



RAUL NUNO GONÇALVES SANTOS TABORDA

**DAS INVESTIGAÇÕES INTERNAS NAS INSTITUIÇÕES DE CRÉDITO:
TRANSFERÊNCIA DAS MENSAGENS DE CORREIO ELETRÓNICO
PARA O PROCESSO DE CONTRAORDENAÇÃO**

Dissertação com vista à obtenção do grau de
Mestre em Direito (Ciências Jurídicas Forenses)

Orientador:

Doutor Frederico Costa Pinto, Professor da Faculdade de Direito da Universidade
Nova de Lisboa

Fevereiro de 2021



RAUL NUNO GONÇALVES SANTOS TABORDA

**DAS INVESTIGAÇÕES INTERNAS NAS INSTITUIÇÕES DE CRÉDITO:
TRANSFERÊNCIA DAS MENSAGENS DE CORREIO ELETRÓNICO
PARA O PROCESSO DE CONTRAORDENAÇÃO**

Dissertação com vista à obtenção do grau de
Mestre em Direito (Ciências Jurídicas Forenses)

Orientador:

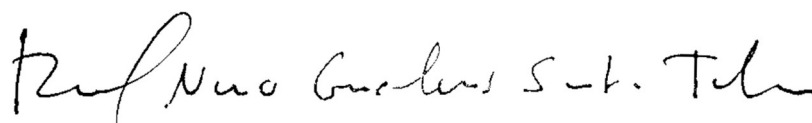
Doutor Frederico Costa Pinto, Professor da Faculdade de Direito da Universidade
Nova de Lisboa

Fevereiro de 2021

DECLARAÇÃO ANTIPLÁGIO

Declaro por minha honra que o trabalho que apresento é original e que todas as minhas citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Lisboa, 08 de fevereiro de 2021



AGRADECIMENTOS

Um agradecimento à minha mãe e à Cláudia, minha companheira, pelo constante e incondicional apoio.

Um agradecimento especial ao meu Orientador, o Senhor Professor Doutor Frederico Costa Pinto, pelo permanente cuidado e apoio ao longo de todo o trabalho, em especial num contexto pandémico, marcado por vicissitudes várias.

MODO DE CITAR E OUTRAS CONVENÇÕES

1. Para efeitos da presente dissertação, optou-se pelo estilo Autor-data.
2. As expressões ou palavras em língua estrangeira são apresentadas em itálico.
3. A presente dissertação foi escrita ao abrigo do novo acordo ortográfico.

LISTA DE ABREVIATURAS

- AdC – Autoridade da Concorrência
- BdP – Banco de Portugal
- CC – Código Civil
- CEDH – Convenção Europeia dos Direitos Humanos
- CEPD – Comité Europeu para a Proteção de Dados
- CSC – Código das Sociedades Comerciais
- CdVM – Código dos Valores Mobiliários
- CMVM – Comissão do Mercado de Valores Mobiliários
- CNPD – Comissão Nacional de Proteção de Dados
- CP – Código Penal
- CPC – Código de Processo Civil
- CPP – Código de Processo Penal
- CRP – Constituição da República Portuguesa
- CT – Código do Trabalho
- EBA – *European Banking Authority*
- IC – Instituição(ões) de Crédito
- IOSCO – *International Organization of Securities Commissions*
- PE – Parlamento Europeu
- PwC – *PricewaterhouseCoopers*
- RGICSF – Regime Geral das Instituições de Crédito e Sociedades Financeiras
- RGCO – Regime Geral das Contraordenações
- RGPD – Regulamento Geral sobre a Proteção de Dados
- RJC – Regime Jurídico da Concorrência
- STJ – Supremo Tribunal de Justiça
- TEDH – Tribunal Europeu dos Direitos Humanos
- TC – Tribunal Constitucional
- TJUE – Tribunal de Justiça da União Europeia

- TRC – Tribunal da Relação de Coimbra
- TRE – Tribunal da Relação de Évora
- TRG – Tribunal da Relação de Guimarães
- TRL – Tribunal da Relação de Lisboa
- TRP – Tribunal da Relação do Porto

DECLARAÇÃO

O corpo da tese, incluindo espaços e notas, ocupa um total de 195 425 caracteres.

RESUMO

O presente estudo pretende responder à questão de saber se, e em que condições, o conteúdo de mensagens de correio eletrónico recolhidas no decurso de uma investigação interna, conduzida por uma IC, pode ser transferido para um processo contraordenacional instaurado pelo BdP, e em curso.

Para o efeito, proceder-se-á à caracterização e à análise das investigações internas, integrando-as no sistema de controlo interno e na função de *compliance*.

As investigações contêm uma fase de recolha de elementos, que se destina a suportar as conclusões do relatório interno que será produzido. Numa era marcada pelas tecnologias da informação e comunicação, em que os fluxos de informação ocorrem primordialmente em meio digital, o correio eletrónico surge como um elemento primordial em qualquer investigação. No entanto, se o investigador proceder à recolha de tais mensagens, de forma indiscriminada, em violação do direito à privacidade ou dos direitos de personalidade dos colaboradores da instituição, poderá ditar não só o fracasso da investigação, como impedir, irremediavelmente, a transferência desses elementos para o processo contraordenacional. Nesse sentido, proceder-se-á à análise dos requisitos de que depende a recolha de mensagens de correio eletrónico, à luz da legislação laboral e à luz da legislação de proteção de dados, oferecendo linhas orientadoras.

Na esteira do relatório final produzido pela IC, existe a possibilidade de o BdP, ao abrigo dos poderes de supervisão que lhe assistem, considerar relevante, para a instrução de um determinado processo de contraordenação, a junção aos autos daquele relatório, bem como dos elementos que suportam as respetivas conclusões (no caso, as mensagens de correio eletrónico recolhidas). Nesse sentido, importa analisar em que moldes uma tal transferência se afigura compatível com os direitos que processualmente assistem ao arguido no processo contraordenacional.

ABSTRACT

The present study aims to answer the question of whether and under which circumstances the content of email messages, collected during an internal investigation conducted by a banking institution, can be legally transferred to an administrative offence proceeding opened by the Bank of Portugal.

To this end, the study will describe and analyse internal investigations, integrating them in the control system and in the compliance function.

Internal investigations comprise a phase that aims to collect elements to support the conclusions of the internal report that will be produced. In an age dominated by information and communication technologies, in which the information flows occur primarily in a digital environment, emails are a key element of any internal investigation. However, if the investigator collects such email messages indiscriminately, in violation of the right to privacy or the personality rights of the institution's employees, he may not only dictate the failure of the investigation but also irremediably prevent the transfer of those messages to an administrative offence proceeding. Thus, this study will analyse the requirements for the collection of email messages, in the light of both labour law and data protection law, and offer guidelines for such collection.

Following the final report produced by the banking institution, the Bank of Portugal, under its supervisory powers, might consider relevant for a certain administrative offense proceeding to add the abovementioned report as well as the elements that support its conclusions (in the case of our study, the email messages that were collected). In this sense, it is important to analyse the compatibility of such transfer with the procedural rights of the defendant in the administrative offence proceeding.

INTRODUÇÃO

As IC têm o dever legal de dispor de dispositivos sólidos em matéria de governo da sociedade, cabendo-lhes organizar processos eficazes de identificação, gestão, controlo e comunicação dos riscos, a que está ou pode vir a estar sujeita (artigo 14.º, n.º 1, alíneas f) e g), do RGICSF).

No exercício da sua atividade, as IC deparam-se com a ocorrência de riscos de *compliance* (risco de continuidade de negócio, risco pecuniário e sancionatório e risco reputacional). Para gerir tais riscos (lidar com as respetivas consequências e prevenir ocorrências futuras), é fundamental que a instituição disponha de processos e de estratégias capazes de reagir à respetiva ocorrência, sendo nestes processos que as investigações internas se inserem.

No decurso das investigações são recolhidos diversos elementos considerados indispensáveis para comprovar determinada realidade, sendo que, entre eles, contam-se as mensagens de correio eletrónico, enviadas e recebidas por pessoas da instituição (designadamente, administradores, diretores e outros colaboradores), mas também as mensagens enviadas por pessoas externas à instituição. Importa, por isso, estudar se, e em que condições, tais mensagens podem ser recolhidas no decurso de uma investigação e se o respetivo conteúdo pode ser analisado pelo investigador.

Ora, o BdP, ao abrigo dos seus poderes de supervisão, e quando tal se afigure necessário à averiguação e à instrução de determinado processo contraordenacional, pode solicitar a quaisquer pessoas e entidades esclarecimentos, informações e a entrega de documentos. A questão a que se pretende dar resposta no âmbito do presente trabalho consiste em saber se, e em que termos, o conteúdo de mensagens de correio eletrónico recolhidas no âmbito e no decurso de uma investigação interna pode ser “transferido” para um processo contraordenacional da competência do BdP.

O presente estudo está dividido em três capítulos.

No primeiro, procedemos à caracterização e à análise das investigações internas, integrando-as no sistema de controlo interno e na função de *compliance*, seguindo-se a descrição e análise das diversas fases da investigação, incluindo a recolha de elementos.

No segundo, identificamos as mensagens de correio eletrónico como possível elemento que pode ser recolhido no decurso de uma investigação e identificamos os requisitos de que depende a respetiva recolha pelo investigador, à luz da legislação laboral e, bem assim, da legislação em matéria de proteção de dados.

No terceiro e último capítulo, respondemos à questão de saber se, e em que condições, é possível transferir o conteúdo de mensagens de correio eletrónico recolhidas numa investigação interna, em conformidade com as conclusões vertidas no Capítulo II. Analisar-se-á a questão à luz dos direitos que processualmente assistem ao arguido, designadamente o direito ao silêncio e à não autoinculpação. Mais se analisarão, neste capítulo, as consequências, para o processo, de uma eventual transferência ilegal do conteúdo dessas mensagens.

CAPÍTULO I – DAS INVESTIGAÇÕES INTERNAS

1. Enquadramento

No presente capítulo procederemos ao enquadramento e à caracterização das investigações internas, as quais, em traços gerais e não obstante estejam mais bem caracterizadas adiante, constituem averiguações reativas que têm como finalidade confirmar ou afastar uma suspeita de risco de incumprimento ou de *compliance*¹. Integrá-las-emos no *compliance* (*lato sensu*) e no sistema de controlo interno, explicando a sua função enquanto meio de reação àquele risco.

A referida configuração permite apresentar a seguinte síntese: **(i)** *compliance*, sendo parte integrante **(ii)** do sistema de controlo interno, concretizado **(iii)** pela função de *compliance*, à qual compete controlar o cumprimento das obrigações legais e dos deveres a que as IC se encontram sujeitas, cabendo-lhe, em especial, prevenir e detetar **(iv)** o risco de *compliance*. Mais compete a esta função, em nossa opinião, reagir ao risco de *compliance*, designadamente através de **(v)** investigações internas.

Nos termos do artigo 3.º do RGICSF, constituem IC: **(i)** os bancos, **(ii)** as caixas económicas, **(iii)** a Caixa Central de Crédito Agrícola mútuo e as caixas de crédito agrícola mútuo, **(iv)** as instituições financeiras de crédito, **(v)** as instituições de crédito hipotecário e **(vi)** outras empresas que, correspondendo à definição anterior, como tal sejam qualificadas pela lei.

Antes de passarmos à caracterização das investigações internas, importa fazer algumas considerações a propósito dos sobreditos conceitos.

¹ Adotaremos a designação de risco de *compliance*.

1.1. *Compliance*

A primeira questão que se coloca é a de saber o que se entende por *compliance*. Sem querer ser exaustivo, pois não é este o tema do presente trabalho, *compliance* – termo anglo-saxónico – tem, desde logo, um significado residual, que pode ser descrito da seguinte forma: «[...] *principio vigente en cada uno de los ordenamientos jurídicos estatales según el cual las empresas y sus órganos deben operar armónicamente con el Derecho vigente*»². *Compliance* é, nesta perspetiva, aquilo que o próprio termo evidencia, *i.e.*, conformidade ao Direito, conformidade à lei – constitucional e infraconstitucional – e às disposições normativas emanadas das entidades reguladoras, como é, por exemplo, o caso dos Avisos e Instruções do BdP, ao abrigo do respetivo poder regulamentar^{3/4}.

Contudo, *compliance* não se esgota naqueles aspetos. Numa perspetiva mais densificada, *compliance* consiste «na adopção de regras e processos intraempresariais que garantam que o cumprimento do Direito não é fruto do acaso, de um comportamento individual ou de interesses parciais de um departamento, antes corresponde a uma “arquitectura de *compliance*” coerente e omnipresente, *i.e.* referida a todas as actividades empresariais, internas e externas»⁵.

² ROTSCH, Thomas (2012), p. 2.

³ «***Compliance* é o dever de cumprir, de estar em conformidade e fazer cumprir normas e regulamentos, internos e externos, impostos à actividade das empresas.**» – JÚNIOR, Filipa Marques e MEDEIROS, João (2018), p. 124.

⁴ «A palavra *compliance* tem origem no verbo inglês “to comply” que significa agir de acordo ou estar em conformidade com uma norma, uma instrução ou um comando.» – PIZARRO, Sebastião Nóbrega (2017), p. 18.

⁵ BRITO, Teresa Quintela de (2018), p. 59. Adicionalmente, tal como refere GERALDO, Tiago (2018), p. 275, *compliance* é: «Um sistema ordenado, transversal à organização empresarial, de prevenção e monitorização de riscos legais». Já para a PwC *compliance* «é o modelo organizacional, processos e sistemas usados para garantir a adesão às leis e regulamentos, às políticas e normas internas, e expectativas dos intervenientes importantes considerando, por exemplo, os seus clientes, empregados, fornecedores, investidores, auditores, e reguladores de forma a que a empresa possa proteger e aumentar o seu modelo de negócio, reputação e condição financeira.» – disponível em <https://www.pwc.com>, acessível em 25.01.2020.

Nesse sentido, podemos representar o *compliance* como se de uma pirâmide se tratasse: na sua base, a “legalidade”, i.e. o cumprimento das normas legais; num patamar acima, as *best practices*, padrões de conduta sectoriais, ou seja, o cumprimento das normas regulamentares; e, no topo da pirâmide, a “responsabilidade social”, i.e. o cumprimento das normas internas, voluntariamente impostas pela organização a si própria⁶. O *compliance* é, em si mesmo, um resultado: o resultado do cumprimento.

O *compliance* tem, no domínio das IC, importância preponderante, porquanto nelas se desenvolvem «atividades com um elevado perfil de risco, intimamente ligado à alavancagem financeira a que estão sujeitas; este efeito traduz-se numa importância acrescida da gestão do risco e da orientação da governação para a sustentabilidade da instituição, impondo-se uma diligência ainda maior aos seus administradores»⁷.

1.2. Sistema de controlo interno

O Instituto Europeu Monetário, em documento datado de 1997, acolhe a seguinte definição de sistema de controlo interno: «*the process, including all the controls, financial or otherwise, effected by a credit institution's board of directors, senior management and other personnel to provide reasonable assurance that the following objectives are achieved: a) accomplishment of established goals and objectives; b) economical and efficient use of resources; c) adequate control of various risks incurred and the safeguarding of assets; d) reliability and integrity of financial and management information; e) compliance with laws and regulations as well as policies, plans, internal rules and procedures*»⁸.

⁶ AYRES, Ian e BRAITHWAITE, John (1992), p. 39.

⁷ AZEVEDO, Sara (2016), p. 16.

⁸ *Internal Control Systems of Credit Institutions*, disponível em <https://www.ecb.europa.eu>, acessível em 19.07.2020.

Na ordem jurídica portuguesa, encontramos em diversos diplomas legais referências ao sistema de controlo interno⁹. Este surge atualmente definido como o «conjunto de estratégias, políticas, processos, sistemas e procedimentos com o objetivo de garantir a sustentabilidade da instituição no médio e longo prazo e o exercício prudente da sua atividade, através [...]», no que aqui releva, «do cumprimento da legislação, da regulamentação e das orientações aplicáveis à atividade da instituição, emitidas pelas autoridades competentes, do cumprimento dos normativos internos da própria instituição, bem como das normas e usos profissionais e deontológicos e das regras de conduta e de relacionamento de clientes»¹⁰.

Por via de regra, a criação e a implementação de um sistema de controlo interno pelas empresas é voluntária. Nas situações de implementação voluntária pretende-se «minorar significativamente os riscos de responsabilização das sociedades comerciais e respetivos dirigentes nos âmbitos civil, contraordenacional e até criminal e, com isso, a defender genericamente os interessados (*Stakeholders*)»^{11/12}. Na generalidade das empresas, em que a autorregulação é, em certa medida, opcional¹³, a implementação de um sistema de controlo interno visa prevenir e reagir a riscos de *compliance*¹⁴, assim se evitando as eventuais consequências desfavoráveis

⁹ São meros exemplos os seguintes: artigo 14.º do RGICSF, artigo 12.º do Aviso do BdP n.º 3/2020, artigo 245.º-A do CdVM, artigo 12.º da Lei n.º 83/2017, de 18 de agosto, entre outros.

¹⁰ Artigo 12.º, n.º 1, alínea c), do Aviso do BdP n.º 3/2020. Esta definição não diverge substancialmente da definição que era dada pelo Aviso do BdP n.º 5/2008. Dogmaticamente, podemos entender que o sistema de controlo interno (conceito amplo, que abarca diversos subsistemas) integra, dentro dele, o sistema de controlo de cumprimento (ou sistema de *compliance*): «Desde logo, o controlo de cumprimento, tanto no conceito como nas suas distintas e concretas manifestações, integra o sistema geral de controlo interno, o que se supõe que se organize, estabeleça e desenvolva no quadro estrutural, hierárquico e funcional de cada entidade» (LABAREDA, João (2014), p. 45). Este autor caracteriza o sistema de controlo de cumprimento «como o conjunto de meios organizados e dirigidos à prevenção, gestão e controlo do risco de incumprimento, aí incluindo, designadamente, as estratégias, políticas, processos, procedimentos, estruturas e recursos vocacionados para o efeito.» (LABAREDA, João (2014), p. 42)

¹¹ MENDES, Paulo Sousa (2018), p. 11.

¹² PEDRO DURO refere que «as empresas portuguesas, fora do setor financeiro [...] ainda estão longe de explorar as potencialidades do *compliance* [...]» (DURO, Pedro (2015), pp. 1 e 2)

¹³ Pelo menos com o conteúdo e o alcance objeto do nosso estudo.

¹⁴ Cujo sentido e alcance nos deteremos adiante.

que decorram da respetiva materialização¹⁵. Na implementação de uma tal cultura organizacional^{16/17}, a empresa procura não só precaver-se contra eventuais sanções aplicáveis, as quais, normalmente têm expressão pecuniária, como almeja, igualmente, evitar o dano reputacional que o incumprimento, designadamente das disposições legais e regulamentares, pode acarretar.

Diferentemente, em determinados setores da atividade económica, o legislador impôs determinados deveres de autorregulação – o que a doutrina designa de situações de autorregulação regulada¹⁸. É o que sucede, designadamente, com as IC, que devem dispor de «mecanismos adequados de controlo interno»¹⁹, devendo, inclusivamente, para efeitos de obtenção da autorização para o exercício da atividade económica, demonstrar que dispõem de «dispositivos sólidos em matéria de governo da sociedade»²⁰, isto é, de «[m]ecanismos adequados de controlo interno»²¹. Nestas situações, a implementação de um sistema de controlo interno efetivo e sólido não é uma opção. É um dever e este decorre diretamente da lei.

Tratam-se de «casos de autorregulação regulada pelo Estado [...]»²², em que o sistema de controlo interno deve, por um lado, permitir «detetar os riscos de incumprimento de normas legais aplicáveis a intermediários financeiros [...]

¹⁵ «Na verdade, ignorar ou não aplicar o *compliance* significa estar em não-*compliance*. Os custos do não-*compliance* não são desprezíveis. Por um lado, podem implicar a lesão na reputação e respetiva marca, o que implica perda potencial da imagem com óbvias consequências. Por outro, o não-*compliance* poderá causar a perda de autorização de funcionamento, alvará, ou outro, determinando o encerramento da organização. Por fim, poderá importar a aplicação de sanções, coimas ou penalidades à organização e aos seus responsáveis, situação que tem feito evoluir o conceito de *criminal compliance*.» – PIZARRO, Sebastião Nóbrega (2017), pp. 12 e 13.

¹⁶ BRITO, Teresa Quintela de (2018), p. 67.

¹⁷ «Da noção de *compliance* deverá constar o desenvolvimento de uma cultura organizacional que instaure e desenvolva o respeito por valores constantes de normas, internos ou externos à organização e valores éticos, o que nunca passará pela sua imposição, mas sim pela sua divulgação e controlo do seu respeito.» – PIZARRO, Sebastião Nóbrega (2017), p. 21.

¹⁸ MARTÍN, Adán Nieto (2015), p. 118.

¹⁹ Artigo 14.º, n.º 1, do RGICSF.

²⁰ Artigo 17.º, n.º 1, alínea f), do RGICSF.

²¹ Artigo 17.º, n.º 2, alínea c), do RGICSF.

²² BRITO, Teresa Quintela de (2018), p. 61.

«assegurar ou permitir às autoridades reguladoras, como o Banco de Portugal (no âmbito da supervisão prudencial) e a Comissão do Mercado de Valores Mobiliários («CMVM») (no âmbito da supervisão comportamental) o exercício eficiente dessas funções de supervisão»²³. Nestas situações de autorregulação imposta, a própria cultura organizacional também é imposta pela lei, cabendo à instituição o dever de garantir que todos os colaboradores²⁴ reconhecem «a importância do controlo interno»²⁵, sensibilizando-os para a necessidade de contribuírem ativamente para o funcionamento do sistema e alertando-os para as consequências do seu incumprimento.

No que em concreto se refere às IC, nos termos do artigo 76.º da Diretiva n.º 2013/36/UE, do PE e do Conselho, de 26 de junho, o órgão de direção deve aprovar e rever periodicamente as estratégias e políticas destinadas a assumir, gerir, acompanhar e atenuar os riscos a que a instituição está ou possa vir a estar exposta e deve participar ativamente e assegurar que sejam afetados recursos adequados à gestão de todos os riscos significativos²⁶.

No plano regulamentar merece destaque o então Aviso do BdP n.º 5/2008²⁷, o qual, logo no seu Preâmbulo, reconhecia a importância que a existência de um sistema de controlo interno adequado e eficaz assume no efetivo cumprimento de deveres a que a IC está sujeita, «assegurando a sua estabilidade e sobrevivência e, assim, a estabilidade do próprio sistema financeiro». Esta importância continua a ser refletida no recente Aviso do BdP n.º 3/2020.

²³ ABREU, Filipe Brum de (2008), p. 86.

²⁴ O termo pretende incluir trabalhadores e prestadores de serviços.

²⁵ Artigo 7.º, n.º 1, do Aviso do BdP n.º 5/2008 (entretanto revogado) e, depois, com maior grau de densificação, o disposto no artigo 2.º do Aviso do BdP n.º 3/2020.

²⁶ Relevam ainda, designadamente, os artigos 73.º e 74.º, transpostos para a ordem jurídica nacional pelo Decreto-Lei n.º 157/2014, de 24 de outubro, que alterou o RGICSF (artigos 115.º-A e seguintes).

²⁷ Entretanto revogado pelo Aviso do BdP n.º 3/2020.

Enfim, o sistema de controlo interno pressupõe a adoção de um sistema de gestão de compliance, i. e., mais especificamente, a criação e a implementação de um conjunto concatenado de procedimentos e mecanismos capazes de fazer cumprir, detetar e de reagir perante riscos de *compliance*. Neste sentido, o sistema de gestão de compliance assenta em três pilares base²⁸: i) prevenção²⁹, ii) deteção³⁰ e iii) reação³¹.

1.3. Função de *compliance*

Por seu turno, a função de *compliance* «convoca a ideia da actividade desenvolvida por uma estrutura própria, cuja razão de ser é, exactamente, promover que a instituição em que se insere actue em consonância com os normativos aplicáveis, reportando-se, ora aquela, ora a esta, ou, frequentemente, a ambas como um todo»^{32/33}.

A função de *compliance*³⁴, ao integrar o sistema de controlo interno, dá-lhe substância, tornando-o perceptível aos olhos de todos que integram a instituição³⁵,

²⁸ Nesse sentido, vide, designadamente *White Paper on the Compliance function*, p. 11, disponível em <https://www.asociacioncompliance.com>, acessível em 20.12.2020.

²⁹ Neste pilar, podemos enquadrar os Códigos de Conduta, Manuais de Procedimentos e Políticas de *Compliance* da IC, bem como a formação destes temas aos seus colaboradores, tendo em vista desenvolver e cimentar a cultura organizacional de *compliance*.

³⁰ No segundo pilar do sistema de gestão de *compliance*, encontramos, nomeadamente, a existência de um canal de denúncias – que desenvolveremos adiante –, a regular avaliação de perceção interna de *compliance* e as auditorias de *compliance*.

³¹ É neste terceiro pilar do sistema de gestão de *compliance* que se inserem, nomeadamente, a aplicação de sanções e as investigações internas, objeto do presente estudo, como reação a um evento *non-compliance* anteriormente detetado.

³² LABAREDA, João (2014), p. 42.

³³ Para um desenvolvimento do tema dos princípios da função de *compliance*, vide *Compliance and Compliance Function in Banks*, produzido pelo Comité de Basileia, pp. 10 e ss, disponível em <https://www.bis.org>, acessível em 25.01.2020.

³⁴ A função de *compliance* era tratada no Aviso do BdP n.º 5/2008 como a função de “compliance”, sendo regulada no respetivo artigo 17.º. Sucede que o Aviso do BdP n.º 3/2020 veio alterar a designação desta função para função de conformidade, sendo regulada pelo respetivo artigo 28.º. No entanto, considerando as constantes e reconhecidas alusões ao termo *compliance*, quer para designar o sistema de *compliance* como um todo, quer para designar os demais termos com aquele relacionados, optamos, por uma questão de coerência, por manter a designação função de *compliance*, enquanto função daquele sistema.

³⁵ LABAREDA, João (2014), p. 43.

tendo como missão cumprir, e fazer cumprir, os deveres e obrigações legais a que a mesma se encontra sujeita^{36/37}.

As IC devem, no que releva para efeitos do presente trabalho, estabelecer e manter uma função de *compliance* responsável por (i) acompanhar e avaliar regularmente a adequação e a eficácia das medidas e procedimentos adotados para detetar riscos de *compliance*, (ii) aconselhar os órgãos de administração e de fiscalização, para efeitos do cumprimento dos deveres legais e regulamentares e (iii) prestar imediatamente aos órgãos de administração e de fiscalização toda a informação de que dispõem sobre quaisquer indícios de violação de deveres legais ou regulamentares³⁸.

Também o Comité de Basileia havia estabelecido, como princípio, a criação e a implementação de uma permanente e efetiva função de *compliance*³⁹.

Ora, para que a função de *compliance* seja permanente e efetiva, a mesma deve dispor de mecanismos que permitam reagir, de forma espontânea, atempada e eficaz, a riscos de *compliance*. Em nossa opinião, as investigações internas constituem um dos mecanismos de que as entidades devem dispor para cumprir tal desiderato, devendo

³⁶ LABAREDA, João (2014), p. 29.

³⁷ De acordo com as orientações da EBA em matéria de governo interno, «A FVC [Função de Verificação do Cumprimento] assegura que o controlo é efetuado através de um programa de acompanhamento da verificação do cumprimento estruturado e bem definido e que a política em matéria de verificação do cumprimento é observada. A FVC deve reportar ao órgão de administração e, se for caso disso, comunicar com a FGR [Função de Gestão de Riscos], sobre o risco de conformidade da instituição e a sua gestão» e «adotam medidas adequadas contra qualquer comportamento fraudulento e infrações disciplinares a nível interno ou externo (p. ex., infrações de procedimentos internos ou violações dos limites).» (p. 44), disponíveis em: <https://eba.europa.eu>, acessível em 22.01.2020.

³⁸ Artigo 28.º do Aviso do BdP n.º 3/2020.

