Guião da entrevista

Introdução:

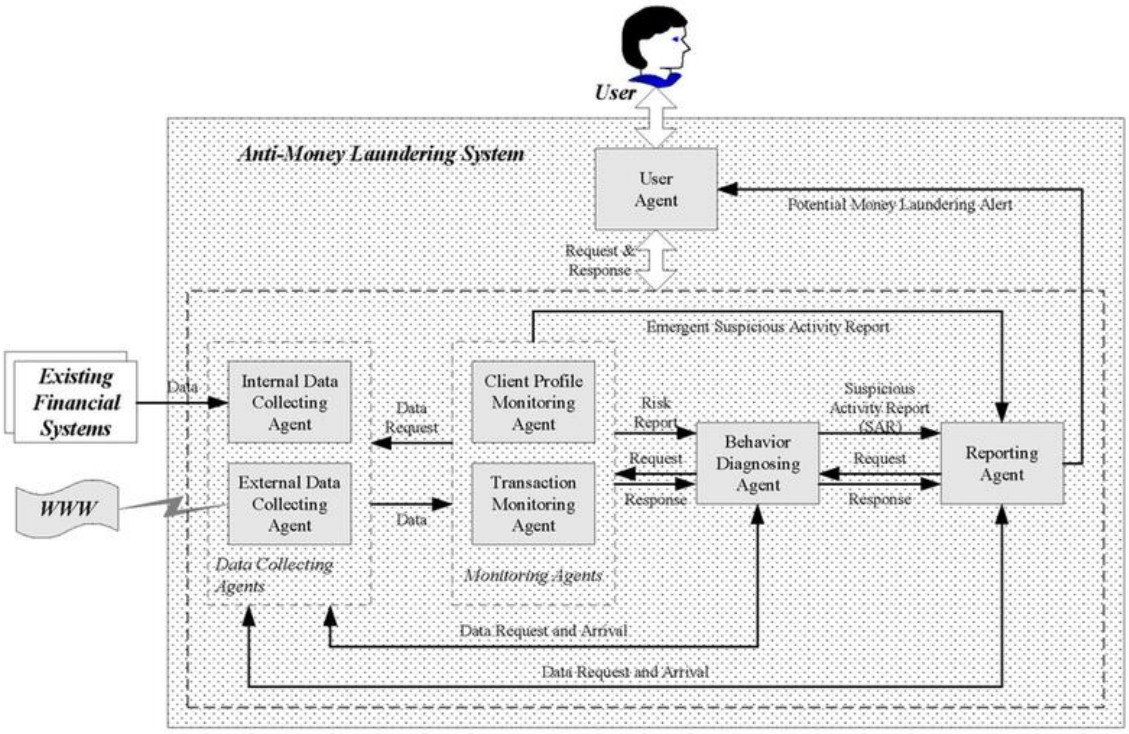
Como disse anteriormente, a minha tese de Mestrado foca-se nas ferramentas tecnológicas utilizadas para o combate do BC e do FT pelo Banco de Portugal, e como tal, através da minha análise documental, constatei que o BdP utiliza uma aplicação informática, o BIIAS - Base de Informação de Inspeções e Averiguações, que assegura a definição do Índice de Atenção Supervisiva (IAS) e a hierarquização das instituições em função desse índice. O IAS é atribuído a cada instituição e calculado com base em informação interna e externa de natureza e proveniência diversa.

Questões:

1) Face ao exposto, gostaria de lhe perguntar se tem conhecimento sobre este tipo de aplicações utilizadas no combate ao BC e ao FT? Se sim, qual/quais? Na sua opinião, como acha que estes sistemas podem ser melhorados?
2) Tendo em conta a sua área de estudo em segurança informática em redes e sistemas, na sua opinião como se deve proteger uma aplicação financeira deste género, de ataques exogéneos?

