

O responsável pelo tratamento de dados (pessoais) gerados pelo *Whistleblowing*

PATRICK DE PITTA SIMÕES*

Resumo: Nas últimas décadas tem sido recorrente a divulgação pública de casos de erros graves, má administração, ilegalidades ou de corrupção. De modo a salvaguardar-se a proteção dos dados pessoais dos indivíduos envolvidos e a imagem das organizações a que pertencem, tem-se implementado por todo o mundo o *Whistleblowing*. O nosso país não é exceção, seja por existir previsão geral na Lei n.º 19/2008, de 21 de janeiro, e em leis setoriais (nomeadamente comercial, bancário-financeira, seguradora ou na área da saúde), seja pela Deliberação n.º 765/2009, de 21 de setembro (Linhas de Ética), da Comissão Nacional de Proteção de Dados. Não obstante, a União Europeia estabeleceu, através da Diretiva 2019/1937, de 23 de outubro, normas mínimas comuns para a proteção dos denunciadores de violações do direito da União. Este texto pretende fazer um sucinto enquadramento sobre o *Whistleblowing* nacional, indagando, à data, quem poderá ser responsável pelo tratamento de dados pessoais gerados pelo *Whistleblowing*.

Palavras-chave: *Divulgação pública, Whistleblowing, Portugal, Diretiva 2019/1937, responsável pelo tratamento de dados.*

* Investigador pelo Centro de Investigação e Desenvolvimento sobre Direito e Sociedade (CEDIS), Árbitro (área administrativa) e Formador Certificado. Doutorando em Direito e Segurança pela Nova *School of Law*, Mestre em Auditoria pelo Instituto Politécnico de Lisboa, Pós-graduado em áreas do Direito Público do Instituto de Ciências Jurídico-Políticas, Especialista em Direito Administrativo e Licenciado em Direito pela Universidade de Lisboa, Licenciado em Geografia e Planeamento Regional pela Universidade Nova de Lisboa. Este texto é uma adaptação, atualização e aditamento, de excertos de subcapítulos da dissertação de mestrado do autor (Os limites da Auditoria Interna – o perfil do Auditor e o *Whistleblowing*). Foi empregue o Novo Acordo Ortográfico, determinado pela Resolução n.º 8/2011 do Conselho de Ministros, publicada no Diário da República, 1.ª série, de 25 de janeiro de 2011, à exceção das transcrições de legislação ou textos anteriores àquele, ou de autores que não tenham aderido ao mesmo.

Abstract: During the last decades, the public disclosure of serious errors, illegalities, wrongdoings, or corruption cases, has been more frequent. To safeguard the protection of the personal data from those involved and the corporate image of organisations to which they belong, Whistleblowing has been implemented all over the world. Portugal is no exception, either because there is a general prediction in Law No. 19/2008, of 21 January, and in sectoral laws (namely commercial, banking-financial, insurance or in the area of health), or by Resolution No. 765 / 2009, of 21 September (Ethics Lines), of the National Data Protection Commission. Nevertheless, the European Union established, through Directive 2019/1937, of 23 October, common minimum standards for the protection of whistleblowers reporting violations of European Union law. This text aims to provide a framework of Whistleblowing, at the national level, and, considering its implementation has not yet been massively verified (which is indicated to happen), to boldly inquire, who may be the responsible for the processing of personal data generated by Whistleblowing.

Keywords: *Public disclosure, Whistleblowing, Portugal, Directive 2019/1937, responsible for handling reports.*

Enquadramento geral

Numa Sociedade de Risco¹ e informação (de *fake news*² e infodemia também), tem-se regularmente conhecimento, através de divulgações públicas, de casos suspeitos de malversação ou de corrupção e infrações conexas.

Como forma de mitigar o julgamento público e os danos reputacionais adjacentes incrementou-se, nos Estados Unidos da América (EUA), o *Whistleblowing* (canais específicos para a comunicação de irregularidades que permitem a proteção de denunciante), que por sua vez, através da influência dos seus mercados bolsistas, tem sido fomentado um pouco por todo o mundo.

Em Portugal, a Comissão do Mercado de Valores Mobiliários (CMVM), através da sua Recomendação 10-A, de novembro de 2005, designada por Comunicação de Irregularidades, incentivou as sociedades empresariais

¹ Como descrita e desenvolvida por BECK, Ulrick, *Sociedade de risco mundial: em busca da segurança perdida*, Edições 70 (Grupo Almedina), 2015.

² Tradução livre do autor: distorção da informação (realidade), notícias falsas, ou simplesmente, desinformação.

a adotarem uma política de comunicação de irregularidades que mencionasse os meios internos através dos quais as comunicações podiam ser feitas, bem como se identificasse as pessoas com legitimidade para aceitá-las.