³⁹ «*Compliance and compliance function in Banks*», p. 9, disponível em <https://www.bis.org>, acessível em 25.01.2020

a sua existência ser contemplada e regulada em programas de *compliance*^{40/41}. A importância destes programas está inclusivamente reconhecida na estratégia nacional de combate à corrupção⁴², prevendo como componente desses programas justamente as investigações internas⁴³.

⁴⁰ «[A] finalidade dos programas de *compliance* consiste em, além do mais, reduzir ao mínimo razoável o risco de lesão dos bens jurídicos, achando um ponto de equilíbrio que não paralise a actividade da empresa. De entre aquelas que são comumente enumeradas como as principais funções de um programa de *compliance*, no âmbito de uma estrutura empresarial, podemos identificar as seguintes: [...] Acompanhamento e verificação do cumprimento das leis, normas e regulamentos [...]» – JÚNIOR, Filipa Marques e MEDEIROS, João (2018), p. 125. Parece-nos que a tendência futura será a imposição, por via legislativa, de programas de *compliance* e, bem assim, a determinação de um conteúdo mínimo. Veja-se, a este propósito a Estratégia Nacional de Combate à Corrupção 2020-2024, aludindo como tendência atual a adoção e uniformização de tais programas – p. 45, disponível em <https://www.portugal.gov.pt>, acessível em 23.01.2021.

⁴¹ «Another Hallmark of a well-designed compliance program is the existence of an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company's code of conduct, company policies, or suspected or actual misconduct. Prosecutors should assess whether the company's complaint-handling process includes proactive measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers. Prosecutors should also assess the company's processes for handling investigations of such complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline.» – U.S. Department of Justice Criminal Division, *Evaluation of Corporate Compliance Programs*, p. 6, disponível em <https://www.justice.gov>, acessível em 01.10.2020. Também a Estratégia Nacional de Combate à Corrupção alude a este aspeto: «A adoção ou o aperfeiçoamento dos programas de cumprimento normativo incentiva-se por via da sua repercussão na responsabilização penal, administrativa ou contraordenacional das pessoas colectivas e entidades equiparadas. Insentando-as de responsabilidade, atenuando a sua punição e prevendo soluções e meios processuais diferenciados e menos restritos, o Estado promove uma cultura empresarial de cumprimento normativo assente na responsabilização penal e contraordenacional das pessoas coletivas e entidades equiparadas. Com ganhos também do ponto de vista da prevenção, deteção e repressão de comportamentos ilícitos por parte das pessoas individuais, nomeadamente por via da possibilidade de denúncia no canal da empresa, e consequente investigação interna, e do seu contributo para a responsabilização penal ou contraordenacional da pessoa individual.» – Estratégia Nacional de Combate à Corrupção 2020-2024, p. 45, disponível em <https://www.portugal.gov.pt>, acessível em 23.01.2021.

⁴² De acordo com o referido documento de estratégia, «[a] obrigatoriedade de adoção de programas de cumprimento normativo [...] facilitará certamente a investigação criminal, por via da prova que poderá ser produzida em sede de investigações internas [...]» – Estratégia Nacional de Combate à Corrupção 2020-2024, p. 60, disponível em <https://www.portugal.gov.pt>, acessível em 23.01.2021.

⁴³ «Reconhece-se que foi feito um grande esforço na adoção de medidas destinadas a dotar a investigação de mais recursos e capacitação através, nomeadamente, do recurso a prova produzida em investigações internas, a ações encobertas, a quebra do sigilo bancário e fiscal e a buscas e pesquisas em ambiente digital» – Estratégia Nacional de Combate à Corrupção 2020-2024, p. 38, disponível em <https://www.portugal.gov.pt>, acessível em 23.01.2021.

De acordo com o estabelecido pelo Comité de Basileia, a função de *compliance* deve ter (i) o direito de conduzir investigações a possíveis incumprimentos da política de *compliance*, bem como ter (ii) o direito de solicitar a especialistas externos o desempenho dessa tarefa⁴⁴, acrescentando, a propósito das investigações internas, que esse direito deve ser reduzido a escrito, integrando a política interna de *compliance* do Banco ou outro documento formal⁴⁵.

Também a IOSCO, em relatório final emitido na sequência de um processo de consulta pública acerca da *função de compliance*, referiu como elemento integrante do princípio “independência e capacidade para agir”, que as pessoas afetas à função de *compliance* devem ter a possibilidade de conduzir investigações de possíveis irregularidades⁴⁶.

Embora os instrumentos normativos portugueses em vigor não vão tão longe, encontramos, no universo das IC, um caso específico na Lei que determina a “abertura” e a condução de uma investigação, a saber: o regime de participação de irregularidades, previsto no artigo 116.º-AA do RGICSF.

Este regime foi recentemente regulado pelo Aviso do BdP n.º 3/2020, cabendo à instituição consagrar «um processo destinado a assegurar que todas as participações efetuadas são registadas em base de dados própria e sujeitas a análise, que é elaborado um relatório fundamentado sobre as mesmas, com indicação das medidas a adotar ou com uma justificação para a não adoção de quaisquer medidas»⁴⁷. Acresce que o relatório mencionado no n.º 7 do artigo 116.º-AA do RGICSF deve conter, entre

⁴⁴ *Compliance and compliance function in Banks*, p. 12, disponível em <https://www.bis.org>, acessível em 25.01.2020.

⁴⁵ *Compliance and compliance function in Banks*, p. 11, disponível em <https://www.bis.org>, acessível em 25.01.2020.

⁴⁶ *Compliance Function at Market Intermediaries – Final Report*, p. 13, disponível em <https://www.iosco.org>, acessível em 25.01.2020. Para garantir a adequação e a independência da função de *compliance*, veja-se o artigo 13.º, n.º 2, alínea a), do Aviso do BdP n.º 3/2020.

⁴⁷ Artigo 35.º, n.º 2, alínea f).

outros aspetos, a descrição sumária das diligências para a averiguação da factualidade participada⁴⁸, se o processo se encontra pendente ou finalizado, bem como o resultado da investigação⁴⁹.

1.4. Risco de *compliance*

O risco de *compliance* vinha definido, no Aviso do BdP n.º 5/2008, como «a probabilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes de violações ou da não conformidade relativamente a leis, regulamentos, determinações específicas, contratos, regras de conduta e de relacionamento com clientes, práticas instituídas ou princípios éticos, que se materializam em sanções de carácter legal, na limitação de oportunidades de negócio, na redução do potencial de expansão ou na impossibilidade de exigir o cumprimento de obrigações contratuais»⁵⁰. Com o Aviso do BdP n.º 3/2020, o Regulador optou por uma abordagem distinta, não tendo incluído a tradicional definição de risco de *compliance*. Ao invés, cabe ao órgão de administração assegurar que a instituição adota categorias de risco que, no seu conjunto, abranjam todos os fatores associados aos eventos de risco a que a instituição está ou possa vir a estar sujeita⁵¹. E identificou na Instrução n.º 18/2020, nas categorias de risco, justamente, o «risco de conformidade»⁵², como integrando a subcategoria «outros riscos»⁵³, embora não o definindo. Ademais,

⁴⁸ Artigo 8.º, n.º 1, alínea b), subparágrafo iv), da Instrução do BdP n.º 18/2020, que regulamenta o Aviso do BdP n.º 3/2020.

⁴⁹ Artigo 8.º, n.º 1, alínea b), subparágrafo vi), da Instrução do BdP n.º 18/2020.

⁵⁰ Artigo 11.º, n.º 4, alínea f), do Aviso do BdP n.º 5/2008. Cabe apenas precisar, estabelecendo aqui um paralelismo com o artigo 305.º-F, n.º 1, do CdVM, que a locução «decorrentes de violações ou da não conformidade», a nosso ver, atentos os princípios subjacentes ao sistema de controlo interno, não diz apenas respeito a irregularidades já consumadas, mas também àquelas que «estejam a ser executadas ou que, à luz dos elementos disponíveis, se possa prever com grande probabilidade que venham a ser praticadas».

⁵¹ Artigo 21.º, n.º 1.

⁵² Uma vez mais substituindo *compliance* por conformidade.

⁵³ Anexo I da Instrução n.º 18/2020.

continuamos a encontrar no texto do Aviso do BdP n.º 3/2020 referência ao “risco de incumprimento”⁵⁴.

Quanto à sua caracterização, «a conformação do risco de «compliance» envolve três momentos ou vertentes distintas e complementares: a causa ou origem, que se reconduz sempre ao desajustamento da realidade da instituição face aos deveres que a oneram; a materialização do perigo de conformidade operada pela produção das consequências desfavoráveis, de diverso tipo, que suporta em razão dela; a determinação e avaliação dos impactos que elas acarretam no plano da situação económico-financeira»⁵⁵.

A definição que encontrávamos no Aviso do BdP n.º 5/2008 diferia, contudo, da constante do documento elaborado pelo Comité de Basileia em supervisão bancária, na medida em que a primeira não inclui a perda de reputação como facto suscetível de constituir risco de *compliance* (incumprimento⁵⁶). Com efeito, para o Comité, o risco de *compliance* define-se como «[...] *the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its bank activities* [...]»⁵⁷.

⁵⁴ No artigo 28.º, n.º 1, alude-se ao «risco de incumprimento de obrigações legais, regulamentares e outros deveres [...]». Antecipamos, por isso, que na definição das categorias de risco, as instituições continuarão, no que se refere ao agora denominado «risco de conformidade», a socorrer-se da definição constante do Aviso do BdP n.º 5/2008, já revogado.

⁵⁵ LABAREDA, João (2014), p. 32.

⁵⁶ O «risco de reputação» era definido autonomamente na alínea j) do n.º 4 do artigo 11.º do Aviso do BdP n.º 5/2008. À semelhança do que se referiu a propósito do risco de *compliance*, atualmente também não encontramos no Aviso do BdP n.º 3/2020 uma definição para risco de reputação, embora o mesmo esteja consagrado no Anexo I à Instrução do BdP n.º 18/2020 (sob a designação «risco reputacional»).

⁵⁷ *Compliance and compliance function in banks*, p. 7, disponível em <https://www.bis.org>, acessível em 25.01.2020.

Em nossa opinião, o risco de *compliance* deve conter, pelo menos, as seguintes dimensões: risco de continuidade de negócio, risco pecuniário e sancionatório e risco reputacional.

As irregularidades que podem consubstanciar situações de risco de *compliance* são, dada a amplitude da respetiva definição, as mais variadas. Em causa está, designadamente, a prática de crimes, de contraordenações, infrações disciplinares, o incumprimento contratual, enfim, o incumprimento de deveres legais ou deveres não legais que possam gerar consequências desfavoráveis para a IC, mormente no plano económico, financeiro e reputacional. No entanto, estando o objeto do nosso estudo intrinsecamente ligado ao BdP, centrar-nos-emos nas contraordenações que a este caiba sancionar.

Dos vetores acima descritos surge o dever legal de as IC criarem e implementarem medidas e procedimentos destinados a prevenir, detetar e reagir a riscos de *compliance*. Um dos procedimentos reativos de que a instituição pode lançar mão para o efeito é, conforme se referiu, as investigações internas, que passaremos a tratar.

2. As Investigações internas

2.1. Definição e objeto

Do acima exposto resulta que as investigações internas derivam do sistema de controlo interno (e do exercício da respetiva função de *compliance*), integrando-o e garantindo-lhe eficácia⁵⁸. As investigações inserem-se na função de *compliance* enquanto medida ou procedimento que se destina a reagir a riscos de incumprimento das obrigações legais e dos deveres a que as instituições se encontram sujeitas, isto é,

⁵⁸ Por razões de economia referir-nos-emos adiante ao sistema de controlo interno, abarcando este, em sentido estrito, o (sub)sistema de controlo de cumprimento e a função de *compliance*.

riscos de *compliance*⁵⁹. Estas podem assim ser definidas⁶⁰ como um mecanismo de averiguação reativo, integrado no sistema de controlo interno, máxime na respetiva função de *compliance* que, face a uma suspeita de risco de *compliance*, materializado ou não, visa (i) determinar se a suspeita se confirma, (ii) identificar as pessoas envolvidas, com o objetivo último de (iii) reagir, controlando as consequências potenciais ou reais daquele risco, mediante a definição e a implementação de medidas para o efeito destinadas^{61/62}.

As investigações internas não constituem um mecanismo de controlo ou de monitorização periódico ou aleatório destinado à deteção de riscos de *compliance*, tratando-se, ao invés, de mecanismo reativo acionado em consequência do conhecimento de uma suspeita de irregularidade⁶³ que constitua um tal risco.

Cabendo à IC definir e formalizar, em documento, os procedimentos inerentes ao sistema de controlo interno⁶⁴, também as investigações internas, enquanto

⁵⁹ «*The stage of investigation involves a firm's policies and practices targeted at determining the existence of and, if relevant, scope of the compliance failure. Investigation requires discovering the facts surrounding the failure, so that decision makers at the firm are equipped with a sufficient amount of knowledge to make informed decisions about the appropriate next steps*» – MARTINEZ, Verónica Root (2019), pp. 223 e 224.

⁶⁰ EIKE BICKER, CHRISTIAN STEINLE e CHRISTOPH SKOUPIL, tomando por referência o ordenamento jurídico alemão – advertindo que, à data, não existem disposições legais específicas que obriguem as empresas a conduzirem investigações –, definem investigações internas como «*[...] a formal procedure that seeks to establish whether obligations applying under the relevant law or internal corporate regulations have been violated, and possibly define the corrective measures*» – BICKER, Eike, STEINLE Christian e SKOUPIL, Christoph (2020).

⁶¹ A doutrina define investigações internas do seguinte modo: «*[...] una herramienta de cumplimiento de carácter reactivo, que se activa por la existencia de una sospecha de irregularidad.*» – MARTÍN, Adán Nieto (2015), p. 232.

⁶² O Aviso do BdP n.º 5/2008 não regulava, em concreto, as investigações internas. Nesse aspeto, como veremos adiante, o Aviso do BdP n.º 3/2020 constitui um passo considerável, na medida em que nele se refere e se reconhece, em diversas ocasiões, a necessidade de se realizarem investigações internas, ainda que para um caso muito específico, a saber: o do mecanismo de participação de irregularidades, previsto no artigo 116.º-AA do RGICSF. Em nossa opinião, pela importância que representam no sistema de controlo interno, este diploma teria constituído uma boa oportunidade para surgirem reguladas, com maior amplitude e densificação, as investigações internas.

⁶³ O termo “suspeita” é aqui utilizado no sentido de factos que constituem risco de *compliance*, embora ainda não comprovados.

⁶⁴ Artigo 62.º do Aviso do BdP n.º 3/2020. Dever que já se encontrava consagrado no artigo 3.º, n.º 4, do Aviso do BdP n.º 5/2008.

procedimento integrante daquele sistema, estarão definidas e formalizadas em documento. Neste podem prever-se aspetos tão elementares como (i) o modo de iniciar uma investigação, (ii) a competência para lhe dar início e dirigi-la, (iii) que elementos podem ser recolhidos e (iv) o destino a dar a tais elementos, enfim todos os aspetos relevantes à tramitação deste procedimento interno.

As investigações, enquanto procedimento interno da instituição, podem afetar direitos fundamentais como a reserva da intimidade da vida privada, devendo estar, por isso, como refere a doutrina, sujeitas a regras bem definidas⁶⁵. Com efeito, no acesso a documentos internos da empresa e nas entrevistas a trabalhadores estão em causa matérias sensíveis, não só do ponto de vista negocial ou comercial, mas da própria intimidade da vida privada das pessoas envolvidas, circunstância que requer cautelas e sobretudo (auto)regulação.

Pode dizer-se que na investigação conduzida pela IC existe já um certo grau de privatização da regulação e da justiça, na medida em que a instituição atua, em certa medida, como uma extensão ou braço coadjuvante do Regulador na supervisão⁶⁶: o Regulador, ao impor apertados mecanismos de controlo interno às IC, está, pelo menos, em parte, a assumir funções de supervisão em segunda linha, cometendo à instituição a tarefa principal de policiamento⁶⁷.

Esta circunstância traz evidentes vantagens, pois seria praticamente impossível ao Regulador supervisionar todas as IC com a extensão e o grau de profundidade necessários que a preservação e a estabilidade do sistema financeiro exigem. Com efeito, quem melhor do que a própria IC para controlar, através de uma função independente, a sua atividade, detetando e investigando riscos de *compliance*? Tal circunstância define o modelo relacional entre a IC e o Regulador: se o sistema de

⁶⁵ MARTÍN, Adán Nieto (2015a), p. 232.

⁶⁶ Veja-se, a propósito, da chamada “delegação” do poder público, GERALDO, Tiago (2018), p. 276.

⁶⁷ O Regulador tem a tarefa de fiscalizar a resiliência do sistema de controlo interno da instituição, mas é a esta que cabe, através daquele sistema, cumprir e fazer cumprir as normas aplicáveis.

controlo interno da IC funcionar, de modo pleno, eficaz e independente, o Regulador tem maiores certezas de que a fiscalização que a IC exerce sobre si própria funciona.

2.2. Das modalidades das investigações internas

A doutrina distingue diversas classificações de investigações internas, consoante o respetivo objeto⁶⁸. Adiante passamos a indicar aquelas que consideramos fazer sentido no universo das investigações internas realizadas pelas IC.

Em primeiro lugar, investigações em sentido estrito de investigações em sentido amplo, «consoante participem no esclarecimento dos factos somente advogados externos ou também membros da própria empresa, respetivamente»⁶⁹. Com efeito, conforme referimos, nada obsta a que a investigação fique a cargo de uma entidade externa, designadamente de um advogado ou de um escritório de advogados, desde que nas condições mais bem descritas *supra*.

Em segundo lugar, investigações de carácter nacional de investigações de carácter internacional, consoante se trate de pessoas coletivas nacionais ou internacionais (ou de âmbito internacional)⁷⁰. Será o caso, por hipótese, de uma IC com sede em Portugal determinar a abertura de uma investigação interna numa sua sucursal no estrangeiro.

A doutrina distingue, em terceiro lugar, investigações pré-judiciais de investigações para-judiciais. Nas primeiras, como o próprio nome indica, os factos não têm relação com qualquer processo judicial. Nas segundas, ao invés, averiguam-se factos que já são investigados num processo judicial (em nossa opinião, extensível a processos de

⁶⁸ Para uma classificação alargada, a respeito das empresas em geral, *vide* CUADRAS, Albert Estrada I e ANGLÍ, Mariona Llobet (2014), pp. 157 a 159.

⁶⁹ Tradução livre do texto original: «*según participen e el esclarecimiento de los hechos solamente abogados o también miembros de la propia empresa, respectivamente*» – MONTIEL, Juan Pablo (2013), pp. 260.

⁷⁰ MONTIEL, Juan Pablo (2013), pp. 260.

contraordenação), sendo, porventura, através desse processo e da respetiva publicidade que a instituição tem conhecimento dos factos em causa^{71/72}.

Adicionalmente, propomos distinguir investigações imediatas das investigações internas diferidas, consoante seja ou não possível, após o conhecimento dos factos pela instituição, dar início à investigação. A título de exemplo, parece-nos que, tendo a instituição tomado conhecimento dos factos através de um inquérito criminal ou de um processo de contraordenação que se encontrem sujeitos a segredo de justiça, esta pode, na prática, ter de sustar o início da investigação, na medida em que (e se) essa atividade tenha como consequência a revelação a terceiros de factos sujeitos a segredo⁷³.

2.3. Da competência para iniciar, dirigir e realizar uma investigação

Nos termos do disposto no artigo 15.º, n.º 2, do RGICSF, a gestão corrente da instituição é confiada ao órgão de administração, que detém poderes de orientação efetiva da atividade da instituição⁷⁴.

Por seu turno, dispõe o artigo 12.º, n.º 1, alínea b), do Aviso do BdP n.º 3/2020 que «o órgão de administração da instituição estabelece e mantém um sistema de controlo interno [...] com o objetivo de garantir a sustentabilidade da instituição no médio e longo prazo e o exercício prudente da sua atividade, através [...] b) Da adequada identificação, avaliação, acompanhamento e controlo dos riscos a que a instituição está ou pode vir a estar exposta», sendo «[...] globalmente responsável por uma

⁷¹ MONTIEL, Juan Pablo (2013), pp. 261.

⁷² Por hipótese, a instituição inicia uma investigação interna na sequência da acusação em processo penal deduzida contra membros do órgão de administração. Neste caso, a instituição tem conhecimento de factos que podem constituir risco de *compliance* em consequência da existência de um processo-crime.

⁷³ O dever de segredo não se esgota no segredo de justiça, abrangendo também o chamado “segredo de supervisão” (artigo 80.º do RGICSF).

⁷⁴ Artigo 15.º, n.º 1, do RGICSF.

adequada gestão de todos os riscos a que a instituição está ou pode vir a estar exposta.⁷⁵».

O órgão de administração é igualmente responsável por implementar um sistema de gestão de riscos, que têm como objetivo a identificação, avaliação, acompanhamento e controlo de todos os riscos⁷⁶.

Da leitura das disposições acima referidas, decorre que o órgão de administração é o centro nevrálgico do sistema de controlo interno, o seu expoente máximo⁷⁷, portanto, competindo-lhe definir e implementar um sistema com as características atrás assinaladas⁷⁸. Porém, é a partir e através das funções que integram o sistema de controlo interno, que o órgão de administração colhe a concretização necessária para a efetivação do sistema por si desenhado.

Ora, por caber, em especial, à função de *compliance*, o dever de controlar o cumprimento das obrigações e dos deveres a que as IC se encontram sujeitas, parece-nos que é também a esta função que compete iniciar e dirigir uma investigação.

Cabendo à função de *compliance* iniciar uma investigação, a direção da investigação é da competência do respetivo responsável. Ao responsável por aquela função compete definir as traves-mestras da investigação, delimitando a atuação dos seus subordinados, em especial – no que releva para efeitos do presente trabalho – em matéria de recolha de elementos.

⁷⁵ Artigo 19.º, n.º 4, do Aviso do BdP n.º 3/2020.

⁷⁶ Artigo 19.º, n.º 1, do Aviso do BdP n.º 3/2020.

⁷⁷ É, aliás, essa a tónica que ressalta ao longo de todo o Aviso do BdP n.º 3/2020.

⁷⁸ Não obstante, como se referiu, o órgão de administração assuma um papel central na definição e na implementação do sistema de controlo interno, este deve assegurar que as funções de controlo, mormente a função de *compliance*, atuam de modo independente (artigo 15.º, n.º 2, do Aviso do BdP n.º 3/2020).

Questão distinta prende-se com a circunstância de saber quem deve realizar a investigação.

Conforme se referiu, compete à função de *compliance* investigar um determinado risco de *compliance*, cabendo-lhe, em especial, iniciar e dirigir (pela mão do respetivo responsável) a investigação. Por via de regra, exclui-se «a possibilidade de externalização da função [de cumprimento], ancorada num qualquer regime de prestação de serviços. [...] Contudo, tarefas específicas que possam ser abrangidas nesse expediente, devem elas ficar sempre sujeitas à supervisão do responsável de cumprimento»⁷⁹.

Consentâneo com este entendimento é o já citado documento produzido pelo Comité de Basileia, referindo, a este propósito, que deve estar expressamente prevista em documento a possibilidade de a função de *compliance* «conduzir investigações a possíveis quebras da política de compliance e o direito de designar especialistas externos para desempenharem a tarefa, caso tal seja apropriado»⁸⁰.

No plano regulamentar nacional, dispõe o Aviso do BdP n.º 3/2020 que «[a]s instituições podem subcontratar tarefas operacionais das funções de controlo interno, caso a subcontratação não tenha impacto negativo na eficiência do sistema de controlo interno e desde que obtido o prévio consentimento dos órgãos de administração e fiscalização»⁸¹, devendo a subcontratação, em qualquer caso, ocorrer a título ocasional, salvo situações excepcionais, devidamente fundamentadas⁸².

Não obstante admitamos que o artigo 36.º do Aviso do BdP n.º 3/2020 não tenha sido especificamente pensado para a subcontratação da tarefa de levar a cabo uma

⁷⁹ LABAREDA, João (2014), p. 44.

⁸⁰ Tradução livre do texto original: «conduct investigations of possible breaches of the compliance policy and to appoint outside experts to perform the task if appropriate» in «Compliance and compliance function in Banks», p. 11, disponível em <https://www.bis.org>, acessível em 25.01.2020.

⁸¹ Artigo 36.º, n.º 1, do Aviso do BdP n.º 3/2020.

⁸² Artigo 36.º, n.º 2, do Aviso do BdP n.º 3/2020.

investigação interna, parece-nos que tal possibilidade tem cabimento no âmbito do aludido preceito. Entendemos, por isso, que, constituindo a investigação de riscos de *compliance* tarefa específica da função de *compliance*, nada impede que a mesma seja subcontratada a uma entidade externa, por hipótese, um advogado, na qualidade de especialista, desde que (i) seja de ocorrência ocasional, (ii) autorizada pelo órgão de administração e de fiscalização e que (iii) a condução da investigação esteja necessariamente sob a supervisão do responsável por aquela função⁸³. É, no entanto, essencial assegurar que o advogado em questão, não se encontra inscrito ou registado em jurisdição com um regime legal que preveja proibições ou restrições que impeçam ou limitem o cumprimento, pela instituição, das normas legais e regulamentares que regem a respetiva atividade, incluindo ao nível da prestação e da circulação de informação⁸⁴.

Em suma, a investigação de riscos de *compliance* é iniciada, dirigida e realizada pela função de *compliance*, não obstante nada impeça a (sub)contratação de uma entidade externa para desempenhar as referidas funções, desde que sejam observadas as condições acima assinaladas e mais bem descritas no Aviso do BdP n.º 3/2020.

2.4. Das fases da investigação

2.4.1 Da abertura da investigação

Conforme se referiu, as investigações internas têm carácter reativo, *i. e.*, iniciam-se na sequência da tomada de conhecimento de um risco de *compliance*.

São várias as fontes de conhecimento de um determinado risco de *compliance*. Este pode provir, designadamente, (i) de uma participação⁸⁵, (ii) de um relatório de

⁸³ Artigo 36.º, n.º 7, do Aviso do BdP n.º 3/2020.

⁸⁴ Artigo 36.º, n.º 3, alínea b), do Aviso do BdP n.º 3/2020.

⁸⁵ Feita diretamente a um superior hierárquico ou através do “canal de denúncias” (artigo 116.º-AA, n.º 1, do RGICSF ou artigo 305.º-F do CVM, por exemplo). De acordo com as orientações da EBA

auditoria de *compliance*, (iii) da imprensa⁸⁶ ou (iv) de um processo que, designadamente, corra termos num tribunal ou numa autoridade administrativa⁸⁷.

Começando pelas comunicações de práticas irregulares, «[a]s instituições de crédito devem implementar os meios específicos, independentes e autónomos adequados de receção, tratamento e arquivo das participações de irregularidades graves com a administração, organização contabilística e fiscalização interna e de indícios sérios de infrações a deveres previstos no Regime Geral ou no Regulamento (UE) n.º 575/2013 [...]»^{88/89}.

Acresce que «[a]s participações recebidas nos termos dos números anteriores são analisadas, sendo preparado um relatório fundamentado, que deve conter as medidas adotadas ou a justificação para a não adopção de quaisquer medidas»⁹⁰.

Embora a letra da lei não determine expressamente a abertura de uma investigação em caso de comunicação de práticas irregulares, o certo é que, ao estipular a respetiva análise, a elaboração de um relatório fundamentado e, bem assim, de um relatório anual que deve conter «o resultado da investigação»⁹¹, está, necessária e implicitamente, a pressupor a condução, pela IC, de um conjunto de diligências

em matéria de governo interno, «[a] fim de evitar conflitos de interesses, deverá ser possível comunicar infrações fora dos canais normais de transmissão de informações (p. ex., através da função de verificação do cumprimento, da função de auditoria interna ou de um procedimento independente de denúncia a nível interno). Os procedimentos de alerta devem assegurar a proteção dos dados pessoais quer da pessoa que comunica a infração quer da pessoa singular que é alegadamente responsável pela infração, nos termos da Diretiva 95/46/CE» (p. 31) disponíveis em: <https://eba.europa.eu>, acessível em 22.01.2020.