3) No caso dos ataques *NotPetya* e do *WannaCry*, que causaram danos a nível mundial e de forma transversal, afetando setores como a banca, a saúde, os operadores de serviços de comunicações, entre outros. Acha que o que me indicou anteriormente teria sido suficiente para prevenir a situação? O que falhou?
4) Por norma, os sistemas operativos do setor bancário estão desatualizados em relação às inovações tecnológicas existentes no mercado e adotadas por diversas empresas. O motivo por trás disto é a manutenção da estabilidade dos sistemas utilizados.
   Assim, na sua opinião qual deveria ser a decisão a tomar? Dar prioridade à estabilidade em detrimento de atualizações dos sistemas operativos (que podem eventualmente implementar mais mecanismos de segurança e *patches* etc)? Ou vice-versa? Impasse: Estabilidade VS Atualizações/ Segurança; Será possível haver a simbiose entre estes dois termos?
5) Tendo em conta as soluções oferecidas pelo mercado para proteger as aplicações financeiras, acha que estas podem continuar a estar adequadas/atualizadas no futuro tendo em conta a velocidade da evolução constante dos sistemas e redes?
6) Tem conhecimento se os órgãos como o centro nacional de cibersegurança estão envolvidos neste tipo de aplicações financeiras? Se sim, como?

7)



Isto é um diagrama que explica em alto nível o funcionamento da aplicação "padrão" que é hoje em dia utilizada em instituições financeiras para combate ao BC. Esta informação é pública e está disponível *online*.

Como poderá constatar a informação é recolhida em tempo real por *Collecting agents* e é posteriormente analisada de forma a detetar padrões e criar perfis levando a um diagnóstico que é então enviado ao operador.

A informação recolhida é proveniente de duas fontes:

- Interna (ou seja outros sistemas financeiros)
- Externa (ou seja informação que está disponível online)

Estes sistemas usam padrões previamente carregados para utilizarem como termo de comparação e quando detetam um novo podem adicionar o mesmo à sua base de dados.

Quando comecei a estudar o funcionamento destes sistemas concluí que (na minha opinião) poderiam ser melhorados de forma relativamente simples:

- À semelhança do que já é feito, por exemplo, com diversas *appliances* de segurança (como *firewalls*, UTMs, etc) estes sistemas poderiam comunicar constantemente com uma base de dados geral (do

fabricante?) e eventualmente uns com os outros. Desta forma, seria possível a partilha rápida e fácil de informação. Por exemplo, sempre que um sistema detetasse uma nova “ameaça” (leia-se tentativa de BC) enviava o padrão/ perfil criado, de imediato para todos os outros sistemas e para a base de dados geral. Assim, numa questão de alguns minutos/ horas, todos os outros sistemas estariam já “informados” da existência do problema e preparados para o resolver. Exemplos: Sophos UTM, HP Aruba, Checkpoint, etc

Até que ponto acha que isto poderia ter implicações a nível de segurança? Como seria possível proteger um sistema destes, tendo em conta a implementação desta funcionalidade (que implicaria comunicação com outros sistemas, externos à rede da instituição, e com a referida “base de dados geral”)?

Anexo H – Declaração de consentimento

Declaração de Consentimento

Eu (nome completo do participante), MIGUEL FILIPE LEITÃO PARDAL declaro que fui informado (a) do objetivo e metodologia da investigação sobre Branqueamento de Capitais e Financiamento do Terrorismo, com enfoque nas ferramentas tecnológicas utilizadas pelo Banco de Portugal.

Estou consciente de que em nenhum momento serei exposto (a) a riscos em virtude da minha participação nesta investigação e que poderei em qualquer momento recusar continuar sem nenhum prejuízo para a minha pessoa. Sei também que os dados da entrevista, por mim respondida serão usados somente para fins científicos. Os resultados do estudo poderão ser consultados sempre que solicitar. Fui informado (a) de que não terei nenhum tipo de despesas nem receberei nenhum pagamento ou gratificação pela minha participação nesta investigação.

Depois do anteriormente referido, decido livremente participar neste projeto de investigação, tal como me foi apresentado pela investigadora.

Miguel Pardal

(Participante)

Lisboa, 11 de OUTUBRO de 2018