Por sua vez, a União Europeia (UE) criou um grupo de trabalho, composto pelas Autoridades Nacionais de Proteção de Dados que, no seu Parecer n.º 1/2006, de 1 de fevereiro, referindo a sua falta de competência e as diferenças histórico-culturais e sociojurídicas de cada Estado-Membro, elaborou um parecer sobre a aplicabilidade do *Whistleblowing*, limitando-o a áreas económico-financeiras e excluindo o direito laboral e penal.

Posteriormente, através da Lei n.º 19/2008, de 21 de abril, o legislador nacional aprovou medidas de combate à corrupção que estabelecem garantias para os trabalhadores que denunciem o cometimento de infrações de que tiverem conhecimento no exercício das suas funções.

No art. 4.º desta Lei estabeleceram-se garantias que se aplicavam, inicialmente, aos trabalhadores da Administração Pública e de empresas do sector empresarial do Estado, e que a partir de 2015 foram alargadas para os trabalhadores do setor privado, com as alterações introduzidas pela Lei n.º 30/2015, de 24 de abril (que procedeu à trigésima quinta alteração ao Código Penal; sexta alteração à Lei n.º 34/87, de 16 de julho; primeira alteração à Lei n.º 20/2008, de 21 de abril; primeira alteração à Lei n.º 50/2007, de 31 de agosto; e primeira alteração à Lei n.º 19/2008, de 21 de abril, no sentido de dar cumprimento às recomendações dirigidas a Portugal em matéria de corrupção pelo Grupo de Estados do Conselho da Europa contra a Corrupção, pelas Nações Unidas e pela Organização para a Cooperação e Desenvolvimento Económico).

No encadeamento de políticas de *compliance*³ e do normativo *soft law*, a Comissão Nacional de Proteção de Dados (CNPd), em consequência do elevado número de notificações de tratamento de dados pessoais

³ Há quem lhe intitule política antifraude, linhas de alerta, comunicação de irregularidades ou canais de reporte. Para mais desenvolvimentos *vide* PITTA SIMÕES, Patrick, *Os limites da Auditoria Interna – O perfil do Auditor e o Whistleblowing*, dissertação de mestrado defendida no Instituto Superior de Contabilidade e Administração de Lisboa (ISCAL), 2017, p. 67. Disponível em: <<http://hdl.handle.net/10400.21/8921>>.

gerados pelas comunicações internas de atos de gestão financeira irregular⁴, deliberou princípios orientadores (Linhas de Ética – cf. designa a Deliberação n.º 765/2009, aprovada a 21 de setembro, de ora avante Deliberação) aplicáveis a este tipo de tratamento, de modo a salvaguardar a privacidade dos intervenientes.

Com a Deliberação, além da previsibilidade de garantias aos denunciantes, passa a haver regras sobre direitos e limites para o tratamento de dados pessoais com aquela finalidade.

Estabelecem-se limites específicos de âmbito objetivo (o sistema de denúncia restringe-se aos domínios dos controlos internos, da contabilidade, da auditoria, do crime bancário e financeiro e da luta contra a corrupção), subjetivo (apenas as pessoas relacionadas com os tais domínios, que pratiquem atos de gestão, podem ser alvo de denúncia), procedimental (a sua natureza deve ser subsidiária à atividade regular da entidade) e de autonomia da vontade (obrigatoriedade da denúncia só nos casos em que a lei penal e processual penal o determina).

Antes do Regulamento Geral de Proteção de Dados (RGPD), a CNPD tinha um poder de controlo prévio deste tipo de tratamento de dados, pelo que as organizações que queriam implementar um sistema de *Whistleblowing*, tinham de pedir autorização à CNPD para criarem o mecanismo (cf. alínea a) do n.º 1 do art. 28.º, *ex vi*, n.º 2 do art. 8.º da Lei n.º 67/98, de 26 de outubro).

Por último, face à grande influência dos mercados financeiros e bolsa de valores dos EUA, com o surgimento de mais *Leaks* (comunicação ou divulgação não autorizada de informação sensível – comprometedora) a envolverem organizações e cidadãos europeus⁵, com a maior sensibilização

⁴ Debatendo este tipo de denominação, REBELO DE SOUSA; Marcelo, e SALGADO DE MATOS, André, *Direito Administrativo Geral – Actividade Administrativa*, Tomo III, 2ª edição, Publicações Dom Quixote, 2010, p. 55, explicam que “[a] irregularidade [será] a consequência reservada pela ordem jurídica para os actos que padeçam de ilegalidades pouco graves [...] (...) insusceptíveis de afectar de forma essencial a produção de efeitos estáveis pelos actos viciados em causa (...)”. Prosseguem dizendo que poderão ser vícios competenciais e formais, mas nunca materiais ou funcionais.

⁵ Como, por exemplo, o *Luxemburgo Leaks* (*Lux Leaks*), em que se soube, em novembro de 2014, detalhes de operações secretas de grandes empresas multinacionais para evitar o pagamento de tributos.

social⁶ e consciencialização política, a UE publicou a 26 de novembro de 2019, no seu Jornal Oficial, a Diretiva 2019/1937, de 23 de outubro, do Parlamento Europeu e do Conselho, relativa à proteção das pessoas que denunciem violações do direito da União (Diretiva *Whistleblowing*, de ora em diante, designada apenas por Diretiva). Esta visa reforçar a aplicação do direito e das políticas da União em domínios específicos, estabelecendo normas mínimas comuns para um nível elevado de proteção dos denunciantes (cf. art. 1.º).

Com este texto traça-se, num primeiro momento um conceito amplo e complexo de *Whistleblowing* e *Whistleblower*, tal como é o assunto e podem ser os seus sujeitos, bem como se procurará, simplificar a sua dialética.

Num segundo momento, pensando na dificuldade que as organizações, públicas e privadas, terão na implementação efetiva do sistema de denúncias, abordar-se-á quem poderá ser responsável por este cumprimento normativo e, conseqüentemente, dos dados pessoais a tratar.

Em seguida, dar-se-á conta de algumas das características das entidades que pediram autorização à CNPD para a implementarem o *Whistleblowing*, tal como da existência deste em quatro das maiores empresas de auditoria. Refira-se que este texto reflete uma síntese do estudo, mais vasto, realizado para a defesa da dissertação de mestrado do autor, que aborda os limites da auditoria (interna).

Numa quarta fase enunciam-se deveres implícitos: aos cidadãos (ainda que numa ótica de providência de cautelas); aos intervenientes no procedimento e processo de *Whistleblowing* (duas componentes distintas), como destaque para o responsável pelo tratamento daquele (e as suas entidades); e aos Estados.

Por fim, tecem-se algumas considerações finais quanto aos desafios eminentes com que o legislador nacional se depara(rá), concluindo que há ainda questões cruciais por refletir e encontrar soluções.

⁶ Tais como a Movemos a Europa (*WeMoveEurope*) que organizou uma petição internacional para a existência de uma lei a nível da UE que protegesse os denunciantes; ou a *Transparency International* uma associação com várias filiais, entre elas, uma portuguesa que tem como missão deter a corrupção e promover a transparência, a responsabilidade e a integridade da sociedade.

1. O conceito de *Whistleblowing* e *Whistleblower*

O que será afinal, no espectro nacional, o *Whistleblowing*? A Deliberação diz-nos que é um sistema que se traduz na criação, nas empresas, de condições para a denúncia de comportamentos, fraudulentos ou irregulares, capazes de afetar seriamente a sua atividade. Estas condições são normalmente designadas por canais (de denúncia), comunicação ou reporte (de irregularidades).

Esse sistema, também designado alternadamente pela Deliberação de mecanismo ou dispositivo, tem como objetivo estabelecer direitos e deveres laborais para os denunciantes, denunciados e indiretamente para os responsáveis pelo tratamento das denúncias que, em última instância, são os mais interessados na descoberta e/ou apuramento de factos, que muito provavelmente de outro modo não iriam saber.

O enquadramento de aplicação da Diretiva é bastante claro: informações sobre violações em contexto profissional [este é definido na alínea 9) do art. 5.º da Diretiva].

Os responsáveis pelo tratamento das denúncias estão incumbidos da receção e seguimento: análise, decisão e conservação daquelas, se for caso disso. O seguimento é definido na alínea 12) do art. 5.º da Diretiva, que se passa a transcrever: “qualquer medida tomada por quem recebe uma denúncia ou por uma autoridade competente, para aferir da exatidão das alegações constantes da denúncia e, se for caso disso, para resolver a violação denunciada, inclusive através de medidas como um inquérito interno, uma investigação, a ação penal, uma medida de recuperação de fundos ou o arquivamento”.

Deste modo, podemos, desde já, perceber que o responsável pelo tratamento é também responsável pelo seguimento da denúncia. Assim sendo, pode ser denominado como responsável pelo seguimento da comunicação da informação sobre violações [que, por seu turno, está definida na alínea 2) do art. 5.º da Diretiva].

Tenha-se em conta que o considerando 57 enuncia que o seguimento poderá incluir, por exemplo, o encaminhamento para outros canais ou procedimentos no caso de denúncias que afetam exclusivamente os direitos individuais do denunciante, o arquivamento por insuficiência de elementos de prova ou por outros motivos, a abertura de um inquérito interno e, eventualmente, as conclusões deste e as eventuais medidas

tomadas para resolver o problema identificado, o encaminhamento para uma autoridade competente para investigação mais aprofundada, na medida em que essas informações não prejudiquem o inquérito interno ou a investigação, nem afetem os direitos da pessoa visada. Deverá ser possível solicitar ao denunciante que preste mais informações, no decurso da investigação, embora não deva ser obrigatório prestar essas informações (vide o considerando 66).

Da conjugação da Deliberação e da Diretiva, sem se abordar outros diplomas legais, tais como os mencionados na Diretiva, além de poder ser confundido com o ato ou a ação em si de denunciar (*blow the whistle*) ao abrigo de uma proteção legal, por *Whistleblowing* deve entender-se um sistema⁷ que possibilita, de forma voluntária e não obrigatória, a existência (ou suscetibilidade) de denúncias⁸ internas⁹, nas organizações públicas e privadas¹⁰, ou de denúncias externas, para as autoridades competentes¹¹ (incluindo em último recurso a divulgação pública)¹², de condutas¹³ irregulares ou violações ao Direito¹⁴, num contexto

⁷ Conjunto de meios (vias possíveis de denunciar), tais como caixas físicas (simples de depósito ou correio postal), correio eletrónico (vulgo *email*), telefone ou outros sistemas de mensagem de voz e, a pedido do denunciante, reunião presencial (cf. considerando 53; n.º 2 do art. 9.º; n.º 2 do art. 12.º; alínea b) do art. 13.º ou art. 18.º da Diretiva). Em sistemas, que se crê poderem designar-se por *Whistleblowing* 2.0 (segunda geração), poderão ser concebidos formulários eletrónicos disponibilizados em *intranet* (dentro da organização) ou na *internet* (*online* – que permite o acesso a não trabalhadores), e por isso também acessíveis via telemóvel, ou ainda como uma opção de uma aplicação (vulgo *app*) de telemóvel inteligente (também conhecidos por *smart phone*).

⁸ Ou comunicações de informações, cf. alínea 3) do art. 5.º da Diretiva. Esta expressão tem uma conotação, político-cultural, mais neutra.

⁹ Preferencialmente (cf. n.º 2 do art. 7.º da Diretiva).

¹⁰ Com 50 ou mais trabalhadores, cf. se depreende do considerando 48 conjugado com o n.º 2 do art. 26.º, com a ressalva dos casos mencionados no considerando 50 da Diretiva.

¹¹ Cf. definido na alínea 14) do art. 5.º e com as competências prevista no art. 11.º da Diretiva.

¹² Cumpridos os pressupostos de tentativa de recurso aos meios internos e, ou, às autoridades competentes, cf. art. 15.º da Diretiva.

¹³ Comportamento por ação ou omissão, doloso ou negligente.

¹⁴ Cf. terminologia usada pela Deliberação, mas também por duas vezes referida na Diretiva, considerando 75 (denúncia de irregularidades) e 89 (denunciar irregularidades). Será discutível se a palavra irregularidades não quererá dizer na prática infrações (disciplinares, ainda que geradoras de uma simples admoestação ou repreensão escrita, ou mesmo

profissional¹⁵; assegurando o direito à defesa do denunciante¹⁶, de boa fé¹⁷ ou convicto de tal (na procura de um interesse coletivo da organização ou interesse público), de pessoas colaterais a este¹⁸ e do denunciado¹⁹; bem

contraordenacionais), ver-se-á o que prática, jurisprudência, dirá sobre este conceito, aparentemente, indeterminado. A palavra irregularidade é usada pela Deliberação, enquanto que a palavra violação é usada pela Diretiva, mas ambas convergem para o significado de atos ou procedimentos errados, incorretos, ilegais ou ilícitos. *Cum grano salis*, entende-se que, numa definição, fará sentido que as irregularidades ou violações sejam ao Direito (num todo) e não a domínios (específicos, ainda que mencionados) tanto na Deliberação, como na Diretiva. Havendo a possibilidade de cada Estado-Membro alargar os domínios de aplicação da Diretiva, que são mais amplos que os da Deliberação (cf. arts. 2.º e 3.º da Diretiva), bem como algumas matérias não serem afetadas pela Diretiva, não se considera prudente delimitar ou especificá-los numa definição.

¹⁵ Relação laboral ou relação comercial (quanto a esta vide, entre outros, o considerando 59 da Diretiva), ocasional ou duradoura; passada, presente ou futura (cf. se depreende do proémio do n.º 1, n.º 2 e proémio do n.º 3 do art. 4.º e, também, da alínea 9) do art. 5.º da Diretiva).

¹⁶ Interno ou externo, atual ou ex-colaborador da organização visada que é alvo de denúncia (a que pertence ou pertencia o denunciado, pessoa singular referida na denúncia como autora da violação ou que a esta esteja associada, cf. alínea 10) do art. 5.º da Diretiva – repare-se que nem a Deliberação, nem a Diretiva mencionam este aