Os conflitos entre os princípios de proteção de dados e os deveres de AML no âmbito do tratamento de dados pelas instituições financeiras

CHRISTIANO AGUIAR *

Resumo: No âmbito da prevenção ao branqueamento de capitais e financiamento do terrorismo, as instituições financeiras tratam os dados das pessoas singulares envolvidas em relações de negócio e transações ocasionais com base no cumprimento de uma obrigação jurídica a que as instituições financeiras estão sujeitas. No entanto, este tratamento de dados envolve conflitos entre os princípios previstos no RGPD e os deveres impostos pelo regime de prevenção ao branqueamento de capitais e financiamento do terrorismo, designadamente o princípio da transparência contra o dever de não divulgação das informações, o princípio da minimização dos dados contra o dever de diligência quanto à clientela e o princípio da limitação da conservação dos dados contra o dever de conservação dos dados

Palavras-chave: *prevenção ao branqueamento de capitais; princípios de proteção de dados; conflitos entre RGPD e Diretiva AML.*

Abstract: In the context of the prevention of money laundering and terrorist financing, financial institutions process the data of individuals involved in business relationships and occasional transactions based on compliance with a legal obligation to which financial institutions are subject. However, this

* Advogado e Data Protection Officer no Banco de Investimento Global, S.A. Mestre em Direito (Especialidade de Direito de Empresa) na Universidade de Lisboa e Pós-Graduando em Direito da Proteção de Dados no Centro de Investigação de Direito Privado. Certificado pela Irish Computer Society – ICS

data processing involves conflicts between the principles provided for in the GDPR and the obligations imposed by the anti-money laundering and terrorist financing legal framework, namely the principle of transparency against the prohibition of disclosure of information, the principle of data minimization against the duty of customer due diligence and the principle of data storage limitation against the duty of data record-retention.

Keywords: *prevention of money laundering; data protection principles; conflicts between GDPR and AML Directive.*

1. Introdução

A proteção dos dados das pessoas singulares é um direito fundamental previsto no art. 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia (UE), e as regras relativas à proteção destes dados, nomeadamente quanto ao seu tratamento e à sua livre circulação, estão estabelecidas no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, mais conhecido como Regulamento Geral Sobre a Proteção de Dados (RGPD).

Ao abrigo do RGPD, os dados pessoais devem ser tratados de forma lícita e equitativa, assegurando a transparência necessária para que os titulares destes dados saibam quem é o responsável pelo tratamento, as suas finalidades, o seu fundamento de licitude e como os direitos do titular podem ser exercidos, entre outras informações.

Num âmbito distinto, a UE assegura a proteção da integridade, da estabilidade e da reputação do seu sistema financeiro e do seu mercado interno, que podem ser prejudicados pelos fluxos de dinheiro com origem ilícita. O branqueamento de capitais e o financiamento do terrorismo são problemas significativos que devem ser tratados ao nível da UE, pelo que releva estabelecer medidas preventivas para o efeito.

A prevenção do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo é regulada pela Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015,

mais conhecida como Diretiva AML (*Anti-Money Laundering*)[1], parcialmente transposta para o regime jurídico português através da Lei n.º 83/2017, de 18 de agosto, ou Lei de Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo (LBCFT)[2].

O RGPD e a Diretiva AML são regimes jurídicos que possuem interesses opostos que serão desenvolvidos no presente trabalho, nomeadamente quanto aos princípios aplicáveis ao tratamento dos dados pessoais, que por vezes entram em conflito com os deveres impostos pelo regime de prevenção ao branqueamento de capitais.

2. O RGPD e a Prevenção ao Branqueamento de Capitais

2.1. O tratamento de dados pessoais no âmbito da prevenção ao branqueamento de capitais

A solidez, a integridade e a estabilidade das instituições financeiras[3] poderão ser gravemente comprometidas pelos esforços dos criminosos e dos seus cúmplices para dissimular a origem do produto do crime, dando origem ao branqueamento de capitais[4].

1 Por se tratar da principal Diretiva AML atualmente em vigor, será o diploma mais estudado no presente trabalho. Sobre a evolução histórica completa do regime da prevenção ao branqueamento de capitais, ver Machado, Miguel (2020), "Deveres antibranqueamento de capitais: De onde vieram, quais são e como vão evoluir (do "4G" ao "5G")", Novos Estudos sobre Law Enforcement, Compliance e Direito Penal, Coord. Maria Fernanda Palma et al, pp. 259-351. Coimbra: Almedina.

2 No âmbito da regulamentação setorial, releva destacar o Aviso n.º 2/2018 do Banco de Portugal, publicado em 26 de setembro de 2018, que regulamenta as condições de exercício, os procedimentos, os instrumentos, os mecanismos, as formalidades de aplicação, as obrigações de prestação de informação e os demais aspetos necessários a assegurar o cumprimento dos deveres preventivos do branqueamento de capitais e do financiamento do terrorismo, no âmbito da atividade das entidades financeiras sujeitas à supervisão do Banco de Portugal.

3 Considerar-se-á a definição de instituição financeira prevista no n.º 2 do art. 3.º da Diretiva AML e na alínea v) do n.º 1 do art. 2.º da LBCFT. Sem prejuízo do termo "instituição financeira", que será adotado no presente trabalho, sublinhe-se que a Diretiva AML estabelece distinções entre a instituição de crédito e a instituição financeira, não obstante ambas sejam consideradas "entidades obrigadas" para efeitos de aplicação deste diploma.

4 Conforme o n.º 3 do art. 1.º da Diretiva AML, entende-se por branqueamento de capitais os comportamentos a seguir descritos, quando praticados intencionalmente: "a) A conversão ou transferência de bens, com conhecimento de que esses bens provêm de uma atividade criminosa ou da participação numa atividade dessa natureza, com o fim de encobrir ou dissimular a sua origem ilícita ou de auxiliar quaisquer pessoas implicadas nessa atividade

É relevante identificar todas as pessoas singulares que detêm a propriedade ou o controlo de uma pessoa coletiva, permitindo às instituições financeiras identificar o beneficiário efetivo[5] desta pessoa coletiva e as diligências que deverão ser adotadas para prevenir o branqueamento de capitais. A necessidade de dispor de informações exatas e atualizadas sobre o beneficiário efetivo é um fator essencial para rastrear os agentes do crime, que de outro modo poderão dissimular a sua identidade numa estrutura societária[6].

Neste âmbito, as instituições financeiras adotam medidas baseadas no risco para compreender a estrutura de propriedade e controlo do cliente, incluindo a recolha de documentos, dados ou informações fiáveis sobre a cadeia de participações ou de controlo. Ao abrigo do n.º 1 do art. 13.º da Diretiva AML, as medidas de diligência quanto à clientela (*Customer Due Diligence*)[7] incluem:

---

a furtarem-se às consequências jurídicas dos atos por elas praticados; b) O encobrimento ou a dissimulação da verdadeira natureza, origem, localização, utilização, circulação ou propriedade de determinados bens ou de direitos sobre esses bens, com conhecimento de que tais bens provêm de uma atividade criminosa ou da participação numa atividade dessa natureza; c) A aquisição, detenção ou utilização de bens, com conhecimento, no momento da sua receção, de que provêm de uma atividade criminosa ou da participação numa atividade dessa natureza; e d) A participação num dos atos a que se referem as alíneas a), b) e c), a associação para praticar o referido ato, a tentativa e a cumplicidade na sua prática, bem como o facto de facilitar a sua execução ou de aconselhar alguém a praticá-lo." No ordenamento jurídico português, o branqueamento constitui um crime previsto no art. 368.º-A do Código Penal (Decreto-Lei n.º 48/95).

5 Conforme o n.º 6 do art. 1.º da Diretiva AML, o beneficiário efetivo é "a pessoa ou pessoas singulares que, em última instância, detêm a propriedade ou o controlo do cliente e/ou a pessoa ou pessoas singulares por conta de quem é realizada uma operação ou atividade (...)". Em Portugal, a Lei n.º 89/2017, de 21 de agosto, aprovou o Regime Jurídico do Registo Central do Beneficiário Efetivo (RJRCBE), e a entidade gestora do Registo Central do Beneficiário Efetivo (RCBE) é o Instituto dos Registos e do Notariado, I. P. (IRN), que designa os serviços que, em cada momento, reúnem as melhores condições para assegurar os procedimentos relativos a este registo.

6 Conforme o Considerando 14 da Diretiva AML.

7 Pizarro, Sebastião Nóbrega (2016), "Manual De Compliance", p.36. Braga: Nova Causa Edições Jurídicas. Na prática de Compliance bancário, este dever de identificação e diligência quanto à clientela diz respeito ao procedimento Know Your Customer (KYC). Também designado de Know Your Client, este procedimento surgiu no âmbito da aprovação do Consolidated KYC Risk Management pelo Comité de Basileia, em outubro de 2004, o qual defendia a necessidade de as instituições bancárias aplicarem políticas e procedimentos de KYC, na perspetiva de garantir a segurança e transparência nas transações.

a) A identificação do cliente e a verificação da respetiva identidade, com base em documentos, informações ou dados obtidos junto de fonte independente e credível;
b) A identificação do beneficiário efetivo e a adoção de medidas razoáveis para verificar a sua identidade para que a entidade obrigada obtenha conhecimento satisfatório;
c) A avaliação e, se necessário, a obtenção de informações sobre o objeto e a pretendida natureza da relação de negócio;
d) A realização de uma vigilância contínua da relação de negócio, incluindo o exame das operações realizadas no decurso dessa relação, a fim de assegurar que tais operações são consentâneas com o conhecimento que a entidade obrigada tem das atividades e do perfil de risco do cliente, incluindo, se necessário, da origem dos fundos.

Assim, uma vez prestados os elementos de identificação por parte do cliente, é-lhe atribuído um nível de risco que pode ser baixo, médio ou alto, o que se vai refletir no tipo de diligência a adotar, podendo tal diligência ser simplificada quando o grau de risco for baixo, nos termos dos art. 15.º a 17.º da Diretiva AML, ou reforçada quando o grau de risco for elevado, de acordo com os critérios estabelecidos nos art. 18.º a 24.º da Diretiva AML[8].

Nos ordenamentos jurídicos sujeitos à Diretiva AML, cada Estado-Membro toma as medidas adequadas para identificar, avaliar, compreender e mitigar os riscos de branqueamento de capitais e de financiamento do terrorismo a que está exposto, bem como quaisquer preocupações conexas em matéria de proteção de dados, e mantém atualizada essa avaliação do risco, conforme determina o n.º 1 do art. 7.º da Diretiva AML.

8 A lista não exaustiva dos fatores e tipos indicativos de risco potencialmente mais baixo está prevista no Anexo II da Diretiva AML, e a lista não exaustiva dos fatores indicativos de situações com um risco potencialmente mais elevado está prevista no Anexo III do mesmo diploma. Ambas as listas dividem os fatores de risco em 3 tipos, nomeadamente os seguintes: (i) fatores de risco de cliente, (ii) fatores de risco associados ao produto, serviço, operação ou canal de distribuição, e (iii) fatores de risco geográfico. Não obstante, as instituições financeiras, ao determinarem o alcance das medidas de diligência quanto à clientela, devem tomar em consideração as seguintes variáveis de risco previstas no Anexo I da Diretiva AML: "i) O objeto de uma conta ou relação; ii) O nível de bens depositados por um cliente ou o volume das operações efetuadas; iii) A regularidade ou a duração da relação de negócio".

O ordenamento jurídico português prevê que as instituições financeiras, antes do estabelecimento de uma relação de negócio ou da realização de qualquer transação ocasional, devem identificar os clientes e seus respetivos representantes, exigindo sempre a apresentação de documentos de identificação válidos. No caso de pessoas singulares, esta identificação ocorre mediante recolha e registo dos seguintes elementos identificativos: i) Fotografia; ii) Nome completo; iii) Assinatura; iv) Data de nascimento; v) Nacionalidade constante do documento de identificação; vi) Tipo, número, data de validade e entidade emitente do documento de identificação; vii) Número de identificação fiscal ou, quando não disponha de número de identificação fiscal, o número equivalente emitido por autoridade estrangeira competente; viii) Profissão e entidade patronal, quando existam; ix) Endereço completo da residência permanente e, quando diverso, do domicílio fiscal; x) Naturalidade; xi) Outras nacionalidades não constantes do documento de identificação[9].

Numa breve análise, percebe-se que o tratamento de dados pessoais no regime da prevenção ao branqueamento de capitais envolve uma grande quantidade de dados do cliente bancário, do seu representante e do beneficiário efetivo, tendo as instituições financeiras, como será visto adiante, o dever de conservar tais dados por longos períodos conforme o regime jurídico aplicável.

2.2 Fundamento de licitude aplicável ao tratamento

No âmbito da prevenção ao branqueamento de capitais, as instituições financeiras assumem a posição de responsáveis pelo tratamento prevista no n.º 7 do art. 4.º do RGPD, uma vez que determinam as finalidades e os meios de tratamento dos dados pessoais dos clientes bancários, seus respetivos representantes e beneficiários efetivos, que são os titulares destes dados.

O fundamento de licitude para este tratamento está previsto na alínea c) do n.º 1 do art. 6.º do RGPD, na medida em que o tratamento dos dados dos clientes bancários e/ou beneficiários efetivos é necessário para o *cumprimento de uma obrigação jurídica* a que a instituição financeira está sujeita.

9 Conforme alínea a) do n.º 1 do art. 24.º, n.º 1 do art. 25.º, e art. 26.º, sem prejuízo dos procedimentos complementares previstos no art. 27.º, todos da LBCFT.

Sublinhe-se que o tratamento dos dados realizado com base nesse fundamento de licitude considera os seguintes requisitos previstos na alínea c) do n.º 1 do art. 6.º do RGPD e no n.º 3 do mesmo artigo:

(i) O tratamento deve ser *necessário*: a necessidade existe na medida em que a lei assim a determine, pelo que a determinação da necessidade pressupõe uma interpretação prévia da lei[10];

(ii) O cumprimento de uma *obrigação jurídica* a que o responsável pelo tratamento esteja sujeito: a expressão obrigação jurídica deverá ser interpretada com o sentido de obrigação legal, pelo que o fundamento da alínea c) será sempre uma disposição legislativa e não uma disposição contratual. A obrigação legal tanto pode ter origem numa lei formal, como numa lei material[11], não sendo necessário uma lei específica para cada tratamento de dados concretos, ou seja, a mesma lei pode impor mais do que uma obrigação legal[12];

(iii) A obrigação jurídica deverá ser definida pelo *direito da UE*[13] ou

10 Menezes Cordeiro, António Barreto (2021), "Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019", p.113, Coord. António Barreto Menezes Cordeiro. Coimbra: Almedina. Ver ainda o Considerando 45 do RGPD.

11 Sobre os dois conceitos, ver Sousa, Miguel Teixeira de (2012), "Introdução ao estudo do Direito", p.145ss. Coimbra: Almedina.

12 Ibidem.

13 Para além da Diretiva AML, releva mencionar a Diretiva (UE) 2019/1153 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa à utilização de informações financeiras e de outro tipo para efeitos de prevenção, deteção, investigação ou repressão de determinadas infrações penais; a Diretiva (UE) 2018/1673 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativa ao combate ao branqueamento de capitais através do direito penal; o Regulamento (UE) 2018/1672 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo ao controlo das somas em dinheiro líquido que entram ou saem da União Europeia; a Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo; o Regulamento Delegado (UE) 2018/1108 da Comissão, de 7 de maio 2018, que estabelece normas técnicas de regulamentação sobre os critérios de nomeação e funcionamento dos pontos de contacto centrais dos emitentes de moeda eletrónica e dos prestadores de serviços de pagamento; a Diretiva (UE) 2016/2258 do Conselho, de 6 de dezembro de 2016, relativa ao acesso às informações anti-branqueamento de capitais por parte das autoridades fiscais; o Regulamento Delegado (UE) 2016/1675 da Comissão, de 14 de julho de 2016, que procede à identificação dos países terceiros de risco elevado que apresentam deficiências estratégicas; e o Regulamento (UE) 2015/847 do Parlamento Europeu e do Conselho, de 20 de maio 2015, que estabelece as informações sobre o ordenante que devem acompanhar as transferências de fundos.

pelo *direito de um Estado-Membro*[14]: a disposição legal que deverá ser cumprida pelo responsável pelo tratamento não pode ter origem no Direito de um Estado terceiro. Além disso, o direito da UE ou do Estado-Membro poderá especificar as condições gerais do RGPD que regem a legalidade do tratamento dos dados pessoais, estabelecer regras específicas para determinar os responsáveis pelo tratamento, o tipo de dados pessoais a tratar, os titulares dos dados em questão, as entidades a que os dados pessoais podem ser comunicados, os limites a que as finalidades do tratamento devem obedecer, os prazos de conservação e outras medidas destinadas a garantir a licitude e equidade do tratamento[15]; (iv) A obrigação jurídica deverá responder a um objetivo de *interesse público* e ser *proporcional* ao objetivo legítimo prosseguido: os dois elementos deste requisito não dizem respeito ao tratamento de dados *per se*, mas sim à delimitação das competências legislativas concretizadoras da UE e dos Estados-Membros, não podendo qualquer um destes extravasar a letra e o espírito do RGPD. Por exemplo, o n.º 3 do art. 57.º da LBCFT reconhece expressamente a prevenção e o combate ao branqueamento de capitais e ao financiamento do terrorismo como um domínio de proteção de um interesse público importante, incluindo no que se refere aos tratamentos de dados pessoais efetuados com base na LBCFT.

Assim, as instituições financeiras estão sujeitas aos deveres preventivos previstos na Diretiva AML, sem prejuízo da legislação aplicável à matéria em cada Estado-Membro, pelo que tratam os dados pessoais neste âmbito com base no cumprimento de uma obrigação jurídica, ao abrigo da alínea c) do n.º 1 do art. 6.º do RGPD.

14 É o caso, por exemplo, da LBCFT (Portugal), da Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (Espanha), do Décret n° 2020-118 du 12 février 2020, renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme (França), e do Decreto Legislativo 21 novembre 2007, n. 231, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (Itália).

15 Conforme o Considerando 45 do RGPD.

No caso da LBCFT, o n.º 1 do art. 57.º autoriza as instituições financeiras a realizar os tratamentos de dados pessoais necessários ao cumprimento dos deveres de prevenção do branqueamento de capitais e do financiamento do terrorismo. Esta é a finalidade exclusiva deste tratamento, não podendo tais dados ser posteriormente tratados para quaisquer outros fins, incluindo os fins comerciais, conforme prevê o n.º 2 do art. 57.º do mesmo diploma.

As categorias de dados pessoais a que as instituições financeiras estão autorizadas a tratar para cumprimento dos deveres preventivos são aquelas previstas no n.º 1 do art. 58.º da LBCFT, nomeadamente as seguintes:

> a) Dados de identificação e de contacto, bem como dados fiscais e profissionais e as qualificações do respetivo titular, incluindo os seguintes elementos: i) Elementos previstos no art. 24.º (mencionadas no capítulo anterior); ii) Elementos caracterizadores das atividades prosseguidas; iii) Elementos relativos aos cargos políticos ou públicos que sejam ou já tenham sido exercidos[16]; iv) Elementos relativos a relações de parentesco e de afinidade[17], bem como a relações societárias, comerciais,

16 As pessoas politicamente expostas, mais conhecidas na prática como PEP (Politically Exposed Person), bem como os membros da família e as pessoas conhecidas como estreitamente associadas às mesmas, impõem sobre as instituições financeiras um dever de diligência reforçada quanto à clientela previsto nos art. 20.º a 22.º da Diretiva AML. O n.º 9 do art. 3.º da Diretiva AML define que as «Pessoas politicamente expostas» são as "pessoas singulares a quem estão ou foram cometidas funções públicas proeminentes, a saber: a) Chefes de Estado, chefes de Governo, ministros, ministros-adjuntos e secretários de Estado; b) Deputados ou membros de órgãos legislativos similares; c) Membros dos órgãos de direção de partidos políticos; d) Membros dos supremos tribunais, dos tribunais constitucionais e de outros órgãos judiciais de alto nível cujas decisões não sejam passíveis de recurso, salvo em circunstâncias excecionais; e) Membros dos tribunais de contas e dos órgãos de administração dos bancos centrais; f) Embaixadores, encarregados de negócios e oficiais de alta patente das forças armadas; g) Membros de órgãos de administração, de direção ou de supervisão de empresas públicas; h) Diretores, diretores-adjuntos e membros do conselho de administração ou pessoas que exercem funções equivalentes numa organização internacional."

17 O n.º 10 do art. 3.º da Diretiva AML define que os «Membros da família» incluem "a) O cônjuge, ou pessoa equiparada ao cônjuge, de pessoa politicamente exposta; b) Os filhos e respetivos cônjuges, ou pessoas equiparadas a cônjuge, de pessoa politicamente exposta; c) Os pais de pessoa politicamente exposta;", e o n.º 11 do mesmo artigo define que «Pessoas conhecidas como estreitamente associadas» podem ser "a) Qualquer pessoa singular que seja notoriamente conhecida por ter a propriedade efetiva conjunta de pessoas coletivas e de centros de interesses coletivos sem personalidade jurídica, ou por manter outro tipo de relações comerciais estreitas com pessoa politicamente exposta; b) Qualquer pessoa singular que tenha a propriedade efetiva de uma pessoa coletiva ou de um centro de interesses coletivos sem

profissionais ou sociais relevantes;

b) Dados financeiros e bancários, incluindo os relativos: i) Ao crédito e à solvabilidade dos respetivos titulares; ii) Aos rendimentos ou outros bens relacionados com os titulares dos dados;

c) Informação sobre a finalidade e a natureza da relação de negócio;

d) Informação sobre a origem e o destino dos fundos ou outros bens movimentados no âmbito de uma relação de negócio ou da realização de uma transação ocasional;

e) Informação sobre os demais elementos caracterizadores de todas as operações realizadas no decurso de uma relação de negócio ou no contexto de uma transação ocasional;

f) Informação sobre suspeitas de infrações penais[18], da prática de contraordenações ou de outras atividades ilícitas, incluindo a seguinte: i) Informação sobre comunicações de operações suspeitas efetuadas pela própria entidade obrigada ou por outras entidades comunicantes; ii) Informação sobre outras participações efetuadas às autoridades competentes; iii) Informação disponibilizada pelas autoridades competentes;

g) Informação sobre decisões que apliquem penas, medidas de segurança, coimas, sanções acessórias ou outras sanções pela prática dos atos a que se refere a alínea anterior.

Portanto, o tratamento dos dados pessoais no âmbito da prevenção ao branqueamento de capitais será lícito desde que a instituição financeira realize esse tratamento com base no cumprimento de uma obrigação jurídica prevista no direito da UE ou no direito de um Estado-membro a que a instituição financeira esteja sujeita.

---

personalidade jurídica notoriamente conhecidos como tendo sido constituídos em benefício de facto da pessoa politicamente exposta."

18 A proteção dos dados das pessoas singulares no que diz respeito ao tratamento, pelas autoridades competentes, para efeitos de prevenção, investigação, deteção ou repressão de infrações penais, é regulado pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Em virtude disto, o RGPD exclui, através de seu art. 2.º, n.º 2, alínea d), o tratamento de dados pessoais para estes efeitos do seu âmbito de aplicação material.

3. Os conflitos entre os princípios do RGPD e os deveres de prevenção ao branqueamento de capitais e financiamento do terrorismo

É fundamental que o regime AML esteja alinhado com a plena observância do quadro legal existente para a proteção de dados, na medida em que certos aspetos da aplicação do regime AML envolvem a recolha, a análise, o armazenamento e a partilha de dados pessoais.

Para tentar encontrar as respostas a tais preocupações opostas, as Diretivas, regulamentos, leis e avisos setoriais normalmente limitam-se a fazer referências genéricas à proteção de dados, questionando-se a proporcionalidade dos meios e as finalidades dos dados exigidos para combater o branqueamento de capitais e outros tipos de crimes[19].

As autoridades e/ou organismos independentes, nomeadamente os 4 citados a seguir, tentam alinhar os dois regimes jurídicos sob estudo: Comité Europeu para a Proteção de Dados **(**CEPD**)** ou *European Data Protection Board* **(**EDPB**)**[20], Autoridade Europeia para a Proteção de Dados (AEPD) ou *European Data Protection Supervisor* **(**EDPS**)**[21], Grupo de Ação Financeira

---

19 Machado, Miguel (2020), "Deveres antibranqueamento de capitais: De onde vieram, quais são e como vão evoluir (do "4G" ao "5G")", Novos Estudos sobre Law Enforcement, Compliance e Direito Penal, Coord. Maria Fernanda Palma et al, pp. 316. Coimbra: Almedina.

20 Considerando os 4 seguintes documentos:

(i) Declaração sobre a proteção dos dados pessoais tratados no quadro da prevenção do branqueamento de capitais e do financiamento do terrorismo, adotada em 15 de dezembro de 2020 pelo CEPD. Disponível em: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_20201215_aml_actionplan_pt.pdf>

(ii) Letter from Andrea Jelinek (Chair of the EDPB) to Ms. Mairead McGuiness (European Commissioner for Financial services, financial stability and Capital Markets Union) and Mr. Didier Reynders (European Commissioner for Justice), sent on 19 May 2021. Disponível em: <https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf>

(iii) Guidelines 10/2020 on restrictions under Article 23 GDPR, adotadas em 13 de outubro de 2021 pelo CEPD. Disponível em: <https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf>

(iv) Parecer 14/2011 sobre questões de proteção dos dados ligadas à prevenção do branqueamento de capitais e ao financiamento do terrorismo, adotado em 13 de junho de 2011 pelo GT29. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_pt.pdf>

21 Considerando os 2 seguintes documentos:

(i) Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, adotada em 23 de julho de 2020 pelo EDPS. Disponível em: <20-07-23_edps_aml_opinion_en.pdf> (europa.eu), e

(GAFI) ou *Financial Action Task Force* (FATF)[22], e Autoridade Bancária Europeia ou *European Banking Authority* (EBA)[23].

De um modo geral, estas diretrizes, opiniões, recomendações e pareceres sublinham que os procedimentos adotados para cumprimento dos deveres preventivos do branqueamento de capitais devem ter em consideração a proteção dos dados das pessoas singulares envolvidas, mas nem todos destes documentos possuem termos que efetivamente esclarecem as dúvidas que surgem no cotidiano das instituições financeiras.

Na prática, a avaliação dos conflitos é casuística, pelo que requer uma análise cuidadosa que pondere os princípios do RGPD e os deveres preventivos de branqueamento de capitais a que as instituições financeiras estão obrigadas.

Sem prejuízo da existência de outros conflitos entre os princípios do RGPD e o regime AML, o presente trabalho estudará três conflitos comuns neste âmbito, designadamente (i) o princípio da transparência contra o dever de não divulgação das informações, (ii) o princípio da minimização dos dados

---

(ii) Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals, adotada em 22 de setembro de 2021 pelo EDPS. Disponível em: <https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf>

22 Considerando os 3 seguintes documentos:

(i) International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, adotado em 2012 e atualizado em outubro de 2021 pela FATF. Disponível em: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

(ii) Private Sector Information Sharing, adotado em novembro de 2017 pela FATF. Disponível em: Private-Sector-Information-Sharing.pdf (fatf-gafi.org), e (iii) Stocktake on Data Pooling, Collaborative Analytics and Data Protection, adotado em julho de 2021 pela FATF. Disponível em: <https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborativeanalytics-data-protection.html>

23 Considerando os 2 seguintes documentos:

(i) Orientações relativas aos Fatores de Risco de BC/FT, adotadas em 01 de março de 2021 pela EBA. Disponível em: <https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/revised-guidelines-on-ml-tf-risk-factors#pane-new-7bdd87fb-e02f-492a-99d6-129449e3cf9d> e

(ii) Draft on Regulatory Technical Standards under Article 9a (1) and (3) of Regulation (EU) n. 1093/2010 setting up an AML/CFT central database and specifying the materiality of weaknesses, the type of information collected, the practical implementation of the information collection and the analysis and dissemination of the information contained therein, adotadas em 06 de maio de 2021 pela EBA. Disponível em: <https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countering-financing-terrorism/regulatory-technical-standards-central-database-amlcft-eu>

contra o dever de diligência quanto à clientela e (iii) o princípio da limitação da conservação dos dados contra o dever de conservação dos dados.

3.1 Princípio da transparência contra o dever de não divulgação das informações

O art. 5.º do RGPD consagra os princípios relativos ao tratamento de dados pessoais, e prevê na alínea a) do n.º 1 deste art. que os dados pessoais são "*objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados*".

A transparência é um dos elementos há muito consagrados no direito da UE. Trata-se de criar confiança nos processos que afetam os cidadãos, fazendo com que estes compreendam e, se necessário, se oponham a esses processos. Trata-se igualmente de uma expressão do princípio da lealdade em relação ao tratamento dos dados pessoais enunciado no art. 8.º da Carta dos Direitos Fundamentais da UE[24].

Nos termos do RGPD, a transparência é uma obrigação abrangente[25], aplicável aos três seguintes domínios centrais:

(i) O fornecimento de informações aos titulares dos dados relacionado com o tratamento leal: por exemplo, a identidade e os contactos do

24 Sobre este princípio, ver também as Orientações relativas à transparência na aceção do Regulamento 2016/679, adotadas em 29 de novembro de 2017 pelo GT29. Disponível em: <https://ec.europa.eu/newsroom/article29/items/622227/en>

25 O Considerando 39 do RGPD prevê que "O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados. As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento. (...)".

responsável pelo tratamento, os contactos do encarregado da proteção de dados, as finalidades do tratamento, o fundamento de licitude para o tratamento, os destinatários ou categorias de destinatários dos dados pessoais, os prazos de conservação, as regras de transferência de dados para um país terceiro, se for o caso, de entre outras informações que possam interessar ao titular dos dados;

(ii) De que forma os responsáveis pelo tratamento comunicam com os titulares dos dados em relação aos direitos destes ao abrigo do RGPD: é suposto o responsável pelo tratamento fornecer ao titular as informações acima e qualquer comunicação de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, devendo tais informações ser prestadas por escrito ou por outros meios, incluindo, se for o caso, por meios eletrónicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios; e

(iii) De que forma os responsáveis pelo tratamento facilitam o exercício dos direitos dos titulares dos dados: o responsável pelo tratamento deve facilitar o exercício dos direitos do titular dos dados previstos nos art. 15.º a 22.º do RGPD, nomeadamente os direitos de acesso, retificação, apagamento, limitação do tratamento, portabilidade, oposição e não sujeição à decisões individuais automatizadas, incluindo definição de perfis.

Decorre também do n.º 2 do art. 5.º do RGPD que o responsável pelo tratamento tem sempre de poder comprovar que os dados pessoais são tratados de forma transparente em relação ao titular dos dados. Associado a isto, o princípio da responsabilidade exige a transparência das operações de tratamento para que os responsáveis pelo tratamento possam comprovar o cumprimento das suas obrigações nos termos do RGPD.

Assim, o conceito de transparência no RGPD, não sendo um conceito legalista, está centrado no utilizador e é concretizado através de requisitos práticos específicos que recaem sobre os responsáveis pelo tratamento e os subcontratantes em diversos artigos. Os requisitos práticos (em matéria de

informação) encontram-se definidos nos art. 12.º a 14.º do RGPD. Contudo, a qualidade, a acessibilidade e a compreensibilidade das informações são tão importantes como o conteúdo efetivo das informações em matéria de transparência, que devem ser fornecidas aos titulares dos dados.

O n.º 3 do art. 41.º da Diretiva AML (refletido no n.º 2 do art. 59.º da LBCFT) prevê que as instituições financeiras, antes de estabelecerem uma relação de negócio ou de efetuarem uma transação ocasional, devem fornecer aos novos clientes as informações exigidas no art. 13.º do RGPD. Essas informações incluem, em especial, um aviso geral quanto às obrigações legais das instituições financeiras em matéria de tratamento de dados pessoais para efeitos da prevenção do branqueamento de capitais e do financiamento do terrorismo. Para efeitos de cumprimento desta disposição legal, é prática comum entre os bancos constar este aviso geral na ficha de abertura de conta, remetendo as informações exigidas no art. 13.º do RGPD para as condições gerais de abertura de conta e/ou para a política de proteção de dados pessoais em vigor.

No entanto, em sentido contrário ao princípio da transparência consagrado pelo RGPD, o art. 39.º da Diretiva AML estabelece o *dever de não divulgação*[26], em que as entidades obrigadas, seus respetivos administradores e funcionários não podem divulgar ao cliente em causa, nem a terceiros, o facto de estarem a ser, irem ser ou terem sido transmitidas informações às Unidades de Informação Financeira (UIF)[27], designadamente as informações relativas ao conhecimento ou suspeita de que os fundos provêm de atividades criminosas,

26 Previsto no art. 54.º da LBCFT.

27 Entidades dos Estados-Membros que devem ser operacionalmente independentes e autónomas para recolher e analisar a informação que recebem com o objetivo de estabelecer ligações entre as operações suspeitas e as atividades criminosas a elas subjacentes, a fim de prevenir e combater o branqueamento de capitais e o financiamento do terrorismo. A alínea jj) do n.º 1 do art. 2.º da LBCFT define a UIF como a "unidade central nacional com competência para: i) Receber, analisar e difundir a informação resultante de comunicações de operações suspeitas nos termos da presente lei e de outras fontes quando relativas a atividades criminosas de que provenham fundos ou outros bens; e ii) Cooperar com as congéneres internacionais e as demais entidades competentes para a prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo". Em Portugal, a UIF está incluída na orgânica da Polícia Judiciária através da alínea b) do n.º 2 do art. 18.º do Decreto-Lei n.º 137/2019, de 13 de setembro, que aprovou a nova estrutura organizacional desta Polícia, como um serviço central diretamente dependente do diretor nacional. As suas competências estão descritas no art. 27.º do Decreto-Lei n.º 137/2019, de 13 de setembro, e no art. 82.º da LBCFT.

nem que está a ser ou pode vir a ser efetuada uma análise sobre branqueamento de capitais ou financiamento do terrorismo.

A divulgação da transmissão destas informações enviadas às UIF pode ser realizada junto das autoridades competentes e até entre as instituições financeiras, sendo ainda permitida para efeitos de aplicação da lei. O n.º 6 do art. 39.º da Diretiva AML autoriza as instituições financeiras a tentarem dissuadir um cliente de realizar uma atividade ilegal, sem que isso constitua uma violação ao dever de não divulgação, mas o cliente e seus respetivos representantes não podem tomar conhecimento de que estão a ser investigados com base no regime AML.

A não divulgação ao titular dos dados da transmissão destas informações entre as instituições financeiras é ancorada pela alínea b) do n.º 5 do art. 14.º do RGPD, uma vez que comunicar este tratamento de dados ao titular prejudicaria a obtenção dos objetivos desse tratamento (investigação da prática de branqueamento de capitais ou financiamento do terrorismo).

As Orientações relativas à transparência na aceção do RGPD, adotadas em 29 de novembro de 2017 pelo GT29, exemplificam o tema sob estudo através do seguinte caso prático[28]:

> "O Banco A está sujeito a uma obrigação ao abrigo da legislação relativa ao combate ao branqueamento de capitais de comunicar qualquer atividade suspeita relacionada com contas abertas no banco à autoridade responsável pela aplicação da lei competente no domínio financeiro. O Banco A recebe informações do Banco B (noutro Estado-Membro) de que o titular de uma conta deu instruções para transferir dinheiro para outra conta aberta no Banco A e que a operação parece suspeita. O Banco A transmite estes dados relativos ao titular da conta e às atividades suspeitas à autoridade responsável pela aplicação da lei competente no domínio financeiro. A legislação de combate ao branqueamento de capitais em causa qualifica como infração penal o facto de um banco que comunica estas informações «alertar» o titular da conta para a possibilidade de estar sujeito a investigações regulamentares. Nesta situação, o artigo 14.º, n.º 5, alínea b), é aplicável porque fornecer ao titular dos dados (o titular da conta no Banco A) as informações relativas ao artigo 14.º sobre o tratamento dos

28 Conforme p.37 das Orientações relativas à transparência na aceção do Regulamento 2016/679, adotadas em 29 de novembro de 2017 pelo GT29. Disponível em: <https://ec.europa.eu/newsroom/article29/items/622227/en>

> dados pessoais do titular da conta recebidos do Banco A iria prejudicar gravemente os objetivos da legislação, que inclui a prevenção deste tipo de «alertas». Contudo, quando abrem uma conta, todos os titulares de conta clientes do Banco A devem receber informações gerais acerca da possibilidade de os seus dados pessoais poderem vir a ser tratados para fins de combate ao branqueamento de capitais*"*.

Em decorrência do dever de não divulgação a que as instituições financeiras estão obrigadas, o n.º 4 do art. 41.º da Diretiva AML estabelece que os Estados-Membros adotam medidas legislativas que restrinjam, total ou parcialmente, o direito de acesso pelo titular dos dados aos dados pessoais que lhe dizem respeito, na medida em que essa restrição total ou parcial constitua uma medida necessária e proporcionada numa sociedade democrática e tenha devidamente em conta os legítimos interesses da pessoa em causa (i) para que a entidade obrigada ou a autoridade nacional competente possa desempenhar cabalmente as suas funções para efeitos da Diretiva AML, ou (ii) para evitar que se constitua um entrave aos inquéritos, análises, investigações ou procedimentos oficiais ou legais e garantir que não seja comprometida a prevenção, investigação e deteção do branqueamento de capitais e do financiamento do terrorismo.

No RGPD, a alínea d) do n.º 1 do art. 23.º estabelece que, para assegurar a prevenção, a investigação, a deteção ou a repressão de infrações penais, o direito da UE ou dos Estados-Membros pode limitar o alcance das obrigações e dos direitos previstos nos art. 12.º a 22.º e no art. 34.º, bem como no art. 5.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática[29].

---

29 O Considerando 19 do RGPD reconhece expressamente a importância dessa possibilidade de limitação na luta contra o branqueamento de capitais: "(...) Nos casos em que o tratamento de dados pessoais por organismos privados fica abrangido pelo presente regulamento, este deverá prever a possibilidade de os Estados-Membros restringirem legalmente, em determinadas condições, certas obrigações e direitos, quando tal restrição constitua medida necessária e proporcionada, numa sociedade democrática, para salvaguardar interesses específicos importantes, incluindo a segurança pública e a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Tal possibilidade é importante, por exemplo, no quadro da luta contra o branqueamento de capitais ou das atividades dos laboratórios de polícia científica".

A alínea h) do n.º 2 do art. 23.º do RGPD complementa que estas medidas legislativas incluem, quando for relevante, disposições explícitas relativas ao direito dos titulares dos dados a serem informados da limitação, a menos que tal possa prejudicar o objetivo da limitação.

No ordenamento jurídico português, a limitação do direito de acesso do titular dos dados no âmbito da prevenção, deteção, investigação ou repressão de infrações penais se encontra refletida no art. 16.º da Lei n.º 59/2019, de 08 de agosto.

No âmbito específico da prevenção ao branqueamento de capitais e financiamento do terrorismo, esta limitação se encontra refletida no n.º 2 do art. 60.º da LBCFT, o qual estabelece que o direito de acesso aos dados pessoais pelo respetivo titular é negado nas situações previstas no n.º 1 do art. 54.º da LBCFT. É com base neste artigo que as instituições financeiras, bem como os membros dos respetivos órgãos sociais, os que nelas exerçam funções de direção, de gerência ou de chefia, os seus empregados, os mandatários e outras pessoas que lhes prestem serviço a título permanente, temporário ou ocasional, não podem revelar ao cliente ou a terceiros:

a) Que foram, estão a ser ou irão ser transmitidas as comunicações de operações suspeitas, comunicações sistemáticas de operações, comunicações realizadas no âmbito do dever de abstenção e as comunicações realizadas no âmbito do dever de colaboração com o Departamento Central de Investigação e Ação Penal da Procuradoria-Geral da República (DCIAP), a UIF, as demais autoridades judiciárias e policiais, as autoridades setoriais e a Autoridade Tributária e Aduaneira;

b) Quaisquer informações relacionadas com as comunicações acima, independentemente de elas decorrerem de análises internas da instituição financeira ou de pedidos efetuados pelas autoridades judiciárias, policiais ou setoriais;

c) Que se encontra ou possa vir a encontrar-se em curso uma investigação ou inquérito criminal, bem como quaisquer outras investigações, inquéritos, averiguações, análises ou procedimentos legais a conduzir pelas autoridades judiciárias, policiais ou setoriais;

d) Quaisquer outras informações ou análises, de foro ou interno ou externo, sempre que disso dependa: i) O cabal exercício das funções conferidas pela LBCFT às instituições financeiras e às autoridades judiciárias, policiais e setoriais; e ii) A preservação de quaisquer investigações, inquéritos, averiguações, análises ou procedimentos legais e, no geral, a prevenção, investigação e deteção do branqueamento de capitais e do financiamento do terrorismo.

Importa sublinhar que as hipóteses acima, que permitem às instituições financeiras negar o acesso aos dados pessoais requerido pelo titular dos dados, não prejudicam o direito de apresentação de queixa ou reclamação à Comissão Nacional de Proteção de Dados (CNPD) pelo titular dos dados, o recurso aos meios de tutela administrativa e o direito que tem o mesmo a obter reparação pelos danos sofridos, ao abrigo do art. 34.º da Lei n.º 58/2019, de 8 de agosto. Além disso, não prejudicam a verificação pela CNPD, oficiosamente ou a pedido do titular dos dados, da licitude do tratamento dos dados, bem como da informação àquele titular de que foram efetuadas todas as verificações necessárias e de que o tratamento de dados em causa reveste natureza lícita ou ilícita[30].

Em 13 de outubro de 2021, o CEPD adotou as *Guidelines 10/2020 on restrictions under Article 23 GDPR*[31], que visam fornecer orientações quanto à aplicação do art. 23.º do RGPD através de uma análise completa dos critérios para aplicar as restrições, as avaliações que têm de ser observadas, como os titulares dos dados podem exercer os seus direitos uma vez levantada a restrição e as consequências para as violações deste artigo.

O parágrafo n.º 24 da secção 3.3.2 das *Guidelines 10/2020 on restrictions under Article 23* GDPR, em comentário à alínea d) do n.º 1 do art. 23.º do

30 Sobre o recurso ao mecanismo da consulta prévia estabelecida no art. 36.º do RGPD, pelas instituições financeiras, para resolver o vácuo entre os princípios do RGPD e a abordagem baseada no risco do regime AML, ver Maxwell, Winston (2021), "The GDPR and Private Sector Measures to Detect Criminal Activity", Revue des Affaires Européennes - Law and European Affairs, p.24. Disponível em: <https://ssrn.com/abstract=3964066>

31 Guidelines 10/2020 on restrictions under Article 23 GDPR, adotadas em 13 de outubro de 2021 pelo CEPD. Disponível em: <https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf>

RGPD, considera que em certos casos o fornecimento de informações aos titulares dos dados que estão a ser investigados pode comprometer o sucesso dessa investigação, pelo que a restrição do direito à informação ou de outros direitos do titular dos dados pode ser necessária. O parágrafo n.º 24 considera expressamente que isto é relevante, por exemplo, no âmbito do combate ao branqueamento de capitais.

No entanto, o parágrafo n.º 25 pondera que as informações omitidas devem, em conformidade com a jurisprudência do Tribunal de Justiça da União Europeia (TJUE)[32], ser fornecidas uma vez e se já não for possível pôr em risco a investigação em curso. Segundo o parágrafo n.º 25, isto significa que deve ser dado um aviso específico de proteção de dados (feito à medida) ao titular dos dados o mais rapidamente possível, indicando os diferentes direitos, tais como acesso e retificação.

Em comentário à alínea h) do n.º 2 do art. 23.º do RGPD, os parágrafos n.ºs 64 a 67 da secção 4.7 das *Guidelines 10/2020 on restrictions under Article 23* GDPR, estabelecem critérios que poderão ser úteis às instituições financeiras que precisam apresentar uma resposta fundamentada a um pedido de acesso a dados pessoais em que o titular é uma pessoa que se encontra sob investigação. As orientações previstas nestes parágrafos entendem que os titulares dos dados devem, em regra, ser informados sobre a restrição ao seu direito à informação, sendo suficiente um aviso geral de proteção de dados para o efeito.

Nas fases muito preliminares de uma investigação, se o titular dos dados em causa solicitar informações sobre se está a ser investigado, o responsável pelo tratamento poderá decidir não conceder essas informações nesse momento – se esta restrição for lícita e estritamente necessária no caso específico para o que seria prejudicial ao objetivo da restrição.

Numa fase posterior, tal como após a conclusão da fase preliminar da investigação ou inquérito, os titulares dos dados em causa devem receber uma notificação específica de proteção de dados. Ainda é possível, nesta fase, que certos direitos continuem a ser restringidos, tais como o direito de acesso à informação sobre a abertura de uma investigação. Segundo os parágrafos

32 Opinion 1/15 of the CJEU (Grand Chamber) on the Draft PNR Agreement between Canada and the European Union, 26 July 2017, ECLI:EU:C:2017:592.

n.ºs 64 a 67, este facto deve ser indicado no aviso de proteção de dados, juntamente com a indicação de um período em que os direitos serão plenamente restabelecidos, se possível.

Em síntese, nos casos em que o fornecimento de informações ao titular dos dados prejudicar os objetivos do tratamento previstos no regime de prevenção ao branqueamento de capitais, o princípio da transparência consagrado pelo RGPD será mitigado pelo dever de não divulgação a que as instituições financeiras estão obrigadas, sem prejuízo de as restrições ao direito de acesso aos dados pelo titular serem levantadas numa fase posterior em que o fornecimento de informações não prejudique os objetivos do tratamento previstos no regime AML.

3.2 Princípio da minimização dos dados contra o Dever de Diligência quanto à clientela

A alínea c) do n.º 1 do art. 5.º do RGPD consagra o princípio da minimização dos dados ao estabelecer que os dados pessoais são "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados". Este princípio é composto pelos três seguintes pilares, que visam propósitos distintos, apesar de dificilmente autonomizáveis (em especial os dois primeiros)[33]:

(i) Adequação: impõe aos responsáveis pelo tratamento que circunscrevam a recolha e demais tratamentos a dados pessoais que se enquadrem nas finalidades prosseguidas. Os dados não relacionados ou inapropriados encontram-se, em princípio, excluídos.
(ii) Pertinência: este pilar circunscreve as atividades dos responsáveis a tratamentos que possam contribuir para a prossecução dessas finalidades. O termo "*relevant*", empregue na versão inglesa do RGPD, é mais feliz que o termo "pertinentes", empregue na versão portuguesa do RGPD.
(iii) Limitação: os dados pessoais são limitados ao que é necessário

33 Menezes Cordeiro, António Barreto (2021), "Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019", p.105, Coord. António Barreto Menezes Cordeiro. Coimbra: Almedina.

> relativamente às finalidades para as quais são tratados. Este pilar tem especial ligação com o princípio da limitação da conservação previsto na alínea b) do n.º 1 do art. 5.º do RGPD, que estabelece que os dados pessoais são "*recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades*".

Assim, o princípio da minimização dos dados tem por base a redução do tratamento dos dados pessoais ao mínimo necessário, pelo que o tratamento apenas será juridicamente aceitável se não existirem métodos alternativos menos intrusivos dos direitos dos titulares, tais como a anonimização prevista na alínea a) do n.º 1 do art. 32.º do RGPD, e a pseudonimização prevista no n.º 1 do art. 32.º do RGPD[34].

O n.º 1 do art. 41.º da Diretiva AML prevê que o tratamento de dados pessoais ao abrigo da mesma está sujeito ao cumprimento do RGPD, conforme transposição da Diretiva AML para o direito nacional, e o n.º 2 do mesmo artigo prevê que os dados pessoais são tratados pelas entidades obrigadas (como é caso das instituições financeiras) com base na Diretiva AML apenas para efeitos da prevenção do branqueamento de capitais e do financiamento do terrorismo, não podendo ser posteriormente tratados de forma incompatível com essas finalidades. Para o efeito, o n.º 2 do art. 41.º proíbe expressamente o tratamento posterior de dados pessoais com base na Diretiva AML para quaisquer outros fins, nomeadamente fins comerciais.

As medidas de luta contra o branqueamento de capitais incluem obrigações muito amplas e de grande alcance impostas às instituições financeiras, designadamente as obrigações de identificar os seus clientes, controlar as transações efetuadas através dos seus serviços e comunicar transações suspeitas, conforme se verifica através do n.º 1 do art. 13.º da Diretiva AML e dos art. 23.º e 24.º da LBCFT.

---

34 O Information Commissioner's Office (ICO), autoridade de controlo britânica no âmbito da proteção de dados, disponibiliza em seu site breves e interessantes orientações sobre o princípio da minimização dos dados, com exemplos práticos em diversos cenários de tratamento. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/.

O cumprimento do dever de identificação e diligência pelas instituições financeiras, é realizado através do tratamento de diversos tipos de dados pessoais, podendo a diligência ser reforçada conforme o risco que o cliente representa ao abrigo do regime AML. É difícil conciliar os deveres deste regime com o princípio da minimização dos dados, pois há fatores de risco que podem alterar a interpretação sobre os dados que são adequados, pertinentes e limitados ao que é necessário para prevenir o branqueamento de capitais e o financiamento do terrorismo no âmbito da abertura de uma conta bancária, bem como no âmbito da manutenção desta relação de negócio.

Tendo em consideração essas dificuldades, as autoridades e/ou organismos independentes tentam alinhar os dois regimes jurídicos. O Grupo de trabalho do art. 29.º para a Proteção dos Dados (GT29), grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD), adotou o Parecer 14/2011 sobre questões de proteção dos dados ligadas à prevenção do branqueamento de capitais e ao financiamento do terrorismo[35], sendo que, através deste Parecer, divulgou alguns entendimentos que relevam ao princípio da minimização de dados, designadamente os que seguem abaixo:

(i) A recolha sistemática de dados ao abrigo das obrigações de identificação e diligência quanto à clientela não deve ser vista como uma finalidade em si mesma, mas aplicada ao risco envolvido e deve ter em conta o princípio da minimização de dados. O requisito de fornecer dados relacionados com a identificação e diligência quanto à clientela deve sempre depender de uma avaliação de risco predefinida que tenha em conta diferentes fatores, tais como a situação do cliente, a natureza das transações, o produto financeiro ou os movimentos financeiros envolvidos;

(ii) O responsável pelo tratamento tem a obrigação de avaliar,

35 Parecer 14/2011 sobre questões de proteção dos dados ligadas à prevenção do branqueamento de capitais e ao financiamento do terrorismo, adotado em 13 de junho de 2011 pelo GT29. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_pt.pdf>

periodicamente, a exatidão dos dados, a necessidade de armazenar avaliações de risco mais antigas e a necessidade de continuar o tratamento de dados mais antigos relativos ao dever de identificação e diligência;
(iii) A recolha e subsequente tratamento de dados sensíveis para efeitos de prevenção do branqueamento de capitais é proibida, a menos que a necessidade desse perfil possa ser provada pela instituição financeira e desde que os legisladores e entidades reguladoras tenham também especificado salvaguardas adequadas, que devem ter como objetivo evitar a interpretação arbitrária das obrigações de identificação e diligência quanto à clientela pelas instituições financeiras. A simples referência a uma exceção legal ou a uma obrigação legal de perfilar é claramente inadequada, uma vez que não acrescenta quaisquer salvaguardas para processar dados sensíveis.

No dia 19 de maio de 2021, o CEPD, atento à necessidade de harmonizar o princípio da minimização de dados com o regime AML, apresentou as seguintes recomendações[36]:

(i) O regime de prevenção do branqueamento de capitais deve especificar o que é necessário e proporcional para cumprir as suas obrigações. Do ponto de vista da proteção de dados, é crucial inserir termos em cada obrigação deste regime que clarifiquem se os dados pessoais necessários para cumprir uma obrigação específica devem (apenas) ser recolhidos junto da pessoa em causa ou se outras fontes (por exemplo, entidades terceiras, públicas ou privadas) podem ou devem ser utilizadas. É igualmente necessário especificar, se for o caso, que tipos de categorias especiais de dados pessoais e/ou dados pessoais relativos a condenações e infrações penais poderão ou deverão ser tratados para cumprir essa obrigação específica;

36 Letter from Andrea Jelinek (Chair of the EDPB) to Ms. Mairead McGuiness (European Commissioner for Financial services, financial stability and Capital Markets Union) and Mr. Didier Reynders (European Commissioner for Justice), sent on 19 May 2021. Disponível em: <https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf>

(ii) Deve ser evitado o comportamento defensivo de entidades obrigadas (como é o caso das instituições financeiras), que as leva a enviar grandes quantidades de suspeitas não relevantes, gerando um elevado número de falsos positivos[37];

(iii) A nova legislação no âmbito AML deve conter, explicitamente, requisitos no sentido de que apenas os dados exatos e relevantes podem ser utilizados para os reportes. Estes requisitos devem também proibir a inclusão de dados pessoais relacionados com condenações penais e infrações que não sejam ligadas ao branqueamento de capitais ou ao financiamento do terrorismo.

Portanto, o princípio da minimização de dados consagrado no RGPD e o dever de diligência quanto à clientela previsto no regime AML devem ser abordados de forma equilibrada que, numa perspetiva de prevenção e combate a estas atividades criminosas, tenha em consideração os dados pessoais que são efetivamente adequados, pertinentes e limitados ao que é necessário para esta finalidade (cumprimento de deveres AML).

3.3. Princípio da limitação da conservação dos dados contra o Dever de conservação dos dados

A alínea e) do n.º 1 do art. 5.º do RGPD consagra o princípio da limitação da conservação dos dados ao estabelecer que os dados pessoais são "*conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais*

37 No contexto em causa, "falsos positivos" são reportes de transações baseados em conclusões equivocadas. Para seguir os padrões de KYC, as empresas devem proceder a uma monitorização contínua das suas relações de negócio para assegurar que os perfis de risco não mudaram de uma forma que exponha a empresa ao não cumprimento dos deveres antibranqueamento de capitais e aos danos reputacionais, mas isto é dispendioso para as instituições financeiras, na medida em que as soluções existentes produzem um grande número de falsos positivos devido à sua dependência de pesquisas manuais em múltiplas bases de dados que são difíceis de auditar. Os falsos positivos podem surgir porque pode haver milhares de nomes ou pontos de dados a combinar, produzindo centenas de resultados. Todos esses resultados têm de ser revistos manualmente para ver se são "falsos positivos" ou não. Ainda sobre o tema, ver o Glossário de Risco e Compliance da Dow Jones, disponível em: <https://www.dowjones.com/professional/risk/glossary/know-your-customer/false-positives/>

são tratados".

Com o término do período necessário para a prossecução dos fins determinados, os dados devem ser, o quanto antes, apagados. Cabe ao responsável pelo tratamento fixar os prazos para o apagamento ou para a revisão periódica da sua conservação, de forma a assegurar que os dados pessoais sejam mantidos apenas durante o período indispensável[38].

O art. 21.º da Lei n.º 58/2019, de 8 de agosto, densifica esta obrigação e prevê que o prazo de conservação de dados pessoais é o que estiver fixado por norma legal ou regulamentar ou, na falta desta, o que se revele necessário para a prossecução da finalidade. O n.º 3 deste artigo dispõe que quando os dados pessoais sejam necessários para o responsável pelo tratamento ou o subcontratante poderem comprovar o cumprimento de obrigações contratuais ou de outra natureza, os mesmos podem ser conservados enquanto não decorrer o prazo de prescrição dos direitos correspetivos. Cessada a finalidade que motivou o tratamento, inicial ou posterior, de dados pessoais, o responsável pelo tratamento deve proceder à sua destruição ou anonimização (n.º 4 do art. 21.º). Por fim, o n.º 5 deste artigo prevê que nos casos em que existe um prazo de conservação de dados imposto por lei, o direito ao apagamento previsto no art. 17.º do RGPD só pode ser exercido após o fim desse prazo.

A CNPD, através do Parecer 20/2018, adotado no dia 2 de maio de 2018, sobre a Proposta de Lei n.º 120/XIII/3.ª (Gov)[39], que acabou por ser adotada na Lei n.º 58/2019, de 8 de agosto, entendeu que o art. 21.º desvirtuou por completo o princípio da limitação da conservação dos dados, apresentando as seguintes críticas:

(i) Independentemente da definição de um prazo máximo de conservação, os dados pessoais devem ser eliminados ou tornados anónimos assim que estiver cumprida, no caso concreto, a finalidade do tratamento. A aplicação deste princípio não prejudica, obviamente, a necessidade de

38 Menezes Cordeiro, António Barreto (2021), "Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019", p.106, Coord. António Barreto Menezes Cordeiro. Coimbra: Almedina.

39 Parecer 20/2018, adotado no dia 02 de maio de 2018 pela Comissão Nacional de Proteção de Dados (CNPD), sobre a Proposta de Lei n.º 120/XIII/3.ª (Gov). Disponível em: https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2018&type=4&ent=

conservar dados quando haja lei que a tal obrigue. Porém, mesmo nestas circunstâncias, só devem ser conservados os dados que forem necessários para o cumprimento da obrigação legal e não outros que para o efeito não sejam necessários. Será o exemplo clássico de um tratamento de dados de gestão de clientes, em que é obrigatório a empresa manter os dados de faturação do cliente por um período de 10 anos para fins fiscais, daí não decorrendo o dever de conservar outros dados relativos ao cliente (tais como contactos, idade, consumos detalhados, interesses e preferências) se a relação contratual for terminada ao fim de dois anos;

(ii) O RGPD só admite ao Estado-Membro legislar dentro dos parâmetros definidos pelo Regulamento, quanto à conservação de dados durante períodos mais longos, quando em causa esteja a prossecução exclusiva de fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos. Contudo, outras vertentes foram reguladas de forma incompreensível nos n.ºs 1 e 4 do art. 21.º, o que é por si só violador do direito da UE, uma vez que o legislador nacional está adstrito a disciplinar apenas as matérias permitidas pelo Regulamento da UE;

(iii) O n.º 2 do art. 21.º dispensou com grande amplitude a limitação da conservação dos dados pessoais através da previsão de que esta conservação é lícita quando, pela natureza e finalidade do tratamento, não seja possível determinar antecipadamente o momento em que o mesmo deixa de ser necessário. Este texto permite a conservação ilimitada de dados pessoais *para qualquer finalidade*, por consideração ainda de um fator que não vem considerado no RGPD – o da *natureza* do tratamento.[40];

(iv) O n.º 3 do art. 21.º introduz uma finalidade autónoma e genérica ("*comprovar o cumprimento de obrigações contratuais ou de outra natureza*") que seria comum a todos os tratamentos e paralela às finalidades legítimas e determinadas de cada um deles, para dar cobertura

40A este propósito, convém recordar o considerando 39 do RGPD: "os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo". Esta relação estreita entre o princípio da limitação da conservação e o princípio da minimização dos dados, enquanto manifestação do princípio da proporcionalidade no âmbito dos tratamentos de dados, obriga a que os dados sejam apenas conservados enquanto forem necessários à prossecução da finalidade que está na base da sua recolha.

a uma conservação de dados por tempo quase ilimitado;

(v) O n.º 5 do art. 21.º opõe-se manifestamente ao teor do art. 17.º do RGPD, pois o facto de existir um prazo de conservação de dados legalmente fixado não impede o titular dos dados de exercer o seu direito ao apagamento, desde que reunidas as condições legais para esse apagamento, o que terá de ser apreciado casuisticamente.

Em conclusão, a CNPD recomendou a eliminação do art. 21.º da Lei n.º 58/2019, de 8 de agosto, com exceção do seu n.º 2, que poderá ser revisto. As críticas a este artigo, acima resumidas, dão alguma previsibilidade sobre o modo como a autoridade de controlo portuguesa aplicará o direito aos casos concretos que envolverem a conservação de dados pessoais.

No sentido contrário à limitação da conservação dos dados apenas durante o período necessário para as finalidades para as quais são tratados, o n.º 1 do art. 40.º da Diretiva AML impõe sobre as instituições financeiras um *dever de conservação* das informações e documentos tratados para efeitos de prevenção, deteção e investigação de possíveis atos de branqueamento de capitais ou financiamento do terrorismo. Esta disposição legal estabelece um prazo de conservação de 5 anos após o termo da relação de negócio com o cliente ou após a data de execução da transação ocasional, podendo os Estados-Membros autorizarem um período de conservação adicional de 5 anos após a realização de uma avaliação da necessidade e proporcionalidade.

Findo o prazo legal de conservação, os Estados-Membros devem assegurar que as entidades obrigadas apagam os dados pessoais, salvo disposição em contrário do direito nacional, que determina as circunstâncias em que as instituições financeiras podem ou devem conservar esses dados por mais tempo.

No ordenamento jurídico português, o art. 51.º da LBCFT estabelece que as informações e os documentos obtidos pelas instituições financeiras devem ser conservados por um período de 7 anos após o momento em que a identificação do cliente se processou ou, no caso das relações de negócio, após o termo delas.

O n.º 1 do art. 57.º da LBCFT autoriza as instituições financeiras a realizar o tratamento de dados pessoais necessários ao cumprimento dos deveres de prevenção ao branqueamento de capitais e financiamento do terrorismo, não podendo tais dados ser posteriormente tratados, com base no mesmo diploma, para quaisquer outros fins, incluindo fins comerciais.

O n.º 4 do art. 57.º da LBCFT dispõe que a finalidade do tratamento de dados exclusivamente para efeitos de cumprimento dos deveres de prevenção do branqueamento de capitais e financiamento do terrorismo não prejudica o tratamento de dados pessoais com base em outras disposições legais, nomeadamente no disposto na Lei n.º 58/2019, de 8 de agosto. Esta disposição é extremamente relevante para guiar as instituições financeiras, que poderão necessitar dos mesmos dados tratados no âmbito da LBCFT para finalidades previstas em outros regimes jurídicos, nomeadamente para cumprimento da lei fiscal[41].

A conservação de dados pessoais (não apenas para cumprimento do regime de prevenção ao branqueamento de capitais, mas também para outras finalidades) é um tema caro às instituições financeiras, uma vez que as relações de negócio que elas têm com seus clientes costumam ser duradouras, pelo que eliminar dados pessoais causa receios e é uma medida que encontra dificuldades operacionais de concretização em virtude da grande quantidade de dados tratados em diversos sistemas ao longo de muitos anos.

O CEPD recomenda que o regime AML especifique os dados pessoais que devem ser conservados e por quanto tempo, tendo em conta os princípios da necessidade e da proporcionalidade. Por exemplo, poderia ser feita uma distinção entre o período de conservação aplicável, por um lado, aos dados relacionados com transações executadas ou que tenham sido consideradas suspeitas e comunicadas à UIF e, por outro lado, o período de conservação aplicável aos dados relacionados com transações não suspeitas[42].

---

41 Designadamente o art. 52.º do Código do Imposto sobre o Valor Acrescentado (IVA).

42 Letter from Andrea Jelinek (Chair of the EDPB) to Ms. Mairead McGuiness (European Commissioner for Financial services, financial stability and Capital Markets Union) and Mr. Didier Reynders (European Commissioner for Justice), sent on 19 May 2021. Disponível em: https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf.

Com efeito, é complexo definir como as instituições financeiras devem proceder *após o fim do período legal de conservação* sem prejudicar o tratamento de dados baseados em outras obrigações legais ou que devam ser conservados ao abrigo de outros fundamentos de licitude. Não obstante, *durante o período legal de conservação*, uma boa prática a adotar pelas instituições financeiras será a pseudonimização dos dados pessoais e a disponibilização do acesso a estes dados exclusivamente aos colaboradores que, por motivos expressamente justificados, precisem tratar os dados dos clientes mesmo após o término da relação de negócio.

O conflito entre o princípio da limitação da conservação consagrado pelo RGPD e o dever de conservação dos dados previsto no regime AML, tal como os outros dois conflitos estudados no presente trabalho, levanta diversas questões e a expetativa é a de que as alterações legislativas e a divulgação de novas diretrizes e recomendações sejam capazes de clarificar as dúvidas existentes.

4. Conclusão

A luta contra o branqueamento de capitais e o financiamento do terrorismo é reconhecida como um domínio de proteção de um interesse público importante, tal como a proteção dos dados das pessoas singulares é reconhecida como um direito fundamental, pelo que os deveres impostos pela Diretiva AML precisam de ser cumpridos tendo em consideração os princípios consagrados pelo RGPD.

No âmbito do regime AML, as instituições financeiras tratam os dados das pessoas singulares envolvidas em relações de negócio e transações ocasionais ao abrigo da alínea c) do n.º 1 do art. 6.º do RGPD, ou seja, com base no cumprimento de uma obrigação jurídica a que estas instituições financeiras estão sujeitas na qualidade de responsáveis pelo tratamento.

Sem prejuízo da existência de outros conflitos entre os princípios do RGPD e o regime AML, o presente trabalho estudou três conflitos comuns neste âmbito, designadamente (i) o princípio da transparência contra o dever de não divulgação das informações, (ii) o princípio da minimização dos dados

contra o dever de diligência quanto à clientela e (iii) o princípio da limitação da conservação dos dados contra o dever de conservação dos dados.

O princípio da transparência, nos casos em que o fornecimento de informações ao titular dos dados prejudicar os objetivos do tratamento previstos no regime de prevenção ao branqueamento de capitais, será mitigado pelo dever de não divulgação a que as instituições financeiras estão obrigadas, sem prejuízo de as restrições ao direito de acesso aos dados pelo titular serem levantadas numa fase posterior em que o fornecimento de informações não prejudique os objetivos do tratamento previstos no regime de prevenção ao branqueamento de capitais.

O princípio da minimização de dados e o dever de diligência quanto à clientela a que as instituições financeiras estão obrigadas devem ser abordados de forma equilibrada, numa perspetiva de prevenção ao branqueamento de capitais e ao financiamento do terrorismo que tenha em consideração o tratamento dos dados pessoais que são efetivamente adequados, pertinentes e limitados ao que é necessário para esta finalidade.

O princípio da limitação da conservação e o dever de conservação dos dados deverão ser articulados à luz dos princípios da necessidade e da proporcionalidade, uma vez que o enquadramento legal aplicável, as diretrizes e recomendações neste âmbito não são suficientemente conclusivas quanto à forma ideal de conservar os dados pessoais tratados pelas instituições financeiras ao abrigo do regime AML, bem como quanto à forma ideal de eliminar esses dados findo o prazo legal de conservação.

A atualização do regime AML deve ser realizada com uma revisão da relação entre as medidas de prevenção ao branqueamento de capitais e os direitos à privacidade e à proteção de dados, pelo que uma articulação mais estreita entre os dois regimes jurídicos poderá beneficiar os dois lados.