⁸⁶ Fazendo referência à imprensa, MARTÍN, Adán Nieto (2015a), p. 232.

⁸⁷ A este propósito, ver ponto 2.2. *supra* (modalidade para-judicial).

⁸⁸ Artigo 116.º-AA, n.º 1, do RGICSF.

⁸⁹ Encontramos no artigo 305.º-F do CdVM preceito legal similar, regulando a comunicação interna de factos, as provas e as informações.

⁹⁰ Artigo 116.º-AA, n.º 4, do RGICSF, densificado pelo artigo 35.º, n.º 2, alínea f), do Aviso do BdP n.º 3/2020.

⁹¹ Cfr. artigo 8.º, n.º 1, alínea b), parágrafo vi) da Instrução do BdP n.º 18/2020.

destinadas **(i)** à comprovação da participação, *rectius*, à condução de uma investigação e **(ii)** à correção do risco de *compliance* detetado e comprovado⁹².

Ademais, o conhecimento de suspeitas de irregularidades que possam constituir risco de *compliance* pode ter origem, conforme se referiu *supra*, em quaisquer ações e avaliações periódicas e ou extraordinárias de controlo no exercício do processo de monitorização do sistema de controlo interno (auditorias de *compliance*)⁹³.

Coloca-se, nesta sede, a questão de se saber se toda e qualquer irregularidade que constitua risco de *compliance* gera, para a IC, o dever de iniciar diligências destinadas a investigá-la e a comprová-la ou se, pelo contrário, tal dever apenas existe em relação a determinadas irregularidades, porventura em função da gravidade que se lhes atribua⁹⁴.

⁹² Por se afigurar um lugar paralelo, tem interesse referir o artigo 305.º-F do CVM, que vai mais longe em termos de densificação, merecendo destaque o dever de descrever as diligências internas efetuadas de averiguação da factualidade participada, bem como os meios de prova usados para tal.

⁹³ Designam-se por auditorias de *compliance*, as ações ou avaliações conduzidas pela IC com uma base contínua ou periódica, por vezes diária, sem que haja prévio conhecimento da existência de um qualquer risco de *compliance*, que têm em vista avaliar o nível de eficácia do sistema de gestão de *compliance* da IC. «La auditoria, y sea realizada por los servicios propios de la empresa (auditoria interna) o por una auditoria externa, tiene como función comprobar el grado de funcionamiento del sistema, sin que existan sospechas de que se ha cometido algún tipo de irregularidad. Por el contrario, la investigación interna parte de la sospecha de que se ha cometido una irregularidad. Como ya se ha dicho tiene carácter reactivo.» – MARTÍN, Adán Nieto (2015), p. 232. As auditorias de *compliance*, para além de integradas no sistema de controlo interno, inserem-se no respetivo processo de monitorização, enquanto «[...] ações e avaliações de controlo desenvolvidas pelas instituições com vista a garantir a adequação e eficácia da cultura organizacional da instituição e dos sistemas de governo e controlo interno, nomeadamente, através da identificação de deficiências na conceção dos controlos, incluindo as relacionadas com a inexistência de controlos, e na sua implementação» – Artigo 31.º, n.º 1, do Aviso do BdP n.º 3/2020 (corresponde parcialmente ao artigo 21.º, n.º 1, do Aviso n.º 5/2008). No entanto, ao contrário das auditorias de *compliance* que têm carácter de deteção, as investigações surgem na sequência de um concreto conhecimento, tendo, por essa razão, conforme se referiu, carácter reativo. Donde não é de estranhar que a auditoria de *compliance* possa, por vezes, constituir a génese de determinada investigação interna, bastando pensar na seguinte situação: o risco de *compliance* detetado em sede de auditoria de *compliance*, a montante, é, depois, investigado, a jusante, numa investigação interna que lhe sucede. Numa situação como esta, a investigação interna é desencadeada na sequência de um mecanismo de monitorização que, de forma estandardizada, detetou determinado risco de *compliance*, ulterior e autonomamente investigado em procedimento interno que lhe é dedicado.

⁹⁴ A título de exemplo, embora a respeito de uma matéria distinta, o artigo 116.º-AA, n.º 1, do RGICSF, dispõe que apenas existe obrigação de comunicação relativamente a irregularidades graves (embora o legislador não especifique o que se entende por irregularidade grave). Para uma

Ao contrário da generalidade das empresas em mercado não regulado, no domínio das IC, estas devem dispor necessariamente de um sistema de controlo interno – assente num sistema e numa função de *compliance* permanente e efetiva –, que visa, entre outros aspetos, garantir «[...] a adequação e a eficácia das medidas e procedimentos adotados para detetar qualquer risco de incumprimento das obrigações legais, regulamentares e outros deveres a que a instituição se encontra sujeita, bem como das medidas tomadas para corrigir eventuais deficiências detetadas⁹⁵». Esta função está encarregada de prestar imediatamente «aos órgãos de administração e de fiscalização toda a informação de que dispõe sobre quaisquer indícios de violação de obrigações legais e regulamentares a que a instituição se encontra sujeita, de regras de conduta e de relacionamento com clientes ou de outros deveres que possam fazer incorrer a instituição ou os seus colaboradores num ilícito de natureza contraordenacional ou causar impacto reputacional negativo»⁹⁶.

Parece-nos, por isso, que a tomada de conhecimento, pela instituição, máxime, pelos seus órgãos de administração, pela função de *compliance* ou pelo seu responsável, de suspeitas de irregularidades que consubstanciem riscos de *compliance*, acarreta o dever reagir, *rectius*, o dever de desencadear as diligências necessárias e destinadas à respetiva investigação e comprovação.

Em suma, parece-nos que, atentas as finalidades do sistema de controlo interno, compete à função de *compliance* dar início a uma investigação sempre que a IC, por via dos seus órgãos e funções competentes, tomar conhecimento de quaisquer suspeitas de irregularidades⁹⁷ que constituam riscos de *compliance*: «[r]ealmente, de

abordagem mais densificada sobre o tema das participações de irregularidades e sobre o conceito de irregularidade grave, *vide* EÇA, Catarina Salazar de (2017), pp. 9 e seguintes.

⁹⁵ Artigo 28.º, n.º 1 alínea a), do Aviso do BdP n.º 3/2020.

⁹⁶ Artigo 28.º, n.º 1, alínea h), do Aviso do BdP n.º 3/2020.

⁹⁷ Em nossa opinião, atentas as características do sistema de controlo interno e respetivas funções, em especial da função de *compliance*, parece-nos deve ser iniciada uma investigação independentemente do concreto grau de suspeita. Se a suspeita se mostrar infundada, pois será esse

cada vez que há uma fractura neste propósito [o bem do cumprimento], nasce necessariamente o perigo de se produzirem consequências desfavoráveis para a instituição infractora»⁹⁸.

2.4.2 Da recolha de elementos na investigação

No decurso da investigação serão recolhidos⁹⁹ e analisados diversos elementos destinados a comprovar ou a afastar uma determinada suspeita de risco de *compliance*. Nesse sentido, cabe à função de *compliance* ou ao terceiro por esta designado, levar a cabo todas as diligências necessárias à averiguação do risco de *compliance* detetado.

2.4.3 Do relatório final e comunicação do resultado da investigação

A final será produzido um relatório fundamentado, que será apresentado ao órgão de administração¹⁰⁰. Este conterá: (i) a descrição dos factos, das diligências realizadas e, bem assim, dos elementos recolhidos e produzidos¹⁰¹, a qualificação jurídica dos factos e as respetivas consequências jurídicas¹⁰², a descrição das medidas tomadas ou a tomar para corrigir eventuais deficiências no respetivo cumprimento, contendo uma

o resultado da investigação. Ao invés, em sentido aparentemente contrário, cumpre mencionar que, de acordo com a EBA uma investigação somente deve ser iniciada se existir um grau de certeza suficiente (Orientações sobre governo interno, p. 31, disponíveis em <https://eba.europa.eu>, acessível em 22.01.2020).

⁹⁸ LABAREDA, João (2014), p. 31.

⁹⁹ Para maiores desenvolvimentos, *vide* Capítulo II *infra*.

¹⁰⁰ Artigo 28.º, n.º 1, alínea h), do Aviso do BdP n.º 3/2020. Relevante era também o já revogado 17.º, n.º 1, alínea d), do Aviso do BdP n.º 5/2008. De acordo com as orientações da EBA em matéria de governo interno, «os procedimentos de alerta a nível interno devem: [...] assegurar que as infrações potenciais ou reais denunciadas são avaliadas e transmitidas ao nível hierárquico superior, incluindo, se for caso disso, à respetiva autoridade competente ou agência responsável pela aplicação da lei [...]» (p. 32), disponíveis em: <https://eba.europa.eu>, acessível em 22.01.2020.

¹⁰¹ Neste sentido, MARTÍN, Adán Nieto (2015a), p. 258. Encontramos acolhimento desta solução no que respeita às investigações internas que têm lugar na sequência de participações de irregularidades (artigo 8.º, n.º 1, alínea b), subparágrafo iv) da Instrução do BdP n.º 18/2020). Sendo também de destacar, pela sua similitude, o artigo 305.º-F, n.º 4, alínea a), do CdVM.

¹⁰² Encontramos acolhimento desta solução no artigo 8.º, n.º 1, alínea b), subparágrafo iii) da Instrução do BdP n.º 18/2020 e, bem assim, no artigo 305.º-F, n.º 4, alínea d), do CdVM.

(re)avaliação do sistema de controlo interno¹⁰³ e (iii) a justificação para a não adoção de quaisquer medidas¹⁰⁴.

Quanto à forma do relatório, parece-nos ser boa prática¹⁰⁵ que o mesmo seja reduzido a escrito, devendo ser conservado durante o prazo de 5 (cinco) anos¹⁰⁶.

De referir também que as IC estão obrigadas a apresentar ao BdP um relatório anual com a indicação sumária das participações recebidas e do respetivo processamento¹⁰⁷, o que significa que as conclusões constantes do relatório final, coincidindo o risco de *compliance* com irregularidades contempladas no artigo 116.º-AA do RGICSF, devem ser sumariamente dadas a conhecer à entidade reguladora.

¹⁰³ MARTÍN, Adán Nieto (2015a), p. 258.

¹⁰⁴ Artigo 116.º-AA, n.º 4, do RGICSF, no caso específico do mecanismo de participação de irregularidades.

¹⁰⁵ Mesmo nos casos em que tal imposição não resulte diretamente do artigo 116.º-AA do RGICSF (por não estar em causa a participação de uma irregularidade), parece-nos que o relatório deve ser reduzido a escrito e conservado.

¹⁰⁶ Por aplicação do disposto no artigo 116.º-AA, n.º 5, do RGICSF. O artigo 305.º-F, n.º 6, do CVM estabelece um prazo idêntico de conservação.

¹⁰⁷ Artigo 116.º-AA, n.º 7, do RGICSF e artigo 8.º da Instrução do BdP n.º 18/2020.

CAPÍTULO II – DA RECOLHA DE ELEMENTOS NAS INVESTIGAÇÕES INTERNAS

1. Introdução

Conforme se referiu, o objeto da investigação consiste numa determinada suspeita de risco de *compliance*. Através da investigação procede-se à averiguação e à comprovação (internas) dos factos sob suspeita, tendo em vista a ulterior neutralização do risco de *compliance*.

A investigação contém uma necessária fase de recolha de elementos com base nos quais o investigador irá formular e suportar as conclusões que irá verter no seu relatório subsequente. Tais elementos constituem a prova.

A prova é, seja qual for a natureza do processo – penal, civil, disciplinar ou outro – «a atividade desenvolvida [...] no sentido do convencimento da realidade de um facto»¹⁰⁸. O objeto da prova é, pois, o «facto juridicamente relevante»^{109/110}. Não obstante prova e objeto da prova tenham uma conotação associada a um processo, socorrer-nos-emos dessa mesma terminologia no contexto das investigações internas, para que possamos identificar realidades similares e lugares paralelos com maior facilidade.

Nesse sentido, o “objeto da prova”, no contexto de uma investigação interna, consiste em qualquer facto suscetível de demonstrar, isolada ou conjuntamente, a verificação de determinado risco de *compliance*¹¹¹. A atividade de demonstração da realidade dos

¹⁰⁸ PIMENTA, Paulo (2014), p. 336.

¹⁰⁹ ALBUQUERQUE, Paulo Pinto (2018), p. 329.

¹¹⁰ Nos termos do disposto no artigo 341.º do CC, «[a]s provas têm por função a demonstração da realidade dos factos».

¹¹¹ Artigo 11.º, n.º 4, alínea f), do já revogado Aviso do BdP n.º 5/2008: «a probabilidade de ocorrência de impactos negativos nos resultados ou no capital [*in casu*, da IC], decorrentes de violações ou da não conformidade relativamente a leis, regulamentos, determinações específicas,

factos, por seu turno, «passa pela utilização de meios susceptíveis de assegurar aquele convencimento, ou seja, passa pela utilização de meios de prova»^{112/113}.

A recolha de elementos (prova) no contexto de uma investigação interna é feita por particulares (o investigador, independentemente de quem, em concreto, seja investido nessa qualidade). Estes atuam desprovidos de poderes públicos, circunstância que suscita diversas questões quanto aos elementos que podem ser recolhidos e utilizados no decurso da investigação.

Para fins estritamente académicos, procedemos à análise de diversas políticas de comunicação de irregularidades¹¹⁴ (artigo 116.º-AA, do RGICSF), sendo possível verificar, como traço comum a cada uma delas, o seguinte: **(i)** não regulam exaustivamente as investigações e **(ii)** em matéria de recolha de elementos, não estipulam qualquer restrição quanto ao respetivo conteúdo e alcance¹¹⁵.

Porém, a ausência de regulamentação legal não tem, naturalmente, como consequência a admissibilidade de todo e qualquer meio de prova. Com efeito, não

contratos, regras de conduta e de relacionamento com clientes, práticas instituídas ou princípios éticos, que se materializam em sanções de carácter legal, na limitação de oportunidades de negócio, na redução do potencial de expansão ou na impossibilidade de exigir o cumprimento de obrigações contratuais». Conforme referimos, apesar de não surgir definido, este risco encontra-se expressamente incluído no catálogo de riscos previsto no Anexo I à Instrução do BdP n.º 18/2020, que regulamenta o Aviso n.º 3/2020.

¹¹² PIMENTA, Paulo (2014), p. 337.

¹¹³ Na perspetiva do Direito Penal, «As provas – enquanto meios de prova – são os elementos com base nos quais os factos relevantes podem ser demonstrados» (cfr. MENDES, Paulo Sousa (2004), p. 133). «Os meios de prova formam-se no momento da sua própria produção no processo, visando a “reprodução” (“avaliação”) do facto e, nessa medida, constituindo um meio de aquisição para o processo de uma prova “posterior” à prática do crime.» (ALBUQUERQUE, Paulo Pinto (2018), p. 331)

¹¹⁴ A título de exemplo, (i) Caixa Central de Crédito Agrícola Mútuo, C.R.L., disponível em <http://www.creditoagricola.pt>; (ii) Bankinter, S.A. – Sucursal em Portugal, disponível em <http://www.bankinter.pt>; (iii) Banco Comercial Português, S.A., disponível em <http://www.millenniumbcp.pt>; (iv) Novo Banco, S.A., disponível em <http://www.novobanco.pt> e (v) Banco Efisa, disponível em <http://www.bancoefisa.pt>, acessível em 20.06.2020.

¹¹⁵ No caso do Novo Banco, S.A. prevê-se inclusivamente que «o Conselho Geral e de Supervisão desenvolve as diligências que entender necessárias, designadamente, a obtenção de prova [...]», não prevendo quaisquer restrições em matéria de recolha de meios de prova.

são, desde logo, admissíveis os meios de prova que ponham em causa direitos ou interesses legalmente protegidos, como o bom nome e reputação, a imagem, a palavra e a reserva da intimidade da vida privada e familiar¹¹⁶. De igual modo, não nos parecem admissíveis os meios de prova recolhidos mediante «tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações»¹¹⁷ e, por maioria de razão, todos aqueles que, de uma maneira geral, sejam proibidos nos termos da legislação penal, por ofenderem direitos, liberdades e garantias¹¹⁸.

Na verdade, apesar de não estarmos no âmbito de uma atividade processual e, muito menos, no âmbito de uma atividade processual conduzida num processo penal, parece-nos indiscutível que as provas e a sua admissibilidade no direito privado devem conformar-se com o disposto no artigo 32.º, n.º 8, da CRP, e, bem assim, com as normas que dele dimanam, como é especificamente o caso do artigo 126.º, n.º 3, do CPP¹¹⁹. O que vale para o processo penal – processo em que existem, por natureza, potenciais lesões a direitos fundamentais dos arguidos – deve valer, por maioria de razão, para os demais processos e procedimentos, tenham eles natureza pública ou privada.

Acresce que, face ao paralelismo que se estabelecerá adiante entre as investigações internas e o processo disciplinar laboral¹²⁰, adiantamos que, no processo disciplinar

¹¹⁶ Artigo 26.º, n.º 1, da CRP.

¹¹⁷ Artigo 32.º, n.º 8, da CRP, preceito que tem, depois, correspondência aplicada no artigo 126.º do CPP.

¹¹⁸ Artigo 126.º do CPP.

¹¹⁹ O TRP assim sustentou, em termos análogos para o processo civil, através de acórdão proferido no processo n.º 10795/08.8TBVNG-A.P1, em 15.04.2010, disponível em <http://www.dgsi.pt>.

¹²⁰ No sentido de tal paralelismo, *vide* ALMEIDA, Joana (2020), p. 68.

laborar, tem sido sustentada a aplicação do n.º 8 do artigo 32.º da CRP, reconhecendo entre este processo e o processo criminal, para este efeito, similitude^{121/122}.

Centrando a questão, o palco das investigações internas é, em regra, o local de trabalho, enquanto espaço físico, no qual o investigador se movimenta, com maiores ou menores restrições, consoante o grau de acesso que lhe seja concedido pelo responsável pela função de *compliance* e/ou pelos dirigentes da instituição¹²³. Mas, atendendo a que o suporte da informação com interesse para a investigação não é só físico, mas também digital, a atividade de investigação não se cinge ao espaço físico, abrangendo quaisquer infraestruturas, designadamente servidores alocados à instituição, nos quais seja armazenada a informação. Certo é que, ao movimentar-se no local de trabalho e pelas infraestruturas adjacentes, o investigador tem, em abstrato, potencialmente acesso a diversos elementos que são produzidos na dinâmica e no contexto laboral: designadamente, faturas, contratos, manuais de procedimento, aos próprios colaboradores e, no que releva para efeitos do presente trabalho, ao conteúdo de mensagens de correio eletrónico.

Como se pode razoavelmente intuir, caso não sejam observados determinados limites, a atividade de recolha desses elementos é suscetível de colidir com direitos fundamentais de trabalhadores ou de terceiros que com aqueles se relacionem¹²⁴. Numa investigação sem limites, o investigador (i) acederá a documentação existente na IC, sem cuidar de saber se os factos constantes nos documentos estão abrangidos

¹²¹ Constituem exemplos o acórdão do STJ, proferido no processo 07S043, em 05.07.2007 e o acórdão do TRP, proferido no processo 101/13.5TTMTS.P1, em 09.08.2014, ambos disponíveis em <http://www.dgsi.pt>. Na doutrina, vide, designadamente, ALVES, Lurdes Dias, (2020), p. 21.

¹²² Ora, conforme se explanará adiante, parece-nos que o estudo das investigações internas beneficia da extração e subsequente adaptação das regras aplicáveis ao processo disciplinar laboral.

¹²³ O local de trabalho «corresponde ao lugar físico de cumprimento da prestação de trabalho, o que habitualmente coincide com as instalações da empresa ou com o estabelecimento do empregador.» (RAMALHO, Maria do Rosário Palma (2016), p. 340).

¹²⁴ «Resulta evidente que la empresa que realiza una investigación interna puede acceder a las comunicaciones de sus empleados, al registro de sus llamadas o de páginas web visitadas de un modo más sencillo que el fiscal o el juez. Por lo tanto, los costes de acceso a esa información son menores que en el proceso penal, si bien, en la misma medida en que lo son las garantías.» – PENA, Ana María Neira (2015), p. 69.

pelo segredo profissional, **(ii)** entrevistará trabalhadores sem os informar dos direitos que lhes assistem, bem como o destino que pode ser dado aos respetivos depoimentos, que serão reduzidos a escrito e **(iii)** acederá ao conteúdo de mensagens de correio eletrónico, independentemente da sua natureza (pessoal ou profissional), com a justificação de que as mesmas podem conter informação relevante para a investigação. A investigação que é conduzida sem limites falha enquanto investigação e constitui a demonstração clara de um sistema de controlo interno deficitário.

Podemos verificar que a dinâmica gerada no decurso da investigação, decorrente, designadamente, da atividade de acesso a documentos, ao conteúdo de mensagens de correio eletrónico e da recolha de depoimentos de trabalhadores apresenta inegáveis semelhanças com a dinâmica estabelecida entre o empregador, ou instrutor por si nomeado, e os trabalhadores, em sede de um inquérito prévio ou mesmo em sede de um procedimento disciplinar laboral. Na verdade, dado que a investigação interna tem lugar no contexto de uma relação de Direito Privado, parece-nos que o estudo da fase de recolha de prova no contexto de uma investigação interna pode beneficiar de um relativo paralelismo com o trabalho (doutrinário e jurisprudencial) já realizado a propósito do Direito do Trabalho.

2. Das mensagens de correio eletrónico¹²⁵

2.1. Introdução

Com a introdução, nas empresas, das novas tecnologias de informação e comunicação, a *internet* surge como o meio de comunicação preferencial, designadamente, entre **(i)** o empregador e os trabalhadores, **(ii)** entre trabalhadores e

¹²⁵ Pelo especial interesse e atualidade da matéria, e por limitações de exposição, iremos, tão-somente, abordar a recolha deste elemento.

(iii) entre a empresa (incluindo os seus trabalhadores) e terceiros que com aquela se relacionem.

Enquanto meio de comunicação, a *internet* oferece serviços de comunicação, nos quais se inserem «o *e-mail*¹²⁶, os *newsgroups*, e a comunicação em tempo real entre os diferentes utilizadores, como é o caso dos *chats*»¹²⁷. Em determinadas condições, tais serviços de comunicação são suscetíveis de ser acedidos pelo empregador, como veremos adiante.

Ora, sucede que, ainda que o trabalhador esteja ciente da possibilidade de o empregador poder, em determinadas circunstâncias, aceder ao conteúdo das mensagens de correio eletrónico – designadamente, porque foi expressamente advertido nesse sentido, em momento prévio à prestação de trabalho ou no decurso da mesma –, o certo é que no dia-a-dia, isto é, no decurso da jornada de trabalho, o trabalhador tende a desvalorizar a possibilidade de tal ocorrência, um pouco como aquele que atua num ambiente controlado, sem ter consciência permanente de que “deve sorrir porque está a ser filmado”. Ao utilizar tais serviços de comunicação, o trabalhador não é permanentemente destinatário de qualquer aviso ou notificação, e assim, de forma mais ou menos espontânea, acaba por comunicar convicto de que lhe assiste um espaço de liberdade de comunicação que é intransponível. Nessa comunicação, aparentemente livre, ficam registados dados que podem relevar para a investigação. Podendo relevar, há o risco de serem recolhidos de forma abusiva.

¹²⁶ «A comunicação eletrónica é rápida e desmaterializada, poupando os gastos e peripécias do tradicional correio por via postal. Isto não obsta, todavia, a que o *email* envolva um variado conjunto de perigos para a segurança dos dados pessoais de quem através dele envie e receba informações.» – SILVEIRA, Luís Lingnau da (2011), p. 142. «O *e-mail* – *electronic mail* – é uma caixa de correio eletrónico que utiliza dois tipos de protocolo, o POP 3 e o SMTP, para o envio do cliente ao servidor quando aquele solicita visualização do seu correio e entre servidores quando a mensagem é enviada de um cliente para o outro. Assim, o *email*, permite que uma pessoa envie uma mensagem electrónica para outra pessoa ou para um conjunto de endereços electrónicos. A mensagem é, geralmente, armazenada por meios electrónicos num servidor, à espera que o destinatário vá verificar a sua caixa de correio electrónico. Esta mensagem pode ser composta quer por texto, imagem e, por vezes, áudio [...].» – MOREIRA, Teresa Coelho (2010), p. 37.

¹²⁷ MOREIRA, Teresa Coelho (2010), p. 38.

Estando assente que «ninguém pode interferir [na relação comunicacional], a não ser que se trate de situações expressamente previstas em sede de legislação penal»¹²⁸, resta-nos compreender em que condições pode o investigador aceder ao conteúdo das mensagens de correio eletrónico, remetidas ou recebidas por colaboradores¹²⁹ da IC na qual a investigação tem lugar.

Situando-se o objeto do nosso estudo no contexto do Direito privado, porventura até no domínio de uma relação laboral, as preocupações com a proteção da privacidade e com a inviolabilidade das comunicações privadas encontram, designadamente, no Direito do Trabalho, no Direito da Proteção de Dados e no Direito Civil, amparo para a generalidade das questões que se possam colocar. O Direito do Trabalho e o Direito da Proteção de Dados têm uma inelutável conexão entre si, devendo, por conseguinte, ser articulados, conforme veremos adiante. Acresce que no contexto de uma investigação, na tensão que se possa gerar entre a tutela da reserva da vida privada e os meios disponíveis ao investigador para a descoberta da verdade, estes últimos saem claramente vencidos.

Não obstante, é necessário destacar que a aludida tensão não tem paralelo com aquela que possa ocorrer em relação à generalidade das empresas, na medida em que na investigação de uma suspeita de risco *compliance*, que tenha lugar no contexto de uma IC, a imposição de um efetivo e permanente sistema de controlo interno não tem somente em vista a contenção de eventuais consequências desfavoráveis para instituição, que decorram da verificação de determinado risco de *compliance*. Está em causa assegurar a «estabilidade e a sobrevivência» da mesma como pressuposto fundamental da preservação da confiança e da estabilidade do sistema financeiro¹³⁰ e

¹²⁸ NEVES, Rita Castanheira (2011), p. 29.

¹²⁹ O termo colaborador é aqui propositadamente utilizado, com o intuito de abranger prestadores de serviços e trabalhadores.

¹³⁰ Conforme resultava do preâmbulo do Aviso do BdP n.º 5/2008 e resulta também do preâmbulo do Aviso do BdP n.º 3/2020.

do “subsistema” bancário. Resta saber se essa diferente dialética justifica uma compressão do direito à privacidade e do direito à inviolabilidade das comunicações privadas.

2.2. O conceito de mensagem de correio eletrônico

Importa, antes de mais, apresentar, ainda que de forma muito sucinta, uma definição de mensagem de correio eletrônico.

A Lei n.º 41/2004, de 18 de agosto¹³¹, é um bom ponto de partida, definindo o correio eletrônico como «qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha»¹³². Contudo, esta definição apresenta limitações, na medida em que «se restringe às mensagens enviadas através de comunicações públicas»¹³³. No nosso caso, interessa-nos também, pela natureza e objeto do nosso trabalho, as comunicações privadas.

Assim, para efeitos do nosso estudo, e por julgarmos acertada, aderimos ao conceito de (mensagem de) correio eletrônico sugerido por BENJAMIM SILVA RODRIGUES, para quem aquele consiste no «[f]luxo informacional e comunicacional digital, sob o formato de texto, voz, som, imagem ou gráfico, que é colocado por um assistente ou consumidor de redes ou serviços de comunicações eletrónicas acessíveis ao público, no âmbito de um ciclo internacional e comunicacional (tendencialmente) fechado, através de um ponto terminal de rede, na rede pública de comunicações eletrónicas, conduzida até ao servidor de *mail* ou ao terminal do destinatário do fluxo até que o mesmo proceda à sua recolha, leitura e/ou posterior eliminação»¹³⁴.

¹³¹ Relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.

¹³² Cfr. alínea b) do n.º 1 do artigo 2.º.

¹³³ RODRIGUES, Benjamim Silva (2008), p. 443.

¹³⁴ RODRIGUES, Benjamim Silva (2008), p. 444.

Por fim, importa delimitar, como daremos nota adiante, que, para efeitos do presente estudo, nos interessa o conteúdo da mensagem de correio eletrónico (texto e ficheiros anexos¹³⁵), mas já não os respetivos dados de tráfego¹³⁶. O investigador procederá, nas condições e nos limites adiante descritos, à recolha e à impressão do conteúdo de mensagens de correio eletrónico, sendo esse o documento¹³⁷ que será, depois, eventualmente objeto de transferência para o processo contraordenacional.

Antes de prosseguirmos, importa percorrer, ainda que de forma sintética, os diversos direitos envolvidos no acesso ao conteúdo de mensagens de correio eletrónico e respetiva recolha.

2.3. Excurso: a tutela dos direitos em causa constitucionalmente consagrados

2.3.1. A tutela do direito à privacidade

Começando pelo direito à privacidade, este tem, no plano internacional, consagração expressa no artigo 8.º da CEDH, e, bem assim, no artigo 7.º da Carta dos Direitos Fundamentais: «direito que cada um tem de dispor dos seus dados pessoais, não sendo permitido, sem autorização, o acesso aos mesmos por parte de terceiros, bem como a sua divulgação»¹³⁸. No caso *Copland* vs. Reino Unido, o TEDH considerou que as mensagens de correio eletrónico, enviadas no local de trabalho, têm uma proteção similar às chamadas telefónicas efetuadas por trabalhadores nesse mesmo local¹³⁹.

¹³⁵ CARDOSO, Rui (2018), p. 59.

¹³⁶ «Percurso percorrido pela mensagem desde a saída da caixa do remetente (*outbox*) até entrar na caixa do destinatário (*inbox*), com registo de cada ponto de passagem e sua data/hora/segundo/fuso horário» – CARDOSO, Rui (2018), p. 59.

¹³⁷ Na definição constante da segunda parte do artigo 362.º do CC.

¹³⁸ NEVES, Rita Castanheira (2011), p. 261.

¹³⁹ Caso *Copland* vs. Reino Unido, de 03.07.2007, disponível em <https://hudoc.echr.coe.int>, acessível em 19.04.2019.

No plano constitucional¹⁴⁰, o direito à privacidade vem consagrado no artigo 26.º, n.º 1, da CRP¹⁴¹. «O conteúdo da mensagem merece, como qualquer outra mensagem privada, uma protecção legal, e até constitucional, por recondução ao artigo 26.º da Constituição da República Portuguesa [...]»¹⁴².

No plano infraconstitucional, o direito à privacidade surge no artigo 80.º do CC, sob a epígrafe «[d]ireito à reserva sobre a intimidade da vida privada».

No âmbito do Direito Penal são punidas, através de diversos tipos de ilícito, as condutas que devessem a esfera da intimidade, designadamente através dos crimes previstos e punidos nos artigos 190.º, 192.º, 193.º, todos do CP, sendo de referir, em particular, o crime previsto e punido no artigo 194.º do mesmo diploma, que tem como epígrafe «[v]iolação de correspondência ou de telecomunicações».

No domínio do Direito do Trabalho, o artigo 22.º, n.º 1, do CT dispõe que «[o] trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de carácter não profissional que envie, receba ou consulte, nomeadamente através do correio eletrónico»¹⁴³.

¹⁴⁰ O TC formulou a seguinte definição do conteúdo da reserva da vida privada: «o direito de cada um a ver protegido o espaço interior ou familiar da pessoa ou do seu lar contra intromissões alheias, i.e., como um direito a uma esfera privada onde ninguém pode penetrar sem autorização do respetivo titular. No entender do Tribunal, esse direito compreende, por um lado, a autonomia, ou seja, o direito a ser o próprio a regular, livre de ingerências estatais e sociais, essa esfera de intimidade e, por outro, o direito a não ver difundido o que é próprio dessa esfera de intimidade, a não ser mediante autorização do interessado (“direito ao segredo do ser”).» (acórdão n.º 403/2015, em 27.08.2015, disponível em <http://www.tribunalconstitucional.pt>)

¹⁴¹ O artigo 26.º, n.º 1, da CRP, tem a seguinte redação: «[a] todos são reconhecidos os direitos à intimidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação».

¹⁴² NEVES, Rita Castanheira (2011), p. 261.

¹⁴³ O legislador ressalva, no entanto, no respetivo n.º 2, a possibilidade de «o empregador estabelecer regras de utilização dos meios de comunicação na empresa, nomeadamente do correio eletrónico».

Quando falamos na utilização do correio eletrónico no contexto laboral, está necessariamente implicado o direito à privacidade¹⁴⁴, em especial na vertente de autodeterminação informacional, isto é, o direito que cada um tem de dispor dos seus dados pessoais, não sendo permitido o acesso e a divulgação não autorizados ¹⁴⁵.

Entendemos que o legislador, no domínio do CT, ao incluir a referência a «mensagens» e «informação», pretendeu incluir, no âmbito de proteção legal do aludido preceito, a mensagem de correio eletrónico de natureza pessoal ou extraprofissional nos seus diversos estádios, isto é, enquanto comunicação, mas também, no fim do circuito comunicacional, enquanto mera informação armazenada no servidor ou localmente, no computador do trabalhador. Assim, independentemente de a mensagem de correio eletrónico, de natureza pessoal ou extraprofissional, ter sido efetivamente aberta ou lida pelo trabalhador, e, portanto, independentemente de a mensagem ser ou não, ainda, comunicação, este goza do direito de reserva e confidencialidade quanto ao respetivo conteúdo¹⁴⁶.

2.3.2. Direito à inviolabilidade das comunicações privadas

O artigo 34.º da CRP consagra a inviolabilidade das comunicações privadas¹⁴⁷, especificando o respetivo n.º 4 que «[é] proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria criminal». A referida proibição vale também, como não podia deixar de ser, para as autoridades privadas,

¹⁴⁴ ALVES, Lurdes Dias (2020), pp. 66 e seguintes.

¹⁴⁵ Em paralelo, na doutrina penal, *vide* NEVES, Rita Castanheira (2011), p. 261.

¹⁴⁶ Na doutrina penal tem sido analisada a questão dos diversos estádios do circuito comunicacional da mensagem de correio eletrónico. Quando o conteúdo da mensagem «jaz localmente num computador ou numa conta de *webmail* [...] a comunicação já não é em bom rigor comunicação. A comunicação cumpriu o seu circuito, deixando em seu lugar o conteúdo transmitido. Neste momento este conteúdo, localizado no computador ou no espaço virtual, é um registo que teve a sua origem numa comunicação, mas é já um ficheiro, ao lado de outros que o utilizador do computador cria, altera, elimina, etc.» (NEVES, Rita Castanheira (2011), p. 260)

¹⁴⁷ A redação integral do artigo 34.º, n.º 1, da CRP, é a seguinte: «[o] domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis».

«que se têm de abster de qualquer ingerência¹⁴⁸». Este direito «pretende assegurar que qualquer pessoa que estabeleça uma comunicação, seja através da correspondência tradicional, seja por via de telecomunicação ou pelos demais meios de comunicação, pode ter segurança que ninguém se intrometerá, nomeadamente em forma de interceptação, gravação e divulgação do teor da própria comunicação»¹⁴⁹. Isto é, no âmbito do artigo 34.º «cabe o chamado correio eletrónico, porque o segredo da correspondência abrange seguramente as correspondências mantidas por via das telecomunicações»¹⁵⁰.

Discutível é, no entanto, a questão de saber se no caso das mensagens de correio eletrónico é sempre possível (i. e., independentemente do seu concreto estágio no circuito comunicacional) falar-se em direito à inviolabilidade das comunicações privadas¹⁵¹. A dúvida coloca-se na medida em que, ao contrário da correspondência dita tradicional, em relação às mensagens de correio eletrónico é difícil determinar quando e se a mensagem foi aberta ou lida. «Poderá, assim, não existir segredo de telecomunicações porque estas [i. e., as comunicações] podem já ter terminado; não existir segredo de correspondência, porque este pode ter cessado com a abertura»¹⁵². Nesse sentido, «nunca estaremos nem completamente dentro, nem completamente fora quer do âmbito do segredo das telecomunicações, quer do âmbito do segredo da correspondência. Mas estaremos sempre perante perigo de ofensa de direitos fundamentais, como ao desenvolvimento da personalidade, à garantia da liberdade individual, à autodeterminação existencial e privacidade, e por isso com necessidade

¹⁴⁸ NEVES, Rita Castanheira (2011), p. 31.

¹⁴⁹ NEVES, Rita Castanheira (2011), p. 51.

¹⁵⁰ CARDOSO, Rui (2018), p. 56.

¹⁵¹ NEVES, Rita Castanheira (2011), p. 51. «*La diferencia entre intimidad y secreto de las comunicaciones radica en el momento en que se produce el acceso a la comunicación. Cuando el acceso al contenido de una comunicación se produce a la vez que ésta tiene lugar, afectando al canal por el que ésta se desarrolla, el derecho fundamental afectado es el secreto de las comunicaciones, el cual goza de garantía jurisdiccional. Sin mandato judicial no es posible su afectación. Por el contrario, el acceso al contenido de conversaciones o comunicaciones una vez ya realizadas forma parte del derecho a la intimidad.*» – MARTÍN, Adán Nieto (2015a), p. 250.

¹⁵² CARDOSO, Rui (2018), p. 57.

de tutela adequada»¹⁵³. Essa tutela (adequada), no contexto laboral, é conferida pelo já referido n.º 1 do artigo 22.º do CT, que reconhece ao trabalhador o direito de reserva e de confidencialidade relativamente ao conteúdo das mensagens de correio eletrónico de natureza pessoal ou extraprofissional, independentemente de estas reterem ou não – à luz do concreto estágio em que se encontram no circuito comunicacional – o *status* de comunicação.

2.4. Comandos normativos em matéria de mensagens de correio eletrónico, no contexto laboral

Antes de mais, cumpre distinguir mensagens de correio eletrónico de natureza pessoal ou extraprofissional das mensagens de correio eletrónico de natureza profissional¹⁵⁴.

Na jurisprudência, o STJ pronunciou-se no sentido de que as mensagens de correio eletrónico de natureza pessoal ou extraprofissional «não [são] apenas as comunicações relativas à vida familiar, afectiva, sexual, saúde, convicções políticas e religiosas do trabalhador, e mencionadas no art. 16º, n.º 2 do CT, que revestem a natureza de comunicações de natureza pessoal, nos termos e para os efeitos do art.º 21º. Como aí se referiu, a definição de natureza particular da mensagem obtém-se por contraposição à natureza profissional da comunicação, relevando, para tal, antes de

¹⁵³ CARDOSO, Rui (2018), p. 58.

¹⁵⁴ «Quanto ao correio electrónico parece oportuno que a obrigação de distinguir correctamente correio pessoal e profissional conste do regulamento interno da empresa, obrigando-se o trabalhador a não qualificar informações profissionais como pessoais e vice-versa. A empresa deve poder presumir que não é pessoal todo o correio que o trabalhador não tenha expressamente qualificado como tal. Devem prever-se mecanismos para situações de ausência dos trabalhadores – férias e sobretudo suspensões do contrato por doença e licenças – em que pode ser necessário, sob pena de informações importantes não poderem ser recebidas em tempo útil, aceder ao correio electrónico: convém que os trabalhadores interessados sejam previamente alertados para essa possibilidade e, preferencialmente, tenham dado o seu consentimento prévio. Afora os casos de ausência do interessado, deve prever-se que a abertura excepcional do correio electrónico de um trabalhador, quando motivada por fortes indícios de violação das regras de utilização dos meios informáticos, e mesmo que referida a correio não classificado como pessoal, seja feita na presença do próprio interessado e de um representante dos trabalhadores.» – GOMES, Júlio Manuel Vieira (2007), p. 383.

mais, a vontade dos intervenientes da comunicação ao postularem, de forma expressa ou implícita, a natureza profissional ou privada das mensagens que trocam [...].

E não é pela circunstância [de os] intervenientes se referirem a aspectos da empresa que, por essa simples razão, a comunicação assume desde logo um carácter profissional, legitimando a sua intercepção pelo empregador»¹⁵⁵.

Também o TRP, embora com menor densificação, contrapõe mensagem de natureza pessoal a mensagem de natureza profissional, expondo que a mensagem de natureza profissional é aquela que é levada «a cabo pelo trabalhador no âmbito do exercício das suas funções ao serviço do empregador»¹⁵⁶.

No limite, parece-nos que a classificação da natureza da mensagem de correio eletrónico sempre competirá ao trabalhador. Se o trabalhador informar o empregador de que a mensagem tem natureza pessoal, na ausência de consentimento do trabalhador, o empregador não deve aceder à mesma¹⁵⁷, mesmo que tal afirmação, negligente ou dolosamente, não corresponda à verdade (doutro modo, estar-se-ia a permitir, através de um ato de confirmação do empregador aquilo que se lhe pretende vedar – *i.e.*, o acesso a mensagens de natureza pessoal ou extraprofissional)¹⁵⁸.

¹⁵⁵ Cfr. Acórdão proferido no processo n.º 07S043, em 05.07.2007, disponível em <http://www.dgsi.pt>.

¹⁵⁶ Cfr. Acórdão proferido no processo n.º 208/14.1TTVFR-D.P1, em 15.12.2016, disponível em www.dgsi.pt. Na doutrina, trazendo à colação o referido acórdão do STJ, LURDES DIAS ALVES refere que as comunicações de natureza privada ou extraprofissional são, «[...] para além das comunicações relativas à vida familiar, afetiva, sexual, saúde, convicções políticas e religiosas do trabalhador, previstas no n.º 2 do artigo 16.º do referido Código do Trabalho, as mensagens relativamente às quais da vontade do seu emissor não resulta de forma clara a natureza profissional das mesmas. [...]» (ALVES, Lurdes Dias (2020), p. 77)

¹⁵⁷ «A visualização de tais mensagens, que apenas se justifica em casos esporádicos, deve ser feita na presença do trabalhador ou de quem o represente e deve limitar-se à visualização do endereço do destinatário ou remetente da mensagem, do assunto, data e hora do envio. O controlo do correio eletrónico deve realizar-se de forma aleatória e não persecutória e ter como finalidade a promoção da segurança do sistema e a sua performance.» – MARTINEZ, Pedro Romano [et al.] (2017), p. 167.

¹⁵⁸ Há, no entanto, vozes na doutrina que vão um pouco mais longe: «parece-nos que o empregador poderá abrir mensagens que pode legitimamente acreditar que não são pessoais. Tal será o caso, designadamente, se não tiver autorizado o uso do correio eletrónico para fins pessoais (se do contexto da mensagem não resultar, apesar disso, que ela é efectivamente pessoal – seja porque foi mesmo qualificada como tal pelo trabalhador, seja porque tal resulta do assunto ou, porventura, do remetente ou do destinatário que é, por exemplo, a mulher do trabalhador) ou se tiver criado dois endereços, um para utilização profissional e outro para uso pessoal, relativamente àquele. Parece-nos já impor-

O acesso às mensagens de correio eletrónico pelo empregador, no contexto de uma relação de trabalho, constituiu um tema debatido na doutrina e na jurisprudência. Contudo, arriscar-nos-íamos a afirmar que é hoje pacífico que «o conteúdo dos *emails* enviados ou rececionados pelo trabalhador, quer de conta de correio pessoal, quer de conta de correio profissional que tenham natureza pessoal/extraprofissional, estão abrangidos pela tutela dos direitos à privacidade e à confidencialidade das mensagens»¹⁵⁹, não podendo o empregador, em circunstância alguma, ter acesso às mensagens de correio eletrónico de natureza pessoal ou extraprofissional¹⁶⁰, salvo quando o trabalhador o consinta.

Acresce que é irrelevante que a conta de correio eletrónico tenha sido disponibilizada pelo empregador¹⁶¹ e/ou que os inerentes dados fiquem armazenados no respetivo servidor. O que releva é o conteúdo – o teor do texto ou dos ficheiros anexos – da mensagem enviada ou recebida, isto é, se a mensagem tem natureza pessoal ou, ao invés, profissional. Tendo natureza pessoal ou extraprofissional, o conteúdo não deve ser acedido.

Dado que o empregador pode, ao abrigo do n.º 2 do artigo 22.º do CT, estabelecer regras de utilização dos meios de comunicação da empresa, «nomeadamente do correio eletrónico»¹⁶², devem distinguir-se «as situações em que existe uma definição clara e precisa, determinada pelo empregador, e comunicada ao trabalhador, acerca

se maior cautela quando o empregador autorize o uso “promíscuo” do correio eletrónico.» – GOMES, Júlio Manuel Vieira (2007), p. 384.

¹⁵⁹ Cfr. Acórdão do TRL, proferido no processo n.º 208/14.1TTVFR-D.P1, em 15.12.2016, disponível em <http://www.dgsi.pt>.

¹⁶⁰ Nesse sentido, também, e fazendo referência à posição da CNPD nesta matéria, ALMEIDA, Joana (2020), p. 77.

¹⁶¹ «Não é o facto de certas mensagens ficarem gravadas em servidores da propriedade do empregador que lhe dá o direito de aceder àquelas mensagens, as quais não perdem a sua natureza pessoal ou confidencial, mesmo quando esteja em causa investigar e provar uma eventual infração disciplinar.» (Cfr. p. 18 da Deliberação n.º 1638/2013, da CNPD, aplicável aos tratamentos de dados pessoais decorrentes do controlo da utilização para fins privados das tecnologias de informação e comunicação no contexto laboral, disponível em <https://www.cnpd.pt>, em 13.02.2020)

¹⁶² Cfr. artigo 22.º, n.º 2, do CT.

da utilização dos meios informáticos, designadamente da utilização da conta de *email* fornecida por este e de acordo com a qual tal conta apenas deverá ser utilizada para fins profissionais, daquelas outras situações em que é permitida a utilização da conta de correio eletrónico para fins profissionais e para efeitos pessoais ou em que não exista tal definição»¹⁶³.

Na situação em que existe uma definição clara das regras de utilização do correio eletrónico disponibilizado pelo empregador, mormente quanto à sua utilização exclusiva para efeitos profissionais, tem-se entendido que o empregador tem uma maior expectativa no sentido de as mensagens enviadas e recebidas pelo trabalhador, terem natureza profissional¹⁶⁴. No entanto, sempre que o empregador se aperceba de que a mensagem, que presumiu ter natureza profissional, tem, ao invés, natureza pessoal, deve parar, de imediato, a leitura¹⁶⁵.

Pelo contrário, nas situações em que o empregador não estabelece regras relativas à utilização do correio eletrónico pelos trabalhadores, nem sempre será fácil distinguir mensagens de natureza pessoal de mensagens de natureza profissional, pelos respetivos dados exteriores, designadamente o assunto da mensagem, até porque o assunto é de inserção opcional e, mesmo quando conste da mensagem, pouco pode revelar sobre o conteúdo da mesma.

¹⁶³ Cfr. Acórdão do TRP, proferido no processo n.º 208/14.1TTVFR-D.P1, em 15.12.2016, disponível em <http://www.dgsi.pt>.

¹⁶⁴ Pelo interesse e relativo paralelismo com o objeto do nosso estudo, consideramos ser oportuno referir a decisão proferida pelo TEDH, no caso *Bărbulescu c. Roménia*. Em causa estava o uso por um trabalhador do *Yahoo Messenger* no computador da empresa durante o horário de trabalho – sendo tal uso vedado, conforme acordado entre o trabalhador e o empregador –, facto que motivou o seu despedimento. A decisão que havia sido inicialmente apreciada em desfavor do queixoso, foi reapreciada pelo *Grand Chamber*, que considerou que as instâncias nacionais não determinaram se o queixoso foi previamente informado pelo empregador de que existia a possibilidade de este monitorizar as comunicações no *Yahoo Messenger*, nem aquele foi informado do conteúdo e extensão dessa monitorização. E, assim, o Tribunal concluiu pela violação do artigo 8.º da CEDH - <https://hudoc.echr.coe.int>, acessível em 15.01.2020. Para uma análise mais detalhada deste acórdão, vide PEREIRA, Francisco Rodrigues (2018), em especial pp. 31 e seguintes.

¹⁶⁵ Nesse sentido, o Acórdão do TRP, proferido no processo n.º 208/14.1TTVFR-D.P1, em 15.12.2016, disponível em <http://www.dgsi.pt>.

Ora, «o facto de o empregador colocar à disposição do trabalhador uma conta de correio eletrónico profissional não permite automaticamente que se possa considerar, “presumir” ou partir do pressuposto de que as mensagens enviadas ou recebidas pelo trabalhador têm natureza profissional. Nesta situação, face à inexistência de regras, designadamente de proibição da sua utilização para efeitos pessoais, é de admitir, e deve o empregador admiti-lo como possível, que essa utilização possa ter lugar para efeitos também pessoais, não havendo razão que fundamente uma maior expectativa por parte do empregador de que a utilização do *email* o será apenas para fins profissionais.». Este aresto do TRP termina referindo que «nas situações em que é disponibilizado ao trabalhador conta de correio eletrónico profissional, mas sem definição das regras quanto à sua utilização, mormente sem que seja proibida a sua utilização para efeitos pessoais, não pode o empregador aceder ao conteúdo dos *emails* enviados ou rececionados nessa conta, mesmo que não estejam marcados como pessoais ou dos seus dados não resulte que sejam pessoais»¹⁶⁶.

Em qualquer caso, o acesso ao conteúdo da mensagem deve ser sempre feito na «presença do trabalhador visado e, de preferência, na presença de um representante da comissão de trabalhadores ou de uma estrutura representativa [...] ou de alguém indicado pelo trabalhador».¹⁶⁷

Em suma, salvo consentimento do trabalhador, ao empregador é vedado o acesso a mensagens de natureza pessoal ou extraprofissional.

Transpondo as considerações acima expostas para a realidade das IC, pode dizer-se que, por princípio, os colaboradores inseridos nas mesmas, sendo parte integrante de uma cultura organizacional na qual eles próprios devem conhecer o respetivo papel

¹⁶⁶ Cfr. Acórdão do TRP, proferido no processo n.º 208/14.1TTVFR-D.P1, 15.12.2016, disponível em <http://www.dgsi.pt>.

¹⁶⁷ Cfr. p. 20 da Deliberação n.º 1638/2013, da CNPD, aplicável aos tratamentos de dados pessoais decorrentes do controlo da utilização para fins privados das tecnologias de informação e comunicação no contexto laboral, disponível em <https://www.cnpd.pt>, acessível em 13.02.2019.

no sistema de controlo interno, para nele desempenharem um papel ativo e efetivo¹⁶⁸, se encontram mais capacitados e mais bem preparados, por comparação com os colaboradores da generalidade das empresas, para colaborar com uma investigação interna, nela podendo até participar ativamente. Uma vez que o sistema de controlo interno deve estar profundamente enraizado na cultura da instituição, a investigação, enquanto elemento fundamental desse sistema, não constitui, para a generalidade dos seus colaboradores um “corpo estranho”. Ao invés, gera, ou deve gerar, um sentido de missão e de entrega incomparáveis com a generalidade das empresas.

Nesse sentido, poder-se-ia, pois, colocar a questão de saber se a lei, ao impor um sistema de controlo interno sólido, que tem por missão preservar a estabilidade e a confiança no sistema financeiro, impõe ou sequer admite restrições ao direito à privacidade e à inviolabilidade das comunicações privadas, como meio para alcançar tal objetivo. Entendemos que a resposta é necessariamente negativa, face ao artigo 18.º, n.º 2, da CRP, que dispõe que «[a] lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição [...]». Ademais, não encontramos na CRP qualquer preceito donde se possa retirar uma permissão para que o legislador ordinário, com o intuito de preservar o sistema financeiro e a confiança que os cidadãos nele depositam, pudesse operar, por via legal, uma restrição aos direitos reconhecidos aos trabalhadores.

Atento o exposto, concluímos que os trabalhadores da IC gozam dos exatos mesmos direitos que assistem aos trabalhadores na generalidade das empresas. Ademais, concluímos que o objetivo fundamental e inerente ao sistema de controlo interno não comporta, nem admite, qualquer restrição, em matéria de direitos fundamentais^{169/170}.

¹⁶⁸ Conforme dispunha o artigo 9.º, n.º 2, alínea d), do Aviso do BdP n.º 5/2008 e agora com maior grau de densificação os artigos 2.º e 3.º do Aviso do BdP n.º 3/2020.

¹⁶⁹ Para uma análise comparada a propósito da monitorização pelo empregador da utilização pelo trabalhador do correio eletrónico, *vide* GOMES, Júlio Manuel Vieira (2007), pp. 369 a 382.

¹⁷⁰ Cumpre referir que o artigo 10.º do CT estendeu «[a]s normas legais respeitantes a direitos de personalidade, igualdade e não discriminação e segurança e saúde no trabalho [...] a situações em

Deste modo, sempre que o conteúdo de uma mensagem de correio eletrónico tenha natureza pessoal, seja de presumir tal natureza ou trabalhador assim a classifique, o investigador está impedido de a recolher ou aceder e, por maioria de razão, de a utilizar na sua investigação.

Mais problemática se afigura a análise da questão na perspetiva do Direito da Proteção de Dados. Vejamos.

2.5. Comandos normativos em matéria de mensagens de correio eletrónico, no contexto da Proteção de Dados

2.5.1. Introdução

A mensagem de correio eletrónico poderá conter os seguintes elementos (i) o endereço de correio eletrónico do remetente, (ii) o endereço de correio eletrónico do destinatário, (iii) a data e a hora do envio da mensagem, (iv) o assunto e (v) a mensagem de texto remetida. Acresce que a conta de correio eletrónico está, na maior parte das vezes, associada ao nome próprio e ao apelido da pessoa associada à conta. Por vezes, até, a fotografia de um ou de ambos os intervenientes na mensagem.

Atenta definição de dados pessoais, nos termos e para os efeitos do RGPD – a saber: a informação relativa a uma pessoa singular identificada ou identificável¹⁷¹ –, é provável que a mensagem contenha, num dos elementos acima descritos (pelo menos,

que ocorra prestação de trabalho por uma pessoa a outra, sem subordinação jurídica, sempre que o prestador deva considerar-se na dependência económica do beneficiário da atividade». Cremos que, nestas condições, também estes prestadores de serviços beneficiam da proteção acima descrita.

¹⁷¹ Cfr. artigo 4.º, n.º 1, do RGPD: «informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular».

e habitualmente, no campo remetente e destinatário), dados pessoais. A pessoa singular em causa não tem de estar identificada, bastando que seja identificável¹⁷². Esta pessoa é o titular dos dados.

Na medida em que as mensagens contenham dados pessoais, a sua recolha, o seu acesso e, bem assim, a sua utilização no contexto de uma investigação, constituem possíveis formas de tratamento daqueles dados¹⁷³.

Ao falarmos de tratamento de dados, temos também necessariamente de falar do responsável pelo tratamento, isto é: «a pessoa singular ou coletiva [...] que individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais»¹⁷⁴. Pode acrescentar-se que «[o] responsável pelo tratamento poderá assumir qualquer forma jurídica – pessoa singular, pessoa coletiva de direito público ou de direito privado [...]» e cumpre a função de «alocar (e de concentrar) a responsabilidade pelo tratamento a um centro de imputação [...]»¹⁷⁵.

No contexto do presente trabalho, que é o das investigações internas, podemos adiantar que, na generalidade das situações, o responsável pelo tratamento será a IC em questão. Mas nem sempre será assim: basta pensar na hipótese de a investigação ser conduzida por um advogado. Aqui acompanhamos TATIANA DUARTE, quando afirma que «[n]o caso do advogado que tenha um vínculo laboral com um empregador, a responsabilidade pelo tratamento começa no momento em que termina o poder de direção; ou seja, nas situações em que o advogado esteja – e possa

¹⁷² Tome-se, como exemplo, o seguinte endereço: responsavelpelafuncaodecumprimento@bgpp.pt. Apesar de não conter a identificação do remetente, é possível, através do endereço de correio eletrónico, identificar a concreta pessoa que remete a mensagem. Nessa medida, aquela informação é um dado pessoal.

¹⁷³ O termo tratamento de dados tem latitude considerável, abrangendo a «recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, comparação ou interconexão, a limitação, o apagamento ou a destruição.» – artigo 4.º, n.º 2, do RGD.

¹⁷⁴ Cfr. artigo 4.º, n.º 7, do RGD.

¹⁷⁵ PINHEIRO, Alexandre Sousa [et al.] (2018), p. 139.

deontologicamente estar – sob o poder de direção do empregador, este é o responsável pelo tratamento. Quando atue de forma independente – tipicamente nos casos de representação judicial –, será responsável pelo tratamento»¹⁷⁶.

Pode adiantar-se, como princípios relativos ao tratamento de dados pessoais, que os dados devem ser (i) objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados¹⁷⁷, (ii) recolhidos para finalidades determinadas, explícitas e legítimas¹⁷⁸, (iii) adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados¹⁷⁹ e (iv) exatos e atualizados sempre que necessário¹⁸⁰. Cabe, assim, indagar, no contexto de uma investigação, em que condições é lícito tratar dados pessoais insertos em mensagens de correio eletrónico.

Parece-nos que a licitude e a finalidade do tratamento são os pontos que maiores dúvidas podem suscitar no contexto de uma investigação interna, motivo pelo qual centraremos o objeto da nossa análise nestes dois princípios.

¹⁷⁶ PINHEIRO, Alexandre Sousa [et al.] (2018), p. 147.

¹⁷⁷ Cfr. artigo 5.º, n.º 1, alínea *a*), do RGPD.

¹⁷⁸ Cfr. artigo 5.º, n.º 1, alínea *b*), do RGPD.

¹⁷⁹ Cfr. artigo 5.º, alínea *c*), do RGPD. No que respeita ao princípio da proporcionalidade (princípio da “minimização de dados”), em sentido estrito, os dados recolhidos devem ser «adequados a prosseguir a finalidade da sua recolha, e os estritamente necessários para o mesmo efeito, devendo, por isso, o tratamento de dados reduzir-se ao mínimo indispensável ao cumprimento da respetiva finalidade. Além disso, impõe-se ainda um último juízo de ponderação entre os benefícios obtidos com o tratamento e os prejuízos decorrentes para os direitos dos trabalhadores, de modo a garantir que o tratamento não seja excessivo», tal como referido na p. 8 da Deliberação da CNPD n.º 1638/2013, disponível em <https://www.cnpd.pt>, acessível em 18.02.2019. Já no que respeita ao princípio da proporcionalidade em sentido amplo, mormente na vertente do princípio da necessidade, o investigador só deve aceder às mensagens de correio eletrónico enviadas e/ou recebidas por trabalhadores na hipótese de não existirem formas menos intrusivas para a privacidade daqueles trabalhadores, e igualmente aptas a atingir o fim pretendido. A este propósito, a CNPD alerta para o facto de a entidade empregadora dever privilegiar «metodologias genéricas de controlo, afastando, sempre que possível, a consulta individualizada de dados pessoais», conforme p. 9 da referida Deliberação. Embora esta análise deva ocorrer casuisticamente, não nos parece que a recolha de mensagens de correio eletrónico nas condições acima descritas se afigure contrária ao princípio da proporcionalidade.

¹⁸⁰ Cfr. artigo 5.º, n.º 1, alínea *d*), do RGPD.

2.5.2. A licitude do tratamento

Conforme se referiu, dispõe o RGPD que os dados pessoais devem ser objeto de um tratamento lícito: a licitude do tratamento depende, na generalidade das situações, da verificação de, pelo menos, uma das situações previstas nas alíneas a) a f) do respetivo n.º 1 do artigo 6.^o¹⁸¹.

Face ao artigo 6.^o, n.º 1, do RGPD, parece-nos que, no contexto das investigações internas, o fundamento da licitude para o tratamento de dados encontra, em abstrato, acolhimento na alínea a) ou na alínea c)¹⁸² daquele preceito, os quais analisaremos em seguida.

i. O consentimento: os pressupostos atinentes a um consentimento válido e eficaz

Neste ponto, faremos uma muito breve referência aos pressupostos atinentes a um consentimento válido e eficaz, apenas densificando os pontos que apresentem alguma especificidade à luz do objeto do nosso estudo¹⁸³.

Nos termos do n.º 11 do artigo 4.^o do RGPD, o consentimento do titular dos dados corresponde a «uma [i] manifestação de vontade, [ii] livre, [iii] específica, [iv] informada e [v] explícita, [vi] pela qual o titular dos dados aceita, mediante

¹⁸¹ «Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento do titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento, quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento [...]» – considerando n.º 40 do RGPD. PINHEIRO, Alexandre Sousa [et al.] (2018), p. 215.

¹⁸² Não excluimos, a título subsidiário, a possibilidade de o responsável pelo tratamento fundar a licitude do tratamento na alínea f) do n.º 1 do artigo 6.^o do RGPD (interesses legítimos prosseguidos pelo responsável).

¹⁸³ Para uma exposição e análise mais detalhadas do consentimento, *vide* Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 do CEPD, disponível em <https://edpb.europa.eu/>, acessível 20.12.2020.

declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento».

O consentimento como **manifestação de vontade** «significa que não existe a figura do consentimento obrigatório. Ou seja, não pode tratar-se nos quadros do consentimento, por exemplo, exigências ou obrigações legais»¹⁸⁴.

Quanto à **liberdade** do consentimento, esta só existe se o mesmo «implic[ar] uma verdadeira escolha e controlo para o titular dos dados». O que significa que se o consentimento «estiver agregado a uma parte não negociável das condições gerais do contrato, presume-se que não foi dado livremente»¹⁸⁵. Deste modo, se o empregador incluir no contrato de trabalho ou em anexo ao mesmo uma cláusula relativa ao tratamento de dados pessoais e fizer depender a celebração do contrato de trabalho da aceitação dessa cláusula, naturalmente que o consentimento não é livre.¹⁸⁶

Mais: em nossa opinião, é fundamental que o consentimento não seja prestado durante o período experimental¹⁸⁷, porquanto (i) neste período, na generalidade das situações, a posição do trabalhador é particularmente frágil, na medida em que a relação de trabalho pode cessar por iniciativa do empregador, por denúncia, sem necessidade de qualquer aviso prévio¹⁸⁸, (ii) sendo de presumir que, nesse período, o trabalhador não está ainda totalmente inserido na cultura organizacional da IC em

¹⁸⁴ PINHEIRO, Alexandre Sousa [et al.] (2018), p. 167.

¹⁸⁵ Cfr. p. 8 das Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 do CEPD, disponível em <https://edpb.europa.eu/>, acessível 20.12.2020.

¹⁸⁶ Para um tratamento mais desenvolvido da liberdade do consentimento, *vide* pp. 8 e seguintes das Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 do CEPD, disponível em <https://edpb.europa.eu/>, acessível 20.12.2020. A este propósito, dispõe o artigo 7.º, n.º 2, do RGPD, que «[s]e o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento».

¹⁸⁷ Cfr. artigo 111.º do CT.

¹⁸⁸ Ressalvadas as situações previstas nos n.ºs 2 e 3 do artigo 114.º do CT, durante o período experimental, o contrato é livremente denunciável pelas partes sem aviso prévio ou invocação de justa causa.

questão, circunstância que é suscetível de condicionar a prestação de um consentimento **livre**.

O tratamento de dados pessoais no contexto laboral suscita as seguintes questões: o consentimento do titular dos dados (o trabalhador) é um fundamento válido? E na ausência de consentimento, o responsável pelo tratamento pode socorrer-se de outro fundamento?

No que respeita ao consentimento, enquanto fundamento da licitude do tratamento, o CEPD, a respeito do tratamento de dados pessoais no contexto laboral, referiu o seguinte: «o CEPD considera problemática a questão de os empregadores procederem ao tratamento de dados pessoais dos seus trabalhadores atuais ou futuros com base no consentimento, uma vez que é improvável que esse consentimento seja dado de livre vontade. Relativamente à maior parte deste tratamento de dados no local de trabalho, o fundamento jurídico não pode nem deve ser o consentimento dos trabalhadores [artigo 6.º, n.º 1, alínea a)], devido à natureza da relação entre empregador e trabalhador». Esclareceu, no entanto, que isto «[...] não significa que os empregadores nunca possam utilizar o consentimento como fundamento jurídico para o tratamento. Pode haver situações em que seja possível ao empregador demonstrar que o consentimento foi dado livremente. Atendendo ao desequilíbrio de poder entre empregadores e empregados, estes só podem dar o seu consentimento livremente em circunstâncias excecionais, quando o ato de dar ou recusar o consentimento não produza quaisquer consequências negativas»¹⁸⁹.

No que se refere ao legislador nacional, este considerou, no artigo 28.º, n.º 3, da Lei n.º 58/2019, de 8 de agosto¹⁹⁰, que, «[s]alvo norma legal em contrário, o

¹⁸⁹ Cfr. p. 10 das Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 do CEPD, disponível em <https://edpb.europa.eu/>, acessível 20.12.2020. Na doutrina, LURDES DIAS ALVES entende que o fundamento legal para o tratamento de dados no local de trabalho, não pode nem deve ser o consentimento dos trabalhadores, face à relação de desequilíbrio entre empregador e trabalhador. (ALVES, Lurdes Dias (2018), p. 60)

¹⁹⁰ Nova Lei da Proteção de Dados.

consentimento do trabalhador não constitui requisito da legitimidade do tratamento dos seus dados pessoais: a) Se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador¹⁹¹; ou b) Se esse tratamento estiver abrangido pelo disposto na alínea b) do n.º 1 do artigo 6.º do RGPD¹⁹²».

A solução preconizada na lei tem como consequência que quando o tratamento, no contexto laboral, não seja enquadrável numa das situações referidas no artigo 28.º, n.º 3, alíneas a) e b), o consentimento do trabalhador pode constituir fundamento da licitude do tratamento de dados.

Sucedem que esta dialética – assente nas questões enunciadas – gera um problema: se para o CEPD, no contexto laboral, o consentimento não constitui, em regra, uma forma válida de conferir licitude ao tratamento de dados pessoais no contexto laboral (conforme acima referimos), ao invés, para o legislador nacional, o consentimento pode constituir, ressalvadas as exceções previstas nas alíneas a) e b) do n.º 3 do artigo 28.º da Lei n.º 58/2019, de 8 de agosto, requisito de legitimidade do tratamento.

Ora, não obstante as diretrizes do CEPD não sejam vinculativas, constituindo apenas orientações gerais para clarificar as normas legais europeias em matéria de proteção de dados, o certo é que compete assegurar a aplicação coerente do RGPD¹⁹³.

¹⁹¹ Na Deliberação da CNPD n.º 494/2019, esta refere que «o disposto na alínea a) do n.º 3 do artigo 28.º, ao determinar precisamente a solução oposta, restringe excessivamente a relevância do consentimento do trabalhador, com isso eliminando qualquer margem de livre arbítrio dos trabalhadores mesmo quando há condições para a sua manifestação sem risco para os seus direitos e interesses. Nessa medida, esta disposição traduz uma restrição injustificada e desproporcionada do disposto na alínea a) do n.º 2 do artigo 9.º do RGPD. Entende, assim, a CNPD que esta disposição não corresponde a uma medida legislativa nacional adequada que salvguarde a dignidade, os direitos fundamentais e os interesses legítimos do trabalhador, não cumprindo, portanto, os requisitos exigidos na alínea b) do n.º 2 do artigo 9.º e do n.º 2 do artigo 88.º do RGPD». E termina dizendo que, com esse fundamento, «desaplicará a referida norma nas situações que venha a apreciar». Cfr. pp. 5 e 6 da referida Deliberação, disponível em <https://www.cnpd.pt>, acessível em 28.09.2019.

¹⁹² Artigo 6.º, n.º 1, alínea b), do RGPD: «O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados».

¹⁹³ Cfr. artigo 70.º do RGPD.

No que respeita à **especificidade** do consentimento, o tratamento deve ter por objeto finalidades específicas e deve ser prestado de forma granular¹⁹⁴. No caso do nosso estudo, o titular dos dados deve ser **prévia**¹⁹⁵ e devidamente **informado**¹⁹⁶ de que o responsável pelo tratamento pretende tratar os dados – cujas modalidades devem estar especificamente descritas (designadamente, a recolha, a sua consulta e a sua eventual transmissão desses dados ao BdP) – no âmbito de uma investigação interna. O titular dos dados deve conhecer, antecipada e especificadamente, o percurso do tratamento dos seus dados (*i. e.*, onde começa e onde acaba o tratamento)¹⁹⁷.

Finalmente, o consentimento deve ser **explícito**, no sentido de que «o titular dos dados deve manifestar expressamente o seu consentimento¹⁹⁸».

Face às fragilidades expostas, evidenciadas pelos desequilíbrios de poder em contexto laboral, consideramos prudente que o tratamento de dados no contexto das investigações internas não assente no consentimento do seu titular, como fundamento da licitude, devendo antes assentar no fundamento que veremos de seguida¹⁹⁹.

¹⁹⁴ Cfr. pp. 15 e seguintes das Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 do CEPD, disponível em <https://edpb.europa.eu/>, acessível 20.12.2020.

¹⁹⁵ «Embora o RGPD não estipule literalmente no artigo 4.º, n.º 11, que o consentimento deve ser dado antes da atividade de tratamento, trata-se de um aspeto claramente implícito. A parte introdutória do artigo 6.º, n.º 1, e a redação «tiver dado» que consta do artigo 6.º, n.º 1, alínea a), corrobora esta interpretação [...]» (p. 23 das Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 do CEPD, disponível em <https://edpb.europa.eu/>, acessível 20.12.2020).

¹⁹⁶ «É fundamental fornecer informações aos titulares dos dados antes da obtenção do consentimento para que estes possam tomar decisões informadas, compreendendo com o que estão a concordar e, por exemplo, exercer o direito de retirar o consentimento dado. Se o responsável pelo tratamento não fornecer informações acessíveis, o controlo do utilizador torna-se ilusório e o consentimento será um fundamento inválido para o tratamento» (p. 17 das Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 do CEPD, disponível em <https://edpb.europa.eu/>, acessível 20.12.2020).

¹⁹⁷ Recorda-se aqui, a este propósito, o caso *Bărbulescu v. Romania*, em que não ficou demonstrado que o empregador tivesse previamente informado o trabalhador da possibilidade de monitorizar as comunicações do trabalhador ou que o tivesse informado do conteúdo e extensão dessa monitorização. Esta circunstância levou a que o Tribunal considerasse existir violação do artigo 8.º da Convenção – <https://hudoc.echr.coe.int>, acessível em 15.01.2020.

¹⁹⁸ Cfr. p. 23 das Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 do CEPD, disponível em <https://edpb.europa.eu/>, acessível 20.12.2020.

¹⁹⁹ A este propósito, pela sua relevância, destacam-se os seguintes parágrafos das diretrizes do CEPD: «121. O artigo 6.º estabelece as condições do tratamento lícito dos dados pessoais e descreve seis

ii. O cumprimento de uma obrigação jurídica pelo responsável pelo tratamento

Conforme se referiu, no contexto das investigações internas, outro dos fundamentos possíveis para a licitude do tratamento de dados reside na alínea c) do n.º 1 do artigo 6.º do RGPD²⁰⁰, a saber: «[o] tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito»²⁰¹.

Conforme se referiu no Capítulo I do presente trabalho²⁰², as investigações internas derivam e são consequência necessária da implementação de um sistema de controlo interno, pleno e efetivo. As investigações, estando integradas no sistema de controlo interno, atuam como mecanismo reativo, de forma a mitigar riscos de *compliance*. Nesse sentido, ao tratar dados pessoais no contexto de uma investigação, o

fundamentos jurídicos que o responsável pelo tratamento pode invocar. A aplicação de um desses seis fundamentos deve ser estabelecida antes da atividade de tratamento e em relação a uma finalidade específica. 122. É importante referir aqui que o responsável pelo tratamento, se optar por invocar o consentimento para qualquer parte do tratamento, deve estar preparado para respeitar essa opção e parar essa parte do tratamento se um indivíduo retirar o consentimento. Passar a mensagem de que os dados serão tratados com base no consentimento enquanto, na verdade, esse tratamento assenta noutro fundamento jurídico, seria essencialmente desleal para com as pessoas. 123. Por outras palavras, o responsável pelo tratamento não pode passar do consentimento para outros fundamentos jurídicos. Por exemplo, não lhe é permitido utilizar retroativamente o fundamento do interesse legítimo para justificar o tratamento, se forem detetados problemas com a validade do consentimento. Uma vez que os responsáveis pelo tratamento têm a obrigação de comunicar o fundamento jurídico em que se baseiam aquando da recolha dos dados pessoais, estes responsáveis devem definir qual o fundamento jurídico aplicável antes da referida recolha.» – p. 29 das Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 do CEPD, disponível em <https://edpb.europa.eu/>, acessível 20.12.2020.

²⁰⁰ Este aspeto é absolutamente relevante, dada a referida controvérsia em torno do consentimento.

²⁰¹ De acordo com a orientação genérica do então Grupo de Trabalho do artigo 29.º, «[t]al pode ser o caso, por exemplo quando os empregadores tenham de fornecer à segurança social ou às autoridades fiscais dados relativos aos salários dos seus trabalhadores, ou quando as instituições financeiras sejam obrigadas a denunciar determinadas transações suspeitas às autoridades competentes nos termos das normas em matéria de luta contra o branqueamento de capitais» – Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento de dados na aceção do artigo 7.º da Diretiva n.º 95/46/CE, do PE e do Conselho, p. 29, disponível em <https://www.gdpd.gov.mo>, acessível em 25.04.2019.

²⁰² Para o qual, por razões de economia se remete, e aqui se dá por integralmente reproduzido.

responsável pelo tratamento tem como objetivo reagir a riscos de *compliance*, quer estes riscos se traduzam em riscos já materializados ou não.

Ora, a obrigação jurídica resulta, a nosso ver, das normas jurídicas aplicáveis ao setor bancário (designadamente, RGICSF e Aviso do BdP n.º 3/2020²⁰³), que impõem à IC, como pressuposto fundamental da preservação da estabilidade do sistema financeiro (em especial, como se referiu, do subsistema bancário) e, bem assim, da manutenção da confiança que os particulares nele depositam, o dever de reagirem a riscos de *compliance*, como vimos através da realização de investigações internas. Ora, a recolha de elementos (incluindo mensagens de correio eletrónico) constitui uma fase essencial de qualquer investigação.

2.5.3. A finalidade do tratamento

Os dados pessoais devem ser recolhidos para «finalidades determinadas, explícitas e legítimas, não podendo os dados ser tratados posteriormente de uma forma incompatível com essas finalidades» (alínea *b*) do n.º 1 do artigo 5.º do RGPD). Os três apontados requisitos já constavam da Diretiva n.º 95/46/CE, de 24 de outubro, e foram estudados pelo então denominado Grupo de Trabalho do Artigo 29.º, que sobre os mesmos se debruçou e emitiu parecer.

i. Finalidades determinadas

O responsável pelo tratamento deve «ponderar cuidadosamente para que finalidade ou finalidades os dados pessoais serão utilizados, e não deve recolher dados pessoais que não sejam necessários, adequados ou relevantes para a finalidade ou finalidades em relação às quais se pretende que os dados sejam objeto de tratamento. [...] A especificação da finalidade requer uma avaliação interna levada a cabo pelo

²⁰³ Conforme mais bem densificado no Capítulo I.

responsável pela proteção de dados», que deve poder «identificar as finalidades, documentando-as, sendo capaz de demonstrar que procedeu à aludida avaliação interna»²⁰⁴. Recomenda-se, sempre que possível e proporcional, que o responsável pelo tratamento especifique que os dados constantes de uma mensagem de correio eletrónico recolhida nos termos acima descritos podem vir a ser tratados no contexto de uma investigação interna, determinando, de forma individualizada, todas as fases de tratamento envolvidas (*i. e.*, todo o processo de tratamento).

ii. Finalidades explícitas

Para além de determinadas, as finalidades do tratamento devem ser «reveladas de forma clara, explicadas ou descritas de forma inteligível»²⁰⁵. Por outras palavras, as finalidades não devem ser ambíguas, devendo o respetivo conteúdo e extensão ser perfeitamente inteligível para qualquer pessoa, designadamente para o responsável pelo tratamento, para um terceiro e, principalmente, para o titular dos dados, que deve conhecer as finalidades nessas condições²⁰⁶.

²⁰⁴ Tradução livre do texto original: «*must therefore carefully consider what purpose or purposes the personal data will be used for, and must not collect personal data which are not necessary, adequate or relevant for the purpose or purposes which are intended to be served [...]. Purpose specification requires an internal assessment carried out by the data controller. [...] must identify what the purposes are, and must also document, and be able to demonstrate, that it has carried out this internal assessment.*» (cfr. p. 15 do documento «*Opinion 03/2013 on purpose limitation (WP 203)*», disponível em <https://ec.europa.eu>, acessível 19.07.2019).

²⁰⁵ Tradução livre do texto original: «*clearly revealed, explained or expressed in some intelligible form.*» (cfr. p. 17 do documento «*Opinion 03/2013 on purpose limitation (WP 203)*», disponível em <https://ec.europa.eu>).

²⁰⁶ Em todo o caso, a respeito do dever de informar destaca-se o seguinte: em relação aos terceiros que remetam espontaneamente mensagens de correio eletrónico à IC, destaca-se a alínea d) do n.º 5 do artigo 14.º do RGPD, a propósito das informações a facultar quando os dados pessoais não são recolhidos junto do titular (segredo de supervisão e segredo bancário). «Assim, quando o fundamento jurídico do tratamento resulte de obrigação legal, não são determinadas imposições de informar» – PINHEIRO, Alexandre Sousa (2018), p. 356.

iii. Finalidades legítimas

Não obstante se encontre intrinsecamente ligado à já tratada licitude do tratamento, a legitimidade do tratamento vai para além do que se expôs a esse propósito, na medida em que, em termos mais genéricos, «requer que as finalidades sejam compatíveis com as disposições legais aplicáveis em matéria de proteção de dados, bem como com outros diplomas legais aplicáveis, tais como legislação laboral, contratos, proteção do consumidor e por aí em diante»²⁰⁷.

Considerando que o tratamento de dados no âmbito de uma investigação interna é também feito no contexto laboral, importa conjugar o RGPD (designadamente, o seu artigo 88.^{o208}) com a Lei n.º 58/2019, de 8 de agosto. Nos termos do artigo 28.º, n.º 1, da referida Lei, «[o] empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais, com as especificidades estabelecidas no presente artigo».

Conforme se referiu no início do presente trabalho, as investigações internas derivam e são consequência necessária da implementação de um sistema de controlo interno, pleno e efetivo. As investigações, estando integradas no sistema de controlo interno, atuam como mecanismo reativo, de forma a mitigar riscos de *compliance*. Nesse sentido, ao tratar dados pessoais no contexto de uma investigação, o responsável pelo tratamento tem como objetivo mais abrangente reagir a riscos de *compliance*, quer estes riscos se traduzam em riscos já materializados ou não.

²⁰⁷ Tradução livre do texto original: «*requires that the purposes must be in accordance with all provisions of applicable data protection law, as well other applicable laws such as employment law, contract law, consumer protection law, and so on.*» (cfr. p. 20 do documento «*Opinion 03/2013 on purpose limitation (WP 203)*», disponível em <https://ec.europa.eu>).

²⁰⁸ Cfr. n.º 1: Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico [...].».

Ora, a **finalidade do tratamento**, enquanto razão específica do tratamento, consiste, justamente, na implementação de mecanismos internos que têm como objetivo investigar suspeitas de riscos de *compliance*. Tais mecanismos (as investigações) comportam, na sua génese, uma fase de recolha de elementos (prova), que compreende o tratamento de dados pessoais, enquanto fase ou estágio necessário à reação àqueles riscos.

Assim, considerando que essa finalidade decorre das normas jurídicas aplicáveis ao setor bancário (designadamente, RGICSF e Aviso do BdP n.º 3/2020²⁰⁹), por constituir pressuposto fundamental da preservação da estabilidade do sistema financeiro (em especial, como se referiu, do subsistema bancário) e, bem assim, da manutenção da confiança que os particulares nele depositam, entendemos que a finalidade descrita é compatível quer com o RGPD, quer com o n.º 1 do artigo 28.º da Lei n.º 58/2019, de 8 de agosto.

Relativamente a terceiros que remetam espontaneamente mensagens de correio eletrónico à IC, quando sejam esses os titulares dos dados, a finalidade do tratamento afigura-se legítima por via da aplicação das normas constantes do RGICSF e, bem assim, Aviso do BdP n.º 3/2020, relativas ao sistema de controlo interno.

²⁰⁹ Conforme mais bem densificado no Capítulo I.

CAPÍTULO III – DA TRANSFERÊNCIA DO RELATÓRIO FINAL PARA O BANCO DE PORTUGAL

1. Introdução

Admitindo que os factos objeto da investigação interna geram responsabilidade contraordenacional, e que o BdP é competente para o respetivo processamento e, bem assim, para a aplicação das respetivas sanções²¹⁰, o relatório final²¹¹, bem como os elementos que o suportam²¹², podem afigurar-se, na perspetiva daquele, elementos essenciais à descoberta da verdade.

A questão que se coloca neste Capítulo consiste em saber se, e em que condições, podem as mensagens de correio eletrónico recolhidas no decurso da investigação (nos termos e nas condições referidas no Capítulo II do presente estudo), ser transferidas para um processo de contraordenação que se encontre em curso, com o intuito de nele valerem como meio de prova²¹³.

Importa precisar, antes de prosseguirmos, que a premissa da nossa análise consiste num processo de contraordenação já instaurado. De fora ficam, pois, o estudo e a análise da transferência de tais elementos em momento prévio à instauração do processo contraordenacional²¹⁴ ou mesmo a questão de saber se tais elementos

²¹⁰ Cfr. artigo 213.º do RGICSF (indicamos apenas a norma geral de atribuição de competência ao BdP, existindo outros diplomas legais que o fazem, a propósito de regimes específicos).

²¹¹ A propósito do relatório final, *vide* pp. 26 e seguintes do presente trabalho.

²¹² Em especial, e no caso do nosso estudo, o conteúdo das mensagens de correio eletrónico recolhidas no decurso da investigação.

²¹³ A propósito da relevância processual dos programas de *compliance*, consta do documento de Estratégia Nacional de Combate à Corrupção 2020-2024 que a mesma «[...] pode ainda concretizar-se no aproveitamento da prova produzida em investigações internas, para tanto devendo a lei processual prever expressamente as condições em que essa prova pode ser valorada em processo penal ou contraordenacional.» – Estratégia Nacional de Combate à Corrupção 2020-2024, p. 46, disponível em <https://www.portugal.gov.pt>, acessível em 23.01.2021.

²¹⁴ Cfr. artigo 120.º, n.º 3, do RGICSF, a propósito do dever de colaboração no âmbito da supervisão prudencial.

podem, depois, ser utilizados no âmbito de um processo contraordenacional que venha a ser instaurado^{215/216}.

Deste modo, a transferência dos aludidos elementos para o processo contraordenacional já instaurado pode ocorrer, pelo menos, através de duas vias possíveis: **(i)** mediante entrega espontânea ao BdP, isto é, por iniciativa da própria instituição²¹⁷ ou **(ii)** através de uma das modalidades de recolha de elementos previstas no artigo 215.º do RGICSF²¹⁸.

O legislador atribuiu ao BdP o direito de exigir de quaisquer pessoas (singulares e coletivas) a entrega de (todos os) documentos «[...] na medida em que os mesmos se revelem necessários à instrução dos processos da sua competência»²¹⁹. Esta disposição legal não é, quanto ao seu conteúdo e alcance, única no RGICSF, sendo possível identificar outros preceitos no mesmo diploma nos quais se dá igual destaque aos deveres de colaboração para com a entidade supervisora²²⁰. A razão de ser de tais

²¹⁵ Note-se que o TC já se pronunciou sobre a concreta questão de saber se «após notícia do ilícito, os Reguladores podem intimar os supervisionados visados a fornecer documentação, sob cominação de sanção por incumprimento do dever de colaboração, fora do quadro de um processo sancionatório formalmente organizado, podendo essa documentação assim obtida, ser utilizada como prova contra o visado/Arguido e/ou outros, em processos sancionatórios futuros», tendo este concluído pela não inconstitucionalidade daquela interpretação normativa (remetendo para a fundamentação constante do acórdão do mesmo Tribunal n.º 360/2013) – acórdão n.º 360/2016, em 08.06.2016, disponível em <http://www.tribunalconstitucional.pt>.

²¹⁶ A opção por restringir o problema que nos ocupa aos processos contraordenacionais em curso deve-se a razões de economia. Com a configuração definida fica, pois, assente que as pessoas contra quem corre determinado processo contraordenacional têm direito ao silêncio e à não autoinculpação, como veremos adiante. Para uma análise aturada do tema da transferência dos elementos obtidos pela autoridade administrativa, na supervisão, para o processo contraordenacional, *vide* MENDES, Paulo Sousa (2012), pp. 307 a 318, BOLINA, Helena Magalhães (2013), pp. 383 a 427 e ALFAFAR, Diana (2013), pp. 319 a 381.

²¹⁷ Não é impossível que tal suceda. Pode, até, fazer sentido, estrategicamente, na medida em que a instituição como que afirma perante o BdP que, não obstante a verificação de determinado risco de *compliance*, o sistema de controlo interno foi eficaz, tendo investigado e contido o risco.

²¹⁸ Pela sua importância prática, ater-nos-emos ao n.º 3 do artigo 215.º do RGICSF.

²¹⁹ Cfr. artigo 215.º, n.º 3, do RGICSF.

²²⁰ A título de exemplo, nos termos do disposto no n.º 3 do artigo 120.º do RGICSF, «[a]s instituições de crédito facultarão ao BdP a inspeção dos seus estabelecimentos e o exame da escrita no local, assim como todos os outros elementos que o Banco considere relevantes para a verificação dos aspetos mencionados no número anterior».

deveres de colaboração prende-se com a circunstância de as IC atuarem profissionalmente nos mercados financeiros, estando, por isso, como contrapartida, sujeitas ao acompanhamento constante do BdP.

Com efeito, estabelecendo um paralelismo com o regime previsto no Código dos Valores Mobiliários, e aqui citando FREDERICO COSTA PINTO, «[...] uma entidade sujeita à supervisão da CMVM [em termos paralelos, sujeita à supervisão do BdP] por actuar profissionalmente no mercado de valores mobiliários [ou nos mercados financeiros] não está perante um processo sancionatório na mesma posição que um cidadão constituído arguido em processo criminal. Este não tem em regra um dever de colaboração com a entidade que conduz o processo, enquanto o profissional do mercado tem um dever de colaboração com a autoridade de supervisão que, como se referiu, é contrapartida do privilégio de acesso ao mercado»²²¹. Ora, dúvidas não podem existir de que tal entendimento vale também para o setor bancário, subsector do sistema financeiro.

Centrando a questão, nos termos do citado n.º 3 do artigo 215.º do RGICSF, a IC tem o dever de entregar «todos os documentos, independentemente da natureza do seu suporte», bastando, para tal, que os mesmos se revelem necessários à instrução do processo de contraordenação. O referido preceito legal atribui, assim, ao BdP um direito potestativo²²², o qual, uma vez exercido, coloca a IC numa situação de sujeição, tendo o dever de entregar os elementos solicitados, sob pena de incorrer, pelo menos, em responsabilidade contraordenacional. É, pois, neste contexto, e ao abrigo desta disposição legal, que o BdP, na pendência de um processo de contraordenação, pode exigir da instituição, no prazo que lhe for concedido, designadamente a entrega do relatório final produzido como consequência da realização de uma investigação interna, bem como os elementos em que este se

²²¹ PINTO, Frederico Costa (2009), p. 97.

²²² «O poder jurídico – ou, quando autonomizado, o direito potestativo – é a prerrogativa resultante de uma norma que permita ao sujeito, pela sua vontade, alterar o ordenamento ou, em regra: modificar uma determinada esfera jurídica.» (CORDEIRO, António Menezes (2009), p. 487)

suportou, *in casu*, as mensagens de correio eletrónico que tenham sido recolhidas no decurso da investigação, para valerem no processo de contraordenação, como meio de prova.

O encadeamento acima descrito levanta, pelo menos, quatro questões, a que cabe dar resposta: (i) a primeira consiste em determinar o conteúdo e o alcance do dever de entrega previsto no n.º 3 do artigo 215.º do RGICSF; (ii) a segunda, de âmbito mais geral, consiste em saber se as mensagens de correio eletrónico que tenham sido recolhidas no âmbito de uma investigação interna têm cabimento na locução legal «todos os documentos»; (iii) em caso afirmativo, a terceira consiste em saber se a IC pode recusar-se a entregar os elementos solicitados, invocando o direito ao silêncio e à não autoinculpação; e (iv) por último, ainda que em termos sumários, importa abordar o tema das proibições de prova em consequência de a IC não ter observado, no decurso da investigação interna, as diretrizes descritas no Capítulo II do presente estudo. De seguida procederemos à análise das questões mencionadas.

2. O conteúdo e o alcance do dever de entrega previsto no n.º 3 do artigo 215.º do RGICSF

«Os meios de obtenção da prova são instrumentos de que se servem as autoridades judiciais e órgãos de polícia criminal para investigar e recolher meios de prova; não são instrumentos de demonstração do *thema probandi*, não são meios de prova, são instrumentos para recolher no processo esses instrumentos»²²³. Nesse sentido, «servem para obter aquelas coisas ou declarações que, por sua vez, servirão para demonstrar a realidade de um facto; trata-se da actividade de recolha dos meios de prova, sejam pessoais ou reais»²²⁴.

²²³ SILVA, Germano Marques da (2011), p. 280. Para uma visão detalhada sobre os pressupostos gerais dos meios de obtenção de prova, vide JESUS, Francisco Marcolino de (2019), pp. 179 e 180.

²²⁴ JESUS, Francisco Marcolino de (2019), p. 179.

Ora, o legislador, ao conferir ao BdP o direito potestativo de exigir das IC a prestação de todos os esclarecimentos e informações, bem como a entrega de todos os documentos que se revelarem necessários à instrução dos processos da sua competência, consagrou um verdadeiro meio de obtenção de prova, através da apreensão²²⁵ de documentos, nomeadamente na sequência de notificação especificamente dirigida à IC para, no prazo que lhe for conferido, entregar os documentos em causa. O incumprimento desse dever é punível como contraordenação.

3. Da entrega, ao Banco de Portugal, de mensagens de correio eletrónico recolhidas no decurso de uma investigação interna

3.1. Da admissibilidade da recolha

A segunda questão colocada consiste em saber se as mensagens de correio eletrónico, recolhidas no contexto de uma investigação interna, têm cabimento na locução legal «todos os documentos, independentemente da natureza do seu suporte»²²⁶ e, por conseguinte, se, em abstrato, o BdP pode exigir das IC a entrega de tais documentos²²⁷.

²²⁵ Sobre a definição de apreensão e respetivas modalidades previstas no CPP, *vide* JESUS, Francisco Marcolino de (2019), pp. 252 e ss.

²²⁶ Note-se que a proposta de lei n.º 227/X, subjacente à Lei n.º 28/2009, de 19 de junho, que introduz o então n.º 3 e atual n.º 5 do artigo 215.º do RGICSF não faz menção expressa às mensagens de correio eletrónico.

²²⁷ Esta questão tem sido igualmente colocada, designadamente pela doutrina, em relação ao artigo 20.º da Lei n.º 19/2012, de 08 de maio (“Novo Regime Jurídico da Concorrência”), em tudo similar, neste segmento, ao artigo 215.º, n.º 3, do RGICSF. Nesse sentido, *vide* o entendimento de GONÇALO ANASTÁCIO e DIANA ALFAFAR: estes autores entendem que o legislador pretendeu excluir daquele preceito a apreensão do correio eletrónico – ANASTÁCIO, Gonçalo e ALFAFAR, Diana (2017), p. 343. Note-se, porém, que o entendimento da AdC nesta matéria é o de que o aludido preceito a habilita a proceder à apreensão de mensagens de correio eletrónico (*vide*, ponto 52 das linhas de orientação sobre instrução de processos, disponível em <http://www.concorrencia.pt>, acessível em 23.11.2020).

Encontramos, quer no Direito Civil²²⁸, quer no Direito Penal²²⁹, uma definição de documento. «Enquanto no direito civil se dá um relevo primacial à função do documento como objecto, no direito penal prima a função do documento como declaração – é esta que constitui o documento, e não o seu suporte material»²³⁰.

VÂNIA COSTA RAMOS aponta três elementos comuns à generalidade dos documentos, a saber: (i) materialização, (ii) ter origem humana e (iii) estar apto para entrada no tráfico jurídico e função probatória²³¹.

Ora, atento o conceito de correio eletrónico que acompanhamos²³², cremos que a mensagem de correio eletrónico, conceptualmente, configura um “documento” na aceção do artigo 215.º, n.º 3, do RGICSF²³³.

Resta determinar se, e em que condições, esse documento goza da tutela conferida à apreensão de correspondência²³⁴ ou à apreensão de correio eletrónico²³⁵, que limite

²²⁸ Cfr. Artigo 362.º, 2.ª parte, do CC.

²²⁹ Cfr. Artigo 255.º, alínea a), do CP.

²³⁰ RAMOS, Vânia Costa (2006), p. 134.

²³¹ RAMOS, Vânia Costa (2006), p. 135.

²³² «Fluxo informacional e comunicacional digital, sob o formato de texto, voz, som, imagem ou gráfico, que é colocado por um assistente ou consumidor de redes ou serviços de comunicações eletrónicas acessíveis ao público, no âmbito de um ciclo internacional e comunicacional (tendencialmente) fechado, através de um ponto terminal de rede, na rede pública de comunicações eletrónicas, conduzida até ao servidor de *mail* ou ao terminal do destinatário do fluxo até que o mesmo proceda à sua recolha, leitura e/ou posterior eliminação.» (RODRIGUES, Benjamim Silva, (2008), p. 444)

²³³ A este propósito, GONÇALO ANASTÁCIO e DIANA ALFAFAR, referem que: «na falta de uma definição legal clara de “documento” para efeitos de aplicação do n.º 1 do artigo 20.º do RJC [em tudo similar ao n.º 3 do artigo 215.º do RGICSF], a proteção do sigilo das comunicações deve ser a fronteira que separa a mensagem de correio eletrónico, protegida pelo sigilo, do documento em suporte digital, não protegido pelo sigilo, e, por isso passível de apreensão.». Mais referem que «o n.º 1 do artigo 20.º, ao permitir a apreensão de documentos independentemente da sua natureza ou do seu suporte [neste segmento, portanto, em tudo similar ao n.º 3 do artigo 215.º do RGICSF], poderá assim abranger, não a apreensão de correio eletrónico que se encontre na caixa de entrada, mas sim que se encontre, por exemplo, impresso em papel, ou de um qualquer documento armazenado em suporte digital (como um documento em formato word ou excel).» – ANASTÁCIO, Gonçalo e ALFAFAR, Diana (2017), p. 343.

²³⁴ Artigo 179.º do CPP.

²³⁵ Artigo 189.º, n.º 1, do CPP e artigo 17.º da Lei n.º 109/2009, de 15 de setembro (“Lei do Cibercrime”).

ou impeça a sua recolha pelo BdP. Em especial, considerando que, nos termos do disposto no artigo 42.º do RGCO «[n]ão é permitida [...] a intromissão na correspondência ou noutros meios de telecomunicação [...]»²³⁶.

Em termos gerais, acompanhamos a doutrina que sustenta que na garantia do domicílio e da correspondência «cabe o chamado correio eletrónico»²³⁷, porque o segredo da correspondência abrange seguramente as correspondências mantidas por via das telecomunicações»²³⁸. E embora a mensagem de correio eletrónico não equivalha à correspondência dita tradicional²³⁹, a mesma é, não obstante, pelo menos em determinado estágio do circuito comunicacional, uma comunicação. Enquanto comunicação, a mensagem de correio eletrónico beneficia da tutela conferida à correspondência e às telecomunicações²⁴⁰.

O dever de não ingerência na correspondência e nas telecomunicações tem uma dimensão negativa e uma dimensão positiva. Na sua dimensão negativa, tal dever acarreta «não só a obrigação de princípio de não divulgar o conteúdo das comunicações privadas, mas também de não aceder às circunstâncias em que as mesmas foram efetuadas». Por seu turno, na sua dimensão positiva, este dever

²³⁶ Podendo suscitar-se a questão de saber se o artigo 42.º do RGCO é subsidiariamente aplicável ao RGICSE, salienta-se que, em termos paralelos, a propósito da Lei da Concorrência, explanou o TC que o artigo 42.º do RGCO «é aplicável aos processos sancionatórios da concorrência, uma vez que a regra geral nele estatuída não foi expressamente afastada pela Lei 18/2003 e do artigo 17.º.» – proferido no processo 937/07, em 16.11.2007 disponível em <http://www.concorrencia.pt>, acessível em 11.07.2019.

²³⁷ No sentido de a correspondência abranger também as comunicações eletrónicas, *vide* JESUS, Francisco de (2019), p. 263.

²³⁸ CANOTILHO, Gomes, MOREIRA, Vital (2007), p. 544.

²³⁹ No sentido de uma carta, impressa em papel, fechada. «A correspondência é por definição fechada – assim que é aberta deixa de o ser e passa a ter natureza documental. Enquanto fechada, a correspondência é sigilosa por natureza, e, logicamente, goza da proteção constitucional que o art. 34.º, n.º 1 da Constituição da República Portuguesa concede ao “sigilo da correspondência”» (acórdão do TRL, proferido no processo n.º 463/07.3TAAML-A.L1-3, em 02.03.2011, disponível em <http://www.dgsi.pt>).

²⁴⁰ «Quando ao correio eletrónico, o princípio fundamental é o de considerar sujeito às regras e exigências – designadamente de sigilo – típicas do correio tradicional, já que acaba por representar, na essência, uma comunicação entre duas pessoas, que a elas deverá ficar confinada» – SILVEIRA, Luís Lingnau da (2013), p. 143.

acarreta a «obrigação de o Estado adotar os instrumentos jurídicos necessários para manter a comunicação e o seu circunstancialismo como “fechados” (nomeadamente, através da aprovação de leis destinadas à proteção dos dados de comunicação)»²⁴¹. Nesta sede, interessa-nos a dimensão negativa do dever de não ingerência.

Ora, para responder à questão de saber se, no caso que nos ocupa, estamos perante uma ingerência, importa compreender se a mensagem de correio eletrónico recolhida no contexto de uma investigação interna, pronta para ser, caso assim seja solicitado, entregue ao BdP, é, ainda, uma comunicação.

Antes de mais e para melhor enquadramento, importa tecer algumas considerações de carácter mais abstrato, aqui recordando o entendimento de RITA CASTANHEIRA NEVES, para quem a comunicação recebida já não é em bom rigor comunicação, uma vez que cumpriu o circuito comunicacional, sendo apenas um registo, enfim, um ficheiro²⁴².

Por princípio, parecer-nos-ia acertado o entendimento de que a mensagem de correio eletrónico deixa de ser comunicação a partir do momento em que é recebida pelo destinatário, isto é, a partir do momento em que a mensagem jaz na respetiva caixa de correio eletrónico. Porém, reconhecemos e concordamos que esta solução é artificial e pode conduzir a situações materialmente injustas, na medida em que casos existirão, de facto, em que a mensagem de correio eletrónico, não obstante tenha sido recebida pelo destinatário, não foi efetivamente aberta/lida, designadamente porque o destinatário de uma mensagem de correio eletrónico pode recebê-la, ler o seu conteúdo e, em seguida, marcá-la como “não lida”²⁴³. Consequentemente, a

²⁴¹ Acórdão do TC n.º 403/2015, em 27.08.2015, disponível em <http://www.tribunalconstitucional.pt>.

²⁴² NEVES, Rita Castanheira (2011), pp. 260 e 261. Em sentido idêntico, acórdãos do TRG, proferido no processo n.º 1396/08.1PBGMR-A.G1, em 12.10.2009 e do TRL, proferido no processo n.º 463/07.3TAALM-A.L1-3, em 02.03.2011, todos disponíveis em www.dgsi.pt.

²⁴³ «O correio eletrónico pode ser arquivado pelo destinatário sem ser lido; pode ser arquivado juntamente com mensagens enviadas e até rascunhos de mensagens eventualmente a enviar» – CARDOSO, Rui (2018), p. 71. «Sendo, inversamente, igualmente possível, e empiricamente constatável como comum que *e-mails* que constam como abertos não tenham sido efetivamente lidos

transposição, sem mais, do critério descrito para o domínio das contraordenações, poderia permitir, de forma artificial e arbitrária, ingerências no conteúdo de comunicações eletrônicas²⁴⁴.

Importa, no entanto, saber se, ainda que em rigor a mensagem de correio eletrónico recebida não seja já uma comunicação, goza ainda assim da tutela conferida pelo artigo 189.º do CPP e, bem assim, pela Lei do Cibercrime.

Ora, JOSÉ LOBO MOUTINHO e PEDRO DURO veem²⁴⁵, na extensão do regime previsto nos artigos 187.º e 188.º do CPP às conversações transmitidas por correio eletrónico, por via do respetivo artigo 189.º, uma intenção clara do legislador no sentido de abranger as mensagens de correio eletrónico, independentemente de se tratar ainda de uma comunicação, abrangendo, portanto, as mensagens de correio eletrónico enquanto documentos produzidos na sequência das comunicações²⁴⁶. Intenção essa que, segundo estes autores, teria ficado definitivamente resolvida com a entrada em vigor da Lei do Cibercrime²⁴⁷, em particular face ao disposto no respetivo artigo

(v.g. por se ter meramente passado o cursor *touch*, ou por apenas se querer ver sinalizadas – indicadas como fechadas – as mensagens que acabam de chegar)» – ANASTÁCIO, Gonçalo e ALFAFAR, Diana (2017), p. 342.

²⁴⁴ A este respeito refere BENJAMIM SILVA RODRIGUES que «[o] problema não surgiria com as mensagens que tenham sido impressas em papel, visto que haveria prova concludente da sua “abertura/leitura” e, por outro lado, com as que tenham sido arquivadas numa pasta do computador distinta da que medeia a sua receção (mail-box)». (RODRIGUES, Benjamim Silva (2008), p. 437). O TC (em momento anterior à Lei do Cibercrime e ainda no domínio da Lei n.º 18/2003), subscrevendo o entendimento de PEDRO VERDELHO, pronunciou-se no sentido de que as «mensagens de correio eletrónico que já tenham sido abertas pelo seu destinatário e foram deixadas gravadas no computador [...]» não são já comunicação (processo n.º 937/07, em 16.11.2007, disponível em: <http://www.concorrencia.pt>, acessível em 20.07.2020).

²⁴⁵ A respeito do Novo Regime Jurídico da Concorrência (MOUTINHO, José Lobo e DURO, Pedro (2017), pp. 319 e 320).

²⁴⁶ No mesmo sentido, PAULO PINTO DE ALBUQUERQUE: «As **comunicações já recebidas** pelo destinatário e guardadas em suporte digital estão incluídas no âmbito da proibição legal, como resulta do disposto no artigo 189.º do CPP. Por exemplo, as mensagens de *email* (já abertas ou não) arquivadas no computador ou as mensagens arquivadas no cartão de telemóvel não podem ser aproveitadas como meio de prova de uma contra-ordenação. As comunicações já abertas, guardadas em suporte não digital, podem ser apreendidas» – ALBUQUERQUE, Paulo Pinto de (2011), p. 160.

²⁴⁷ Lei n.º 109/2009, de 15 de setembro.

17.²⁴⁸, que não distingue mensagens de correio eletrónico abertas de mensagens de correio eletrónico não abertas²⁴⁹.

Porém, salvo melhor opinião, entendemos que, quer o disposto no artigo 189.º do CPP, quer o disposto na Lei do Cibercrime, não são subsidiariamente aplicáveis ao processo de contraordenação em geral e ao processo de contraordenação setorial bancário, da competência do Banco de Portugal. É certo que o n.º 1 do artigo 41.º do RGCO, *ex vi* artigo 232.º do RGICSF dispõe que «sempre que o contrário não resulte deste diploma, são aplicáveis, devidamente adaptados, os preceitos reguladores do processo criminal». Porém, o artigo 42.º, n.º 1, do RGCO, exclui expressamente a intromissão na correspondência ou nos meios de telecomunicação, pelo que não nos parece defensável a asserção de que tais regimes sejam subsidiariamente aplicáveis ao processo de contraordenação²⁵⁰.

²⁴⁸ Nos termos deste preceito, «[q]uando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal».

²⁴⁹ Nesse sentido, CARDOSO, Rui (2018), p. 69 e RAMALHO, David Silva (2017), pp. 278 e 279. Também, em sentido idêntico, o TRL explanou que «o legislador [na lei do cibercrime] não quis admitir qualquer destriça entre correio eletrónico fechado ou aberto, por considerar igualmente não existirem razões para considerar diminuídas as exigências garantísticas do correio eletrónico quando aberto relativamente ao correio eletrónico fechado, atenta a natureza própria destas comunicações». Tendo concluído que «[...] a lei do Cibercrime criou em relação à apreensão de “correio electrónico e registos de comunicações de natureza semelhante” um regime específico e unitário, que visou submeter ao regime da apreensão da correspondência, independentemente de as mensagens se encontrarem abertas ou fechadas. Deste modo, somos a entender que as mensagens de correio electrónico que se encontrem armazenadas num sistema informático só podem ser apreendidas mediante despacho prévio do Juiz de Instrução Criminal, devendo ser o juiz a primeira pessoa a tomar conhecimento do conteúdo da correspondência, conforme remissão expressa para o artº 179º do CPP» – processo n.º 184/12.5TELSB-B.L1-3, proferido em 07.03.2018, disponível em <http://www.dgsi.pt>.

²⁵⁰ Estabelecendo um paralelismo com o Novo Regime da Concorrência, GONÇALO ANASTÁCIO e DIANA ALFAFAR sustentam que «[...] tão pouco se poderá autorizar a AdC a apreender mensagens de correio eletrónico com base numa aplicação subsidiária dos regimes para a apreensão de correio eletrónico estabelecidos no CPP ou na Lei do Cibercrime. Em primeiro lugar porque, como vimos, os artigos 42.º do RGCO e 34.º, n.º 4 da CRP afastam a possibilidade de apreensão de correspondência em processos de contraordenação, impedindo assim a apreensão de correio eletrónico nos termos do artigo 17.º da Lei do Cibercrime. Por outro lado, o regime das escutas

Porém, no caso do nosso estudo, cremos que a problemática acima descrita é ultrapassada pelas circunstâncias particulares em que a transferência das mensagens de correio eletrónico para o processo contraordenacional ocorre²⁵¹: estamos a tratar de mensagens necessariamente recebidas, abertas e lidas, na medida em que foram recolhidas pelo investigador no decurso da investigação interna, cumprindo as condições descritas no Capítulo II.

Ora, a mensagem de correio eletrónico recolhida nestes termos, cumpriu o seu circuito comunicacional, não estando já, sequer, na esfera jurídica (e, por maioria de razão, no computador) do remetente e do destinatário originários.

De todo o modo, nem por isso o conteúdo da mensagem de correio eletrónico deixa de merecer, em abstrato, a tutela conferida à privacidade, sendo a propósito deste ponto que a análise expendida no Capítulo II do presente trabalho se interliga com a análise constante do presente Capítulo. O tratamento que se segue é um tratamento bifurcado, em função do(s) concreto(s) interveniente(s) da mensagem.

3.2. Na perspetiva do colaborador da instituição

Conforme tratámos a respeito do Capítulo II *supra*, por regra²⁵², só é admitida a recolha, pelo investigador, de mensagens de correio eletrónico que tenham natureza

consagrado no n.º 1 do artigo 189.º do CPP apenas se aplica nos tais casos restritos do artigo 187.º do CPP, já mencionados.» – ANASTÁCIO, Gonçalo e ALFAFAR, Diana (2017), P. 344.

²⁵¹ A propósito da discussão em torno da eventual aplicação subsidiária da Lei do Cibercrime ao processo contraordenacional, ainda que se entendesse que a mesma é aplicável, o que não se concede, parece-nos que o respetivo artigo 17.º nunca teria aplicação ao caso objeto do nosso estudo, desde logo porque a recolha não é consequência de uma «pesquisa informática ou outro acesso legítimo a um sistema informático». Na verdade, conforme se referiu anteriormente, as mensagens de correio eletrónico serão recolhidas pelo BdP, na estrita medida em que as mesmas constituem parte integrante do relatório produzido pela IC, voluntariamente apresento ou na sequência de notificação do BdP ao abrigo do n.º 3 do artigo 215.º do RGICSF.

²⁵² Dizemos por regra, na medida em que, tendo a mensagem natureza pessoal ou extraprofissional, a mesma só pode ser recolhida se o trabalhador consentir nessa recolha.

exclusivamente profissional e na estrita medida em que se encontrem assegurados os pressupostos atinentes ao tratamento de dados pessoais²⁵³.

Ora, na medida em que concluímos que numa investigação interna somente é admissível a recolha de mensagens de correio eletrónico de natureza profissional – estando, por conseguinte, vedada a recolha de quaisquer mensagens de natureza privada ou extraprofissional, salvo consentimento do colaborador (nos termos e nas condições *supra* descritos no Capítulo II do presente trabalho) –, admitindo que a instituição cumpriu esta diretriz, a tutela da privacidade, pelo menos no que ao colaborador da instituição diz respeito, deixa, a nosso ver, de fazer sentido. É que a recolha teve justamente como fundamento o facto de a concreta mensagem não conter quaisquer elementos ou informações pessoais ou extraprofissionais²⁵⁴.

Nas hipóteses em que a mensagem contenha elementos ou informações pessoais, a entrega só ocorreu porque o colaborador deu o seu consentimento (conhecendo e prevendo que a transferência para o processo contraordenacional e a correspondente utilização como meio de prova seriam uma possibilidade). Nestes casos, é fundamental que o colaborador seja expressamente advertido da possibilidade de a mensagem de correio eletrónico poder ser transferida para o BdP, sob pena de o consentimento não ser válido em toda a sua extensão²⁵⁵.

Deste modo, no que se refere ao colaborador da instituição, admitindo que a recolha da mensagem de correio eletrónico teve lugar nas condições *supra* descritas, não vislumbramos, em abstrato, quaisquer obstáculos à respetiva transferência para o processo contraordenacional²⁵⁶.

²⁵³ O que, no contexto laboral, implica a observância dos requisitos descritos no Capítulo II.

²⁵⁴ Nos termos do disposto no artigo 22.º, n.º 1, do CT.

²⁵⁵ Sendo aconselhável que, do auto de entrega, conste uma qualquer declaração do trabalhador que ateste que tomou conhecimento dessa possibilidade.

²⁵⁶ O fundamento do tratamento de dados reside na alínea e) do n.º 1 do artigo 6.º do RGPD. Este fundamento «[...] pode abranger as situações nas quais o responsável pelo tratamento comunique, de forma proactiva, dados a um terceiro investido de tal autoridade pública. Tal pode acontecer, por

Porém, se a mensagem tiver como interveniente um terceiro, o percurso lógico não é exatamente o descrito. É o que veremos de seguida.

3.3. Na perspetiva de um terceiro que figure na mensagem de correio eletrónico

Pode suceder que, na mensagem de correio eletrónico, para além de figurar um colaborador da instituição, figure também um terceiro²⁵⁷. A recolha, nestas circunstâncias, ocorreria, muito provavelmente, sem a intervenção do terceiro, o qual pode até nem ter conhecimento da entrega. Esta possibilidade é, à primeira vista, alarmante. Mais alarmante se afiguraria se pensarmos na possibilidade de a mensagem de correio eletrónico poder conter, na perspetiva do terceiro, menções ou declarações autoinculpatórias.

Existem, contudo, vários pontos a tomar em consideração. O primeiro prende-se com a **natureza da informação veiculada** (confidencial ou não confidencial), o segundo com a **qualidade do destinatário** e o terceiro com a qualidade do próprio **Supervisor e do respetivo âmbito de intervenção**, enquanto destinatário último da mensagem de correio eletrónico.

Ainda que não em termos exatamente coincidentes, tem interesse estabelecer um paralelismo com o Direito Civil em matéria de cartas missivas. No Direito Civil, a menos que o remetente de uma carta missiva lhe atribua natureza confidencial²⁵⁸, a

exemplo, no caso de um responsável pelo tratamento se aperceber de que foi cometido um crime e facultar essa informação às autoridades competentes por iniciativa própria» – Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento de dados na aceção do artigo 7.º da Diretiva n.º 95/46/CE, do PE e do Conselho, p. 29, disponível em <https://www.gdpd.gov.mo>, acessível em 25.04.2019.

²⁵⁷ No sentido de pessoa externa à instituição. Para este exercício, vamos assumir que esse terceiro é cliente da instituição.

²⁵⁸ Fazendo o paralelismo com o regime previsto no CC, a propósito das cartas-missivas confidenciais (artigo 75.º), «[a] natureza confidencial da carta missiva deve resultar de declaração feita pelo seu

mesma não tem tal natureza. Ora, sendo a missiva confidencial, a mesma só pode ser divulgada «com o consentimento do seu autor»²⁵⁹. Não sendo confidencial, o destinatário apenas pode divulgá-la se a divulgação não contrariar a expectativa do autor²⁶⁰.

Estabelecendo um paralelismo com o regime que acabou de se descrever, mesmo na hipótese de o remetente não atribuir natureza confidencial à mensagem de correio eletrónico, a mesma só poderia ser divulgada a terceiros se a divulgação não contrariasse a expectativa do autor, «isto é, [se a mesma não contrariar] as limitações que resultem implicitamente do conteúdo e natureza da carta».

Delimitado o regime geral, o nosso caso, porém, apresenta, desde logo uma diferença: a confidencialidade da mensagem pode resultar *ope legis*, não estando dependente de qualquer manifestação de vontade (expressa ou tácita) do remetente, na medida em que, nos termos da lei, a IC tem o dever de segredo em relação «a factos ou elementos respeitantes à vida da instituição ou às relações desta com os seus clientes»²⁶¹ cujo conhecimento lhes advenha exclusivamente do exercício das suas funções ou da prestação dos seus serviços»²⁶². A mensagem poderá, por isso, e por força da lei, ser confidencial. Da circunstância descrita decorreria, mais uma vez com recurso às normas do Direito Civil, que, tendo a mensagem natureza confidencial, a mesma não deveria ser divulgada, salvo consentimento do remetente.

Contudo, o destinatário da mensagem não é um destinatário qualquer. É uma IC, sujeita, por isso, e de forma conatural, à supervisão do BdP, com o conteúdo e a

autor. Esta declaração não tem, todavia, de ser expressa» (LIMA, Pires de e VARELA, Antunes, (1987), p. 107).

²⁵⁹ Cfr. artigo 76.º, n.º 1, do CC.

²⁶⁰ Cfr. artigo 78.º do CC.

²⁶¹ O termo cliente deve ser interpretado num sentido lato, abrangendo quer as pessoas (singulares ou coletivas) com as quais a instituição tem uma determinada relação contratual, como as pessoas que estiveram em vias de contratar ou cujo relação contratual cessou por qualquer motivo.

²⁶² Cfr. artigo 78.º, n.º 1, do RGICSF.

extensão previstos na lei. Ora, quando o remetente envia a sua mensagem à IC, conhece ou, pelo menos, devia conhecer esta circunstância. De facto, conforme tem vindo a ser referido ao longo do presente trabalho, a IC, em matéria de controlo de cumprimento, deve cuidar, de forma autorregulada, do cumprimento da lei, como modo de assegurar o regular funcionamento da atividade bancária, assim preservando a estabilidade dos mercados financeiros e a confiança que os cidadãos neles depositam. Nesse sentido, não obstante a instituição (e todos que nela exerçam funções) tenha o dever de guardar segredo relativamente a factos que respeitem à sua relação com os seus clientes, tal dever não é absoluto, cedendo em determinadas circunstâncias.

Com efeito, nos termos do disposto na alínea *a*) do n.º 2 do artigo 79.º do RGICSF, «[f]ora do caso previsto no número anterior [a hipótese de o cliente consentir na revelação dos factos sujeitos a segredo], os factos e elementos cobertos pelo dever de segredo só podem ser revelados: [...] a) Ao Banco de Portugal, no âmbito das suas atribuições». Ora, quando o BdP, na sequência de um processo de contraordenação que tenha sido instaurado, pretende obter, por uma das vias acima descritas, mensagens de correio eletrónico que tenham sido recolhidas no decurso de uma investigação interna, está, naturalmente, a atuar ao abrigo das suas atribuições²⁶³ (supervisão sancionatória).

Nesse sentido, à luz do RGICSF, parece-nos que a tutela legal conferida a esse terceiro (cliente), através do segredo bancário, cede em prol de valores protegidos

²⁶³ Cfr. artigo 17.º da Lei Orgânica do BdP.

como a estabilidade e a confiança no sistema financeiro, bem como o regular funcionamento da atividade bancária^{264/265}.

Em suma, nos termos e com aqueles fundamentos, parece-nos que as mensagens de correio eletrónico que tenham sido recolhidas e impressas no decurso de uma investigação interna, nas quais figure um terceiro (cliente), podem ser transferidas para determinado processo contraordenacional que corra os seus termos no BdP, na medida em que as mesmas se revelem necessárias à instrução de processos da sua competência.

4. O problema do direito ao silêncio e à não autoinculpação²⁶⁶

4.1. Introdução

Constatámos, nas linhas que antecedem, que as mensagens de correio eletrónico que tenham sido recolhidas e impressas no contexto de uma investigação interna podem ser objeto de transferência para um processo contraordenacional em curso.

A questão que inelutavelmente se coloca consiste em saber se a instituição em causa se pode recusar a entregar os mencionados documentos, invocando, *per se*, isto é, independentemente do conteúdo da mensagem de correio eletrónico, o direito ao

²⁶⁴ Este entendimento parece sair reforçado pela leitura do n.º 6 do artigo 215.º do RGICSF, segundo o qual «[s]empre que, no decurso de uma busca, sejam apreendidos equipamentos ou suportes de informação que sejam suscetíveis de conter informação que não respeite apenas a clientes, operações ou informação de natureza contabilística e prudencial da instituição, são os mesmos apresentados à autoridade judiciária competente [...]», na medida em que, sendo a informação restrita àqueles elementos (clientes, operações ou informação de natureza contabilística e prudencial da instituição), o BdP pode tomar conhecimento dela sem o crivo da autoridade judiciária competente.

²⁶⁵ Vimos, a propósito do Capítulo II, que o facto de risco de *compliance* constituir a prática de uma contraordenação constitui um elemento preponderante a tomar em consideração no teste de ponderação, a propósito da licitude do tratamento de dados.

²⁶⁶ Acolhemos a expressão utilizada por AUGUSTO SILVA DIAS e VÂNIA COSTA RAMOS, por nos parecer mais adequada às contraordenações, na medida em que não há uma incriminação, no sentido da assunção da prática de um crime (DIAS, Augusto Silva e RAMOS, Vânia Costa (2009)).

silêncio e à não autoinculpação²⁶⁷. E, adicionalmente, como subquestão relacionada com a primeira enunciada, consiste em saber que tratamento dar às mensagens de correio eletrónico que contenham declarações autoinculpatórias.

Para responder às questões enunciadas, importa primeiramente traçar o fundamento e o alcance do direito ao silêncio e à não autoinculpação.

4.2. Fundamento e alcance do direito ao silêncio e à não autoinculpação

Segundo o princípio *nemo tenetur se ipsum accusare*²⁶⁸, «ninguém é obrigado a admitir a sua participação numa infracção, a contribuir para a sua própria incriminação»²⁶⁹. Não obstante este princípio não surja expressamente consagrado na CRP²⁷⁰, o mesmo tem consagração expressa no CPP, «na vertente do direito ao silêncio (arts. 61.º, n.º 1, al. d), 132.º, n.º 2, 141.º, n.º 4, al. a), e 343.º, n.º 1, do CPP)»²⁷¹.

O aludido princípio é aplicável aos processos de contraordenação²⁷², por via do disposto no n.º 10 do artigo 32.º e n.º 4 do artigo 20.º, ambos da CRP²⁷³.

²⁶⁷ «Embora não tenham exatamente o mesmo conteúdo, o direito ao silêncio e o direito à não autoincriminação estão incindivelmente ligados: não lhe sendo reconhecido o direito a manter-se em silêncio, o arguido seria obrigado a pronunciar-se revelando informações que o podem eventualmente prejudicar na medida em que contribuem para a sua condenação» – DIAS, Jorge de Figueiredo e ANDRADE, Manuel da Costa (2009), p. 38.

²⁶⁸ Sobre a origem do princípio *nemo tenetur*, vide DIAS, Augusto Silva e RAMOS, Vânia Costa (2009), pp. 9 a 14.

²⁶⁹ MENDES, Paulo Sousa (2009), p. 15.

²⁷⁰ Sobre o concreto fundamento constitucional do direito ao silêncio e à não autoinculpação vide, acerca da divergência entre a tese substantiva e a tese processualista, (DIAS, Jorge de Figueiredo e ANDRADE, Manuel da Costa (2009), pp. 40 e seguintes.

²⁷¹ DIAS, Augusto Silva e RAMOS, Vânia Costa (2009), p. 14.

²⁷² «[D]e acordo não só com a Constituição, mas também com a Convenção Europeia dos Direitos do Homem o direito ao silêncio, enquanto garantia de defesa, deve estender-se a qualquer processo onde possam ser aplicadas sanções de carácter punitivo, ainda que não criminal.» (DIAS, Jorge de Figueiredo e ANDRADE, Manuel da Costa (2009), pp. 46)

²⁷³ MENDES, Paulo Sousa (2009), p. 16.

Relativamente ao alcance do direito ao silêncio²⁷⁴ e à não autoinculpação²⁷⁵, importa, a título prévio, recordar o que atrás referimos a propósito dos especiais deveres de colaboração da IC, enquanto entidade supervisionada, para com o supervisor, *in casu*, o BdP. A este propósito escreveu FREDERICO DA COSTA PINTO que «[a]s entidades que atuam profissionalmente ou de forma qualificada no mercado de valores mobiliários e que estão, por isso, sujeitas a um acompanhamento regular da CMVM (artigo 359.º do CdVM) têm o dever legal de prestar toda a colaboração solicitada à autoridade de supervisão [...]»²⁷⁶. Apesar de este entendimento ter sido exposto no âmbito de um parecer que tinha como elemento fáctico o subsector de mercado de valores mobiliários e, por conseguinte, a relação entre a entidade supervisionada e a CMVM, o mesmo é, quanto a nós, integralmente extensível ao setor bancário, enquanto subsector do mesmo setor financeiro. Deve acrescentar-se, a esse propósito, que «[o] facto de existir em abstracto tutela sancionatória para garantir este regime de transparência absoluta e a efectividade dos poderes da autoridade de supervisão em nada colide com a concreta posição jurídica dos visados ao ponto de converter os elementos fornecidos numa prova proibida [...]»²⁷⁷.

Dito isto, no que releva para efeitos do presente trabalho, pelo menos três teses podem ser avançadas quanto à relação entre o citado dever de colaboração e o alcance do direito ao silêncio e à não autoinculpação, no âmbito das contraordenações.

A primeira reconhece ao arguido o direito de recusar contribuir, por que forma for, designadamente através da entrega de quaisquer documentos, para a sua

²⁷⁴ Este direito «traduz-se na faculdade reconhecida ao arguido de não se pronunciar sobre os factos que lhe são imputados [...]» (acórdão do TC, proferido no processo n.º 298/2019, em 15.05.2019, disponível em <http://www.tribunalconstitucional.pt>)

²⁷⁵ Este direito «impede a transformação do arguido em meio de prova por via de uma colaboração involuntária obtida com recurso a meios coercivos ou enganosos.» (acórdão do TC, proferido no processo n.º 298/2019, em 15.05.2019, disponível em <http://www.tribunalconstitucional.pt>)

²⁷⁶ PINTO, Frederico Costa (2009), pp. 81 e seguintes.

²⁷⁷ PINTO, Frederico Costa (2009), pp. 85 e seguintes.

autoinculpação²⁷⁸. A este propósito, refere AUGUSTO SILVA DIAS que «[n]a verdade, se num vulgar procedimento administrativo um sujeito pode legitimamente recusar-se a entregar um documento invocando o direito à não auto-inculpação seria incompreensível que outro tanto não sucedesse num processo de contra-ordenação punível com coima da ordem dos milhões de euros. Atentaria contra o princípio da proporcionalidade se um procedimento instituído para apuramento da responsabilidade pela prática de infrações graves pudesse ser dotado de menos garantias do que um outro concebido para determinar a responsabilidade por infrações comparativamente menores»²⁷⁹.

A segunda tese, pugnada por JORGE DE FIGUEIREDO DIAS e MANUEL DA COSTA ANDRADE sustenta que os deveres de colaboração entre as entidades supervisionadas e o supervisor operam uma restrição ao princípio do *nemo tenetur*²⁸⁰.

A terceira, ao invés, entende que «[o] direito ao silêncio abrange apenas e só o direito a não responder a perguntas ou prestar declarações sobre os factos que lhe são imputados e não abrange o direito de recusar a entrega de elementos que estejam em seu poder»²⁸¹. Ou seja, de acordo com este entendimento, o arguido tem o dever de entregar os documentos que se encontrem na sua posse, quando assim seja solicitado pelo supervisor, salvo se os mesmos, acrescentamos, consubstanciarem ou integrarem, eles próprios, declarações sobre os factos que lhe são imputados²⁸².

²⁷⁸ A questão tal como vem tratada pelo 1.º juízo de pequena instância criminal de Lisboa é diferente. Em causa estava a utilização em processo de contraordenação de documentos entregues pelo arguido à CMVM antes da instauração de qualquer processo. Contudo, aquele entendimento está implícito (sentença proferida no processo n.º 4907/06.3TFLSB, não publicada, mas a que tivemos acesso).

²⁷⁹ DIAS, Augusto Silva (2018), p. 201. Esta primeira tese, debruçando-se especificamente sobre os aludidos pareceres prestados por FREDERICO COSTA PINTO e por Jorge de FIGUEIREDO DIAS e MANUEL DA COSTA ANDRADE, discorda que a previsão de deveres de cooperação entre a entidade supervisora e o supervisionado operem uma restrição legislativa à vigência do *nemo tenetur* – DIAS, Augusto Silva (2010), pp. 249 e 250.

²⁸⁰ DIAS, Jorge de Figueiredo e ANDRADE, Manuel da Costa (2009), p. 48.

²⁸¹ PINTO, Frederico Costa (2009), pp. 95. Nesse sentido, também, o acórdão do TRL, proferido no processo n.º 2140/08-9, em 30.10.2008, disponível em <https://www.cmvm.pt>, acessível em 18.01.2020.

²⁸² «Não obstante o dever de colaboração, todas as pessoas notificadas pela AdC gozam da prerrogativa de não autoinculpação, no sentido de não serem obrigadas a confessar a prática de

Assim, sobre o arguido recai, tão-somente, o dever de «fornecer as informações estritamente factuais que lh[e] forem pedidas e os documentos preexistentes referenciados pelas autoridades reguladoras»²⁸³.

Deste modo, conforme refere FREDERICO COSTA PINTO, estando em curso determinado processo contraordenacional, ocorre uma cessação parcial dos deveres de colaboração do arguido para com o supervisor²⁸⁴. A propósito desta terceira tese referiu muito recentemente o TC que esta abordagem «é conciliável, quer com a jurisprudência Orkem²⁸⁵ do Tribunal de Justiça da União Europeia (nesse sentido, v. O Acórdão n.º 461/2011), quer com a jurisprudência do TEDH relativa aos direitos ao silêncio e à não autoincriminação, entendidos como dimensão do direito ao processo equitativo e exigência da presunção de inocência [...]»²⁸⁶. Assim, o que se veda é apenas a interferência «no conteúdo essencial do direito à não autoincriminação: o direito ao silêncio sobre os factos que lhe sejam ou possam ser imputados a título de infração».²⁸⁷

quaisquer ilícitos (ou seja, de não terem de prestar declarações que por si só e independentemente de outros meios de prova e valorações sejam equivalentes à admissão da prática de uma infração), mas apenas devem fornecer as informações estritamente factuais que lhes forem pedidas e os documentos preexistentes referenciados pela AdC.» (MENDES, Paulo Sousa (2012), p. 312)

²⁸³ MENDES, Paulo Sousa (2018), p. 460.

²⁸⁴ «[Q]uando já está em curso um processo de contra-ordenação, deve entender-se, em minha opinião, que cessa parcialmente o dever de colaboração do arguido relativamente aos factos que o possam responsabilizar, passando a ter direito ao silêncio (isto é, a não prestar declarações sobre os factos que o podem responsabilizar), por aplicação subsidiária das regras do processo penal. [...] O arguido tem direito ao silêncio relativamente a factos que o podem responsabilizar, mas já não pode ocultar ou dissipar factos ou elementos relativos a outras pessoas ou relativamente à entidade colectiva a que pertence [...]» (PINTO, Frederico Costa (2009), p. 95)

²⁸⁵ Acórdão do TJUE de 18.10.1989, disponível em <https://eur-lex.europa.eu>.

²⁸⁶ O TC acrescenta que «a colaboração com a Autoridade tributária exigida aos contribuintes, à semelhança do que sucede relativamente a entidades reguladoras como a Autoridade da Concorrência ou a Comissão do Mercado de Valores Mobiliários, é imprescindível para viabilizar o exercício da função fiscalizadora que àquela se encontra legalmente cometida.» (acórdão do TC, proferido no processo n.º 298/2019, em 15.05.2019, disponível em <http://www.tribunalconstitucional.pt>)

²⁸⁷ Acórdão do TC, proferido no processo n.º 298/2019, em 15.05.2019, disponível em <http://www.tribunalconstitucional.pt>). Também o TRE explanou que «[o] cumprimento do dever de prestar informações completas e verdadeiras ao Banco de Portugal, sob pena de prática da contraordenação prevista e punível pelo artigo 211.º do Regime Geral das Instituições de Crédito e Sociedades Financeiras, não viola o direito à não autoincriminação ou o direito ao silêncio da ora arguida» (acórdão proferido no processo n.º 35/12.0YQSTR.E1, em 07.11.2013, disponível em <http://www.dgsi.pt>).

Salvo melhor opinião, aderimos aos argumentos expendidos pela terceira tese²⁸⁸. De facto, no confronto entre os deveres de colaboração impostos ao supervisionado e o direito ao silêncio e à não autoinculpação, parece-nos que o núcleo essencial deste último reside no direito que assiste ao arguido de não declarar sobre os factos, em moldes que tal conduta possa representar a sua autoinculpação. Mas já não lhe confere o direito de recusar a entrega de documentos (existentes à data do pedido) que se encontrem na sua posse, mesmo que os mesmos possam vir a servir de meio de prova para fundar a responsabilidade contraordenacional do arguido. Esclarecido este ponto, importa transpô-lo para o caso que nos ocupa.

4.3. O dever de entrega, por referência ao conteúdo da mensagem de correio eletrónico; e o tratamento de declarações autoinculpatórias

O conteúdo da mensagem pode assumir múltiplas configurações: a mensagem tanto pode conter, designadamente, informações ou ficheiros inócuos, do ponto de vista do preenchimento do tipo de um determinado ilícito contraordenacional, como pode, ao invés, conter informações ou ficheiros suscetíveis de fundar a responsabilidade contraordenacional da pessoa sujeita ao dever de colaboração. As situações descritas não levantam, a nosso ver, problemas em termos da sua transferência para o processo contraordenacional²⁸⁹. Sendo a instituição arguida notificada para entregar tais mensagens de correio eletrónico, deve entregá-las, pois o que o direito ao silêncio permite é que «o arguido não preste declarações quando inquirido no âmbito de um processo de contra-ordenação, ou seja, que não responda a perguntas que lhe são dirigidas, mas não se aplica fora do processo e não permite que o arguido frustre a execução de diligências de prova com a recusa de entrega de elementos»²⁹⁰.

²⁸⁸ Em sentido coincidente, MENDES, Paulo Sousa (2009), p. 28, PALMA, Maria Fernanda (2009), pp. 1 e 2 e, mais recentemente, SANTOS, Filipe Matias (2020), p. 497.

²⁸⁹ No sentido de questões autonomizáveis das acima tratadas.

²⁹⁰ PINTO, Frederico Costa (2009), p. 96.

Porém, pode também suceder que o conteúdo da mensagem de correio eletrónico configure ele próprio, materialmente, uma declaração autoinculpatória, para a pessoa legalmente obrigada ao dever de colaboração. Um exemplo académico seria, por hipótese, um determinado titular do órgão de administração da instituição declarar, numa mensagem de correio eletrónico, o seguinte: «De facto, a informação que prestámos ao BdP estava, deliberadamente, incompleta» (alínea *p*) do n.º 1 do artigo 211.º do RGICSF). Neste ponto, concordamos com CATARINA ANASTÁCIO quando refere que «[a] única forma possível de [...] salvaguardar simultaneamente o núcleo essencial da prerrogativa de não auto-incriminação e o efeito útil daqueles deveres de colaboração consiste em limitar o conceito de “declarações auto-incriminatórias” àquelas declarações que, por si só, isoladamente (isto é, independentemente de outras provas) e sem valorações (ou seja, sem margem para interpretações sobre o seu significado) sejam equivalentes à admissão da participação na infração e como tal sejam suficientes para a prova da infração»²⁹¹.

Ora, no exemplo dado, parece-nos que a declaração contida na mensagem equivale à admissão da infração²⁹², podendo a mesma ser suficiente para demonstrar a prática da infração – admitindo que, no caso, é possível demonstrar que a informação foi prestada de modo incompleta. Assim, entendemos que face a uma declaração com este teor, o arguido poderia legitimamente invocar o direito ao silêncio e à não autoinculpação, recusando-se a entregar aquele concreto documento²⁹³.

Naturalmente que o que acaba de se explanar não vale para quaisquer documentos que possam, em abstrato, fundar a responsabilidade contraordenacional do arguido. Conforme referimos acima, aquela prerrogativa diz apenas respeito àqueles documentos, muito específicos – e acrescentamos, por razões óbvias, de existência

²⁹¹ ANASTÁCIO, Catarina (2010), pp. 223 e 224.

²⁹² Se não totalmente, pelo menos em parte, na medida em que sempre caberia ao BdP alegar e provar que a informação prestada é efetivamente incompleta.

²⁹³ Mas entendemos que não pode limitar-se a não responder. Deve, ao abrigo do dever de colaboração, responder e explicar que não procederá à entrega de um determinado documento, na medida em que o mesmo contém uma declaração autoinculpatória.

excecional – que contenham declarações autoinculpatórias equivalentes àquelas que seriam prestadas na pendência de um processo contraordenacional se o arguido, quando interrogado sobre os factos, tivesse de responder e de responder com verdade, autoinculpando-se²⁹⁴.

Adicionalmente, pode também suceder que a mensagem de correio eletrónico que se encontre na posse da IC não contenha uma declaração autoinculpatória, na perspetiva da instituição, passamos a redundância, mas antes na perspetiva de um terceiro, alheio ao dever de colaboração. Neste caso, parece-nos que, uma vez que o direito ao silêncio e à não autoinculpação diz respeito «a factos que [...] podem responsabilizar [o arguido, este] não pode ocultar ou dissipar factos ou elementos relativos a outras pessoas [...]»²⁹⁵.

Em suma, na generalidade dos casos, quando tal seja solicitado pelo BdP, parece-nos que a IC sujeita aos deveres de colaboração com aquela entidade, tem o dever de entregar as mensagens de correio eletrónico que tenham sido recolhidas e impressas no âmbito de uma investigação interna. A sua validade está, no entanto, dependente do cumprimento, pela instituição, das diretrizes indicadas no Capítulo II do presente trabalho.

5. Das proibições de prova

Por último, importa ainda fazer uma breve referência ao problema que decorre da possibilidade de a IC, no decurso de uma investigação interna, não ter observado as diretrizes estabelecidas no Capítulo II do presente trabalho e, assim, ter,

²⁹⁴ «Ir mais longe do que isto, considerando que é auto-incriminatória qualquer declaração que possa ser usada como meio de prova, dessa forma contribuindo para a condenação do arguido, não nos parece compatível com o dever de colaboração que àquele cabe ao abrigo dos dispositivos legais já referidos.» (ANASTÁCIO, Catarina (2010), p. 223)

²⁹⁵ PINTO, Frederico Costa (2009), p. 96.

designadamente²⁹⁶, recolhido mensagens de correio eletrónico de natureza pessoal, sem o consentimento do colaborador²⁹⁷.

Neste caso, parece-nos ter plena aplicação o disposto no n.º 3 do artigo 126.º do CPP²⁹⁸, *ex vi* artigo 41.º, n.º 1, do RGCO, *ex vi* artigo 232.º do RGICSF^{299/300}. Assim, as provas que tenham sido obtidas, pela instituição, em violação das diretrizes mencionadas no Capítulo II do presente trabalho são nulas, não podendo ser utilizadas. Não podendo ser utilizadas na investigação interna, não podem, também, ser utilizadas no próprio processo contraordenacional.

Nesta configuração denota-se o verdadeiro impacto da “privatização da justiça”: a investigação interna, enquanto meio de obtenção de prova no domínio de uma entidade privada, está umbilicalmente ligada ao meio de obtenção de prova previsto no artigo 215.º, n.º 3, do RGICSF. Nessa medida, as invalidades cometidas na investigação interna, que passem despercebidas ao BdP, podem afetar o processo contraordenacional³⁰¹.

Estas circunstâncias impõem especiais cautelas ao BdP, na medida em que, na prática, este tem o ónus de verificar em que condições as mensagens de correio eletrónico foram recolhidas. Se nas mensagens de natureza profissional tal ónus está, de certa

²⁹⁶ Damos este exemplo, por ser, talvez, aquele que, à luz do nosso capítulo II, se afigurou como aquele que poderia assumir uma ocorrência mais frequente ou comum.

²⁹⁷ Seja porque este, confrontado com a intenção de recolha, não consentiu com a mesma, seja porque nem sequer lhe foi dada essa oportunidade, tendo a recolha ocorrido sem o seu conhecimento.

²⁹⁸ Segundo o qual «[r]essalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular».

²⁹⁹ Resultando também do n.º 8 do artigo 32.º da CRP.

³⁰⁰ «Do mesmo vício padece a apreensão de correspondência, face à proibição legal de apreensão de correspondência a que já fizemos referência (artigo 126.º, n.º 3 CPP) e ao preceito constitucional previsto no n.º 8 do artigo 32.º: “São nulas todas as provas obtidas mediante (...), abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações” (nulidade esta sanável mediante consentimento).» – ANASTÁCIO, Gonçalo e ALFAFAR, Diana (2017), p. 346.

³⁰¹ Artigo 122.º, n.º 1, do CPP: «As nulidades tornam inválido o acto em que se verificaram, bem como os que dele dependerem e aquelas puderem afetar». Para uma análise detalhada sobre as consequências processuais das proibições de prova, *vide* ROSA, Luís Bértolo (2010), pp. 219 a 277.

forma facilitado, tratando-se de mensagens de natureza pessoal ou não exclusivamente profissionais, cuja recolha foi alegadamente consentida, podem suscitar-se dificuldades práticas adicionais. Um erro, doloso ou negligente, numa investigação, pode ter consequências na validade da prova, aquando da sua transferência para o BdP.

CONCLUSÃO

As investigações internas constituem um mecanismo de averiguação reativo, integrado no sistema de controlo interno, máxime na respetiva função de *compliance*. Visam apurar se determinada suspeita de risco de *compliance* se confirma, identificando as pessoas envolvidas, com o objetivo último de reagir e de mitigar as consequências potenciais ou reais daquele risco. A final, será produzido um relatório fundamentado que contém **(i)** a descrição dos factos, **(ii)** a descrição das diligências realizadas e dos elementos recolhidos, **(iii)** a qualificação jurídica dos factos e as respetivas consequências jurídicas, **(iv)** a descrição das medidas tomadas ou a tomar para corrigir eventuais deficiências no respetivo cumprimento, contendo uma (re)avaliação do sistema de controlo interno e a justificação para a não adoção de medidas.

A investigação contém uma necessária fase de recolha de elementos, com base nos quais o investigador formula as conclusões que irá verter no relatório. Fruto das tecnologias da informação e comunicação, as mensagens de correio eletrónico constituem um dos elementos que podem, em abstrato, ser recolhidos, sendo, no entanto, vedado ao investigador aceder ao conteúdo de mensagens de correio eletrónico de natureza pessoal ou extraprofissional, salvo consentimento do colaborador. Em todo o caso, o acesso deve ser feito na presença do colaborador – que intervenha como remetente ou destinatário da mensagem – ou na presença de alguém por este indicado (designadamente nas situações de ausência imprevista ou programada).

Ademais, considerando que, ao aceder ao conteúdo de determinada mensagem de correio eletrónico, estar-se-á a proceder ao tratamento de dados pessoais, a licitude do tratamento depende da verificação de um dos fundamentos previstos no n.º 1 do artigo 6.º do RGPD.

Face aos desequilíbrios de poder em contexto laboral, entendemos ser prudente que o fundamento do tratamento não assente no consentimento do titular dos dados previsto na alínea a), mas antes no fundamento de cumprimento de uma obrigação jurídica, previsto na alínea c).

A mensagem de correio eletrónico, que obedeça aos requisitos acima enunciados, pode ser recolhida pelo investigador.

Dito isto, a questão que se coloca consiste em saber se, e em que condições, podem as mensagens de correio eletrónico, recolhidas (e, muito provavelmente, impressas) no decurso da investigação, ser transferidas para um processo de contraordenação que se encontre em curso, com o intuito de nele valerem como meio de prova.

Ora, o legislador, ao conferir ao BdP o direito potestativo de exigir das IC a prestação de todos os esclarecimentos e informações, bem como a entrega de todos os documentos que se revelem necessários à instrução dos processos de contraordenação da sua competência, consagrou um verdadeiro meio de obtenção de prova. No que releva para efeitos do presente estudo, este pode ter lugar na sequência notificação especificamente dirigida ao arguido para, no prazo que lhe for conferido, entregar os documentos em causa.

Entendemos que a “transferência” de mensagens de correio eletrónico que tenham sido recolhidas no âmbito de uma investigação interna, nas condições descritas no Capítulo II, não constitui uma ingerência numa comunicação, na medida em que o conteúdo da mensagem recolhida (por conseguinte, necessariamente recebida, aberta e lida) não constitui já, em si mesmo, uma comunicação (merecendo, em todo o caso, a tutela legalmente conferida a qualquer documento privado).

No que se refere ao colaborador da instituição, enquanto interveniente da mensagem de correio eletrónico, admitindo que a sua recolha teve lugar nas condições descritas

no Capítulo II, não vislumbramos, em abstrato, quaisquer obstáculos à respetiva transferência para o processo contraordenacional.

Mesmo relativamente a terceiros que intervenham numa mensagem de correio eletrónico, parece-nos que a tutela conferida a terceiro (cliente), através do segredo bancário, cede em prol de valores protegidos como a estabilidade e a confiança no sistema financeiro, bem como o regular funcionamento da atividade bancária.

No confronto entre os deveres de colaboração impostos ao supervisionado e o direito ao silêncio e à não autoinculpação, parece-nos que o núcleo essencial deste último reside no direito que assiste ao arguido de não declarar sobre os factos, em moldes que tal conduta possa representar a sua autoinculpação. Mas já não lhe confere o direito de recusar a entrega de documentos (preexistentes) que se encontrem na sua posse, mesmo que os mesmos possam servir de meio de prova para fundar a responsabilidade contraordenacional do arguido.

Nesse sentido, ressalvadas as hipóteses em que a mensagem de correio eletrónico contenha declarações autoinculpatórias equivalentes àquelas que seriam prestadas pelo arguido na pendência de um processo contraordenacional, a mesma pode, desde que verificadas as condições descritas no Capítulo II do presente trabalho, ser “transferida” para o processo de contraordenação.

Por último, se a IC, no decurso de uma investigação interna, não tiver observado as diretrizes estabelecidas no Capítulo II do presente trabalho e, assim, tiver, designadamente, recolhido mensagens de correio eletrónico de natureza pessoal, sem o consentimento do colaborador, parece-nos que tem plena aplicação o disposto no n.º 3 do artigo 126.º do CPP, *ex vi* artigo 41.º, n.º 1, do RGCO, *ex vi* artigo 232.º do RGICSF. Consequentemente, as provas recolhidas em violação daquelas diretrizes são nulas, não podendo ser utilizadas.

BIBLIOGRAFIA

ABREU, Filipe Brum de (2008) - «Deveres de controlo interno dos intermediários financeiros ao abrigo da MIFID» in *Actualidad Jurídica Uría Menéndez* [Em linha], dir. de Mariano Magide Herrero, n.º 21, Madrid: Uría Menéndez Abogados, S.L.P., 2008, p. 86-89, [consult. 02 de março de 2020], disponível em WWW:

<https://www.uria.com/documentos/publicaciones/2116/documento/articuloUM.pdf?id=3123>

AYRES, Ian e BRAITHWAITE, John (1992) - *Responsive regulation: transcending the deregulation debate* [Em linha], New York Oxford: Oxford University Press, Inc., 1992 (ISBN 0-19-507070-4), [consult. 01 de outubro de 2020], disponível em WWW:

<http://johnbraithwaite.com/wp-content/uploads/2016/06/Responsive-Regulation-Transce.pdf>

ALBUQUERQUE, Paulo Pinto de (2011) - *Comentário do Regime Geral das Contra-Ordenações à luz da Constituição da República e da Convenção dos Direitos do Homem*, Lisboa: Universidade Católica Editora, 2011 (ISBN 978-972-54-0246-7)

ALBUQUERQUE, Paulo Pinto de (2018) - *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4.ª Edição, Lisboa: Universidade Católica Editora, 2018 (ISBN 978-972-5402-95-5)

ALFAFAR, Diana (2013) - «O dever de colaboração e o *nemo tenetur se ipsum accusare* no direito sancionatório da concorrência» in *Revista de Concorrência e*

Regulação, Autoridade da Concorrência, Ano III, n.º 11 e 12, Coimbra: Almedina, 2013, p. 307-318 (ISBN 978-110-00-5801-6)

ALMEIDA, Joana (2020) - «Investigações internas: ponderações e limites» *in Novos Estudos sobre Law Enforcement, Compliance e Direito Penal*, coord. científica de Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes, Coimbra: Almedina, 2020, p. 59-78 (ISBN 978-972-40-8451-0)

ALVES, Lurdes Dias (2020) – *Proteção de Dados Pessoais no Contexto Laboral – O Direito à Privacidade do Trabalhador*, Coimbra: Almedina, 2020 (ISBN 978-972-40-8581-4)

ANASTÁCIO, Catarina (2010) - «O dever de colaboração no âmbito dos processos de contra-ordenação por infracção às regras de defesa da concorrência e o princípio *nemo tenetur se ipsum accusare*» *in Revista de Concorrência e Regulação*, Autoridade da Concorrência, Ano I, n.º 1, Coimbra: Almedina, 2010, p. 199-236 (ISBN 978-972-40-4102-5)

ANASTÁCIO, Gonçalo e ALFAFAR, Diana (2017) - «Anotação ao artigo 20.º da Lei da Concorrência» *in Lei da Concorrência - Comentário Conimbricense*, coord. de Manuel Lopes Porto [et al.], Coimbra: Almedina, 2017, p.332-349 (ISBN 978-972-40-7192-3)

Asociación Española de Compliance – *White Paper on the Compliance function* [Em linha], 2017, [consult. 20 de dezembro de 2020], disponível em WWW: <https://www.asociacioncompliance.com/wp-content/uploads/2017/08/White-Paper-Compliance-ASCOM.pdf>

Autoridade da Concorrência - *Linhas de Orientação sobre a instrução de processos relativos à aplicação dos artigos 9.º, 11.º e 12.º da Lei n.º 19/2012, de*

8 de maio e dos artigos 101.º e 102.º do TFUE [Em linha], 2013, [consult. 23 de janeiro de 2021], disponível em WWW:

http://www.concorrencia.pt/vPT/Noticias_Eventos/Noticias/Paginas/LO_Instrucao_Processos2013.aspx

AZEVEDO, Sara (2016) - *O Governo Interno das Instituições de Crédito – Adequação, Funções de Controlo, Conduta e Cultura* [Em linha], Porto: [S.n.], 2016, Dissertação de mestrado, [consult. 02 de novembro de 2019], disponível em WWW:

https://repositorio.ucp.pt/bitstream/10400.14/21574/1/Diserta%C3%A7%C3%A3o%20Sara%20Azevedo_%20O%20Governo%20Interno%20das%20IC.pdf

Basel Committee on Banking Supervision - *Compliance and compliance function in Banks* [Em linha], 2005 [consult. 25 de janeiro de 2020], disponível em WWW:

<https://www.bis.org/publ/bcbs113.pdf>

BICKER, Eike, STEINLE, Christian e SKOUPIL, Christoph (2020) - «Principles and Guidelines for Internal Investigations in Germany» in *Global Investigations Review - Europe, Middle East and Africa Investigations Review 2020* [Em linha], 2020, [consult. 02 de outubro de 2020], disponível em WWW:

<https://globalinvestigationsreview.com/benchmarking/europe-middle-east-and-africa-investigations-review-2020/1227369/principles-and-guidelines-for-internal-investigations-in-germany>

BOLINA, Helena Magalhães (2013) - «O direito ao silêncio e o estatuto dos supervisionados no mercado de valores mobiliários» in *Revista de Concorrência e Regulação*, Autoridade da Concorrência, Ano III, n.º 11 e 12, Coimbra: Almedina, 2013, p. 307-318 (ISBN 978-110-00-5801-6)

BRITO, Teresa Quintela de (2018) - «Compliance, Cultura Corporativa e Culpa da Pessoa Jurídica» in *Estudos sobre Law Enforcement, Compliance e Direito Penal*, coord. científica de Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes, Coimbra: Almedina, 2018, p. 57-100 (ISBN 978-972-40-7362-0)

CANOTILHO, J. J. Gomes e MOREIRA, Vital (2007) - *Constituição da República Portuguesa Anotada, Volume I*, 4.^a Edição, Coimbra: Coimbra Editora, 2007 (ISBN 978-972-32-1462-8)

CARDOSO, Rui (2018) - «Apreensão de correio electrónico e registos de comunicações de natureza semelhante - artigo 17.º da Lei n.º 109/2009, de 15.IX.» in *Cibercriminalidade e Prova Digital - Jurisdição Penal e Processual Penal* [Em linha], Centro de Estudos Judiciários, Lisboa: Centro de Estudos Judiciários, 2018, p. 57-88 (ISBN 978-989-8908-17-9), [consult. 04 de janeiro de 2020], disponível em WWW:

http://www.cej.mj.pt/cej/recursos/ebooks/penal/eb_Ciber_PDigital2018.pdf.

CORDEIRO, António Menezes (2009) - *Tratado de Direito Civil Português, II, Direito das Obrigações, Tomo I*, Coimbra: Almedina, 2009 (ISBN 978-972-40-3936-7)

CUADRAS, Albert Estrada I e ANGLÍ, Mariona Llobet (2014) - «Derechos de los trabajadores y deberes del empresario: conflicto en las investigaciones empresariales internas» in *Revista Brasileira de Ciências Criminais*, coord. científica de Leandro Ayres França, Ano 22, n.º 108, Brasil: Thomson Reuters, 2014, p. 151-188 (ISSN 1415-5400)

DIAS, Augusto Silva e RAMOS, Vânia Costa (2009) - *O Direito à não auto-inculpação (nemo tenetur se ipsum accusare) no processo penal e contra-*

ordenacional português, Coimbra: Coimbra Editora, 2009 (ISBN 978-972-32-1718-6)

DIAS, Augusto Silva (2010) - «O direito à não auto-inculpação no âmbito das contra-ordenações do código dos valores mobiliários» in *Revista de Concorrência e Regulação*, Autoridade da Concorrência, Ano I, n.º 1, Coimbra: Almedina, 2010, p. 237-275 (ISBN 978-972-40-4102-5)

DIAS, Augusto Silva (2018) - *Direito das Contra-ordenações*, Coimbra: Almedina, 2018 (ISBN 978-972-40-7342-2)

DIAS, Jorge de Figueiredo e ANDRADE, Manuel Costa (2009) - «Poderes de Supervisão, Direito ao Silêncio e Provas Proibidas» in *Supervisão, Direito ao Silêncio e Legalidade da Prova*, Jorge Figueiredo Dias, Manuel Costa Andrade e Frederico Costa Pinto, Coimbra: Almedina, 2009, p. 11-56 (ISBN 978-972-40-3763-9)

DURO, Pedro (2015) – «Novos Rumos para o Compliance - o Efeito Espanhol» in *Destaque Penal, Contra-ordenações e Compliance* [Em linha], Campos Ferreira, Sá Carneiro & Associados, 2015, [consult. em 22 de novembro de 2019], disponível em WWW:

https://www.csassociados.pt/xms/files/v1/DESTAQUES/Destaque_pdl_Novos_rumos_para_o_Compliance_o_efeito_espanhol.pdf

EÇA, Catarina Salazar de (2017) – *Whistleblowing – Denúncias de Irregularidades* [Em linha], Universidade Católica Portuguesa, Escola de Lisboa, Faculdade de Direito, [consult. em 20.10.2020], disponível em WWW:

<https://repositorio.ucp.pt/bitstream/10400.14/28707/1/Disserta%C3%A7%C3%A3o%20de%20Mestrado%20-%20Whistleblowing%20-%20Catarina%20Salazar%20de%20E%C3%A7a.pdf>

FERNÁNDEZ, Raquel Montaner (2015) - «El *Criminal Compliance* desde la Perspectiva de La Delegación de Funciones» in *Estudios Penales Y Criminológicos* [Em linha], vol. XXXV, Espanha: Universidad de Santiago de Compostela, 2015, p 733-782 (ISSN 1137-7550), [consult. em 10 de novembro de 2019], disponível em WWW:

<https://revistas.usc.es/index.php/epc/article/view/2704/3188>

GERALDO, Tiago (2018) - «A responsabilidade penal do *compliance officer*: fundamentos e limites do dever de auto-vigilância empresarial» in *Estudos sobre Law Enforcement, Compliance e Direito Penal*, coord. científica de Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes, Coimbra: Almedina, 2018, p. 267-302 (ISBN 978-972-40-7362-0)

GOMES, Júlio Manuel Vieira (2007) - *Direito do Trabalho - Relações Individuais de Trabalho, Volume I*, Coimbra: Coimbra Editora, 2007 (ISBN 978-972-32-1482-6)

Governo de Portugal – *Estratégia Nacional de Combate à Corrupção 2020-2024* [Em linha], 2020, [consult. 23 de janeiro de 2021], disponível em WWW:

<https://www.portugal.gov.pt/pt/gc22/comunicacao/documento?i=estrategia-nacional-de-combate-a-corrupcao-2020-2024>

JESUS, Francisco Marcolino de (2019) - *Os Meios de Obtenção de Prova em Processo Penal*, 2.^a Edição, Coimbra: Almedina, 2019 (ISBN 978-972-40-5874-0)

JÚNIOR, Filipa Marques e MEDEIROS, João (2018) - «A elaboração de programas de *compliance*» in *Estudos sobre Law Enforcement, Compliance e Direito Penal*, coord. científica de Maria Fernanda Palma, Augusto Silva Dias

e Paulo de Sousa Mendes, Coimbra: Almedina, 2018, p. 123-148 (ISBN 978-972-40-7362-0)

LABAREDA, João (2014) – *Contributo para o Estudo do Sistema de Controlo e da Função de Cumprimento («compliance»)* [Em linha], Lisboa: Instituto dos Valores Mobiliários, 2014, [consult. 10 de novembro de 2019], disponível em WWW: <http://www.institutovaloresmobiliarios.pt/>

LIMA, Pires de e VARELA, Antunes (2010) - *Código Civil Anotado, Volume I*, 4.^a Edição (Reimp.), Coimbra: Coimbra Editora, 2010 (ISBN 978-972-32-0037-9)

NEVES, Rita Castanheira (2011) - *As Ingerências nas Comunicações Electrónicas em Processo Penal - Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra: Coimbra Editora, 2011 (ISBN 978-972-32-1942-5)

MARTIN, Adán Nieto (2015a) - «Investigaciones Internas» in *Manual de Cumplimento Penal en la Empresa*, dir. de Adán Nieto Martin, Valencia: Tirant lo Blanch, 2015, p. 231-270 (ISBN 978-849-08-6326-8)

MARTIN, Adán Nieto (2015b) - «Fundamento y estructura de los programas de cumplimiento normativo» in *Manual de Cumplimento Penal en la Empresa*, dir. de Adán Nieto Martin, Valencia: Tirant lo Blanch, 2015, p. 111-134 (ISBN 978-849-08-6326-8)

MARTINEZ, Pedro Romano [et al.] (2017) - *Código do Trabalho Anotado*, 11.^a Edição, Coimbra: Almedina, 2017 (ISBN 978-972-40-7086-5)

MARTINEZ, Veronica Root (2019) - «The Compliance Process» in *Indiana Law Journal Vol. 94:203* [Em linha], Estados Unidos da América: Notre Dame Law School, 2019 [consult. em 22 de janeiro de 2020], disponível em WWW: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3151893

MENDES, Paulo Sousa (2004) - «As proibições de Prova no Processo Penal» in *Jornadas de Direito Processual Penal e Direitos Fundamentais*. coord. científica de Maria Fernanda Palma, Coimbra: Almedina, 2004, p. 133-154 (ISBN 978-972-40-2217-8)

MENDES, Paulo Sousa (2009) - «O dever de colaboração e as garantias de defesa no processo sancionatório especial por práticas restritivas da concorrência» in *Julgar*, dir. de José Igreja de Matos, n.º 9, Coimbra: Coimbra Editora, 2009, p. 11-28 (ISBN 977-164-66-8509-8)

MENDES, Paulo Sousa (2013) - «O problema da utilização de elementos recolhidos em ações de supervisão como meios de prova em processo sancionatório» in *Revista de Concorrência e Regulação*, Autoridade da Concorrência, Ano III, n.º 11 e 12, Coimbra: Almedina, 2013, p. 307-318 (ISBN 978-110-00-5801-6)

MENDES, Paulo Sousa (2018) - «Law Enforcement & Compliance» in *Estudos sobre Law Enforcement, Compliance e Direito Penal*, coord. científica de Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes, Coimbra: Almedina, 2018, p. 11-20 (ISBN 978-972-40-7362-0)

MONTIEL, Juan Pablo (2013) - «Sentido y Alcance de Las Investigaciones Internas en la Empresa» in *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, dir. de Patricio Lazo, Vol. 40, n.º 1, Chile: Ediciones Universitarias de Valparaíso, 2013, p. 251-257 (ISSN 0718-6851)

MOREIRA, Teresa Coelho (2010) - «A privacidade dos trabalhadores e o controlo electrónico da utilização da internet», in *Questões Laborais*, Júlio Gomes, Francisco Liberal Fernandes e Jorge Leite, n.º 35/36, Coimbra: Coimbra Editora, 2010, p. 23-82 (ISSN 0872-8267)

MOUTINHO, José Lobo e DURO, Pedro (2017) - «Anotação ao artigo 18.º da Lei da Concorrência» in *Lei da Concorrência - Comentário Conimbricense*, coord. de Manuel Lopes Porto [et al.], Coimbra: Almedina, 2017, p.313-324 (ISBN 978-972-40-7192-3)

PALMA, Maria Fernanda (2009) - *O direito à não auto-incriminação* [Em linha], 2009, [consult. 01 de outubro de 2020], disponível em WWW:
<https://www.cmjornal.pt/opiniaao/detalhe/o-direito-a-nao-auto-incriminacao>

PENA, Ana María Neira (2015) - «Sherlock Holmes en el centro de trabajo: Las Investigaciones Internas Empresariales» in *Revista Derecho y Proceso Penal*, dir. de Fermín Morales Prats e Ángel Sanz Morán, n.º 37, Pamplona: Aranzadi, 2015, p. 49-89 (ISSN 1575-4022)

PEREIRA, Francisco Rodrigues (2018) – *O controlo das comunicações eletrónicas do trabalhador: Análise do Caso do TEDH – Bărbulescu c. Roménia, de 5 de setembro de 2017* [Em linha], Faculdade de Direito, Escola do Porto, 2018, [consult. em 20.08.2020], disponível em WWW:
https://repositorio.ucp.pt/bitstream/10400.14/28542/1/FranciscoPereira_Tese.pdf

PIMENTA, Paulo (2014) - *Processo Civil Declarativo*, Coimbra: Almedina, 2014 (ISBN 978-972-40-5726-2)

PINHEIRO, Alexandre Sousa [et al.] (2018) - *Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra: Almedina, 2018 (ISBN 978-972-40-7786-4)

PINTO, Frederico Costa (2009) - «Supervisão do Mercado, Legalidade da Prova e Direito de Defesa em Processo de Contra-ordenações» in *Supervisão, Direito ao Silêncio e Legalidade da Prova*, Jorge Figueiredo Dias, Manuel Costa Andrade e Frederico Costa Pinto, Coimbra: Almedina, 2009, p. 11-56 (ISBN 978-972-40-3763-9)

PIZARRO, Sebastião Nóbrega (2017) - *Manual de Compliance*, Vila Nova de Famalicão: Nova Causa Edições Jurídicas, 2017 (ISBN 978-989-85-1536-0)

RAMALHO, David Silva (2017) - *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Coimbra: Almedina, 2017 (ISBN 978-972-40-7000-1)

RAMALHO, Maria do Rosário Palma (2016) - *Tratado do Direito do Trabalho, Parte II – Situações Laborais Individuais*, 6.^a Edição, Coimbra: Almedina, 2016 (ISBN 978-972-40-6814-5)

RAMOS, Vânia Costa (2006) - «Corpus Juris 2000: imposição ao arguido de entrega de documentos para prova e nemo tenetur se ipsum accusare» in *Revista do Ministério Público*, Prop. Sindicato dos Magistrados do Ministério Público, ano 27, n.º 108, Lisboa: Sindicato dos Magistrados do Ministério Público, 2006, p. 125-149 (ISSN 0870-6107)

RODRIGUES, Benjamim Silva (2008) - *Das escutas telefónicas Tomo I - A monitorização dos Fluxos Informacionais e Comunicacionais*, 2.^a Edição, Coimbra: Coimbra Editora, 2008 (ISBN 978-989-95-7791-6)

ROSA, Luís Bértolo (2010) - «Consequências Processuais das Proibições de Prova» in *Revista Portuguesa de Ciência Criminal*, dir. de Jorge Figueiredo Dias, ano 20, Coimbra: Coimbra Editora, 2010, p. 219-277 (ISSN 0871-8563)

ROTSCH, Thomas (2012) - «Criminal Compliance» in *InDret Revista para el Análisis del Derecho* [Em linha], dir. de Jesús María Silva Sánchez, n.º 1, Barcelona: Universitat Pompeu Fabra, 2012 (ISSN: 1698-739X), [consult. 02 de março de 2020], disponível em WWW:

<https://indret.com/wp-content/themes/indret/pdf/876a.pdf>

SANTOS, Filipe Matias (2020) - «Compatibilização dos Deveres de Informação e Colaboração com o Princípio da Não Autoinculpação» in *Novos Estudos sobre Law Enforcement, Compliance e Direito Penal*, coord. científica de Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes, Coimbra: Almedina, 2020, p. 471-500 (ISBN 978-972-40-8451-0)

SILVA, Germano Marques da (2011) - *Curso de Processo Penal - Volume II*, Lisboa: Verbo, 2011 (ISBN 978-972-22-3043-8)

SILVEIRA, Luís Lingnau da (2011) - «A proteção de dados pessoais e a internet» in *A sociedade do conhecimento / Centro de Informação Europeia Jacques Delors - Europa: Novas Fronteiras*, Ministério dos Negócios Estrangeiros, Direção Geral dos Assuntos Europeus e Centro de Informação Europeia Jacques Delors, n.º 28/29, Parede: Princípa Editora, 2011, p. 139-143 (ISSN 0873-8068)

Technical Committee of the International Organization of Securities Commissions - *Compliance Function at Market Intermediaries - Final Report* [Em linha], 2006, [consult. 22 de janeiro de 2020], disponível em WWW:

<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD214.pdf>

U.S. Department of Justice Criminal Division - *Evaluation of Corporate Compliance Programs* [Em linha], 2020, [consult. 01 de outubro de 2020], disponível em WWW:

<https://www.justice.gov/criminal-fraud/page/file/937501/download>

ÍNDICE

DECLARAÇÃO	vii
RESUMO.....	viii
INTRODUÇÃO.....	1
CAPÍTULO I – DAS INVESTIGAÇÕES INTERNAS.....	3
1. Enquadramento.....	3
1.1. <i>Compliance</i>	4
1.2. Sistema de controlo interno	5
1.3. Função de <i>compliance</i>	9
1.4. Risco de <i>compliance</i>	13
2. As Investigações internas	15
2.1. Definição e objeto	15
2.2. Das modalidades das investigações internas.....	18
2.3. Da competência para iniciar, dirigir e realizar uma investigação.....	19
2.4. Das fases da investigação.....	22
2.4.1 Da abertura da investigação.....	22
2.4.2 Da recolha de elementos na investigação	26
2.4.3 Do relatório final e comunicação do resultado da investigação	26
CAPÍTULO II – DA RECOLHA DE ELEMENTOS NAS INVESTIGAÇÕES INTERNAS	28
1. Introdução.....	28
2. Das mensagens de correio eletrónico	32
2.1. Introdução	32
2.2. O conceito de mensagem de correio eletrónico	35
2.3. Excurso: a tutela dos direitos em causa constitucionalmente consagrados.....	36
2.3.1. A tutela do direito à privacidade.....	36
2.3.2. Direito à inviolabilidade das comunicações privadas	38

2.4.	Comandos normativos em matéria de mensagens de correio eletrónico, no contexto laboral.....	40
2.5.	Comandos normativos em matéria de mensagens de correio eletrónico, no contexto da Proteção de Dados.....	46
2.5.1.	Introdução	46
2.5.2.	A licitude do tratamento	49
i.	O consentimento: os pressupostos atinentes a um consentimento válido e eficaz	49
ii.	O cumprimento de uma obrigação jurídica pelo responsável pelo tratamento	54
2.5.3.	A finalidade do tratamento	55
i.	Finalidades determinadas	55
ii.	Finalidades explícitas	56
iii.	Finalidades legítimas	57
CAPÍTULO III – DA TRANSFERÊNCIA DO RELATÓRIO FINAL PARA O BANCO DE PORTUGAL.....		59
1.	Introdução.....	59
2.	O conteúdo e o alcance do dever de entrega previsto no n.º 3 do artigo 215.º do RGICSF.....	62
3.	Da entrega, ao Banco de Portugal, de mensagens de correio eletrónico recolhidas no decurso de uma investigação interna.....	63
3.1.	Da admissibilidade da recolha	63
3.2.	Na perspetiva do colaborador da instituição.....	69
3.3.	Na perspetiva de um terceiro que figure na mensagem de correio eletrónico	71
4.	O problema do direito ao silêncio e à não autoinculpação.....	74
4.1.	Introdução	74
4.2.	Fundamento e alcance do direito ao silêncio e à não autoinculpação ...	75
4.3.	O dever de entrega, por referência ao conteúdo da mensagem de correio eletrónico; e o tratamento de declarações autoinculpatórias	79

5. Das proibições de prova	81
CONCLUSÃO	84
BIBLIOGRAFIA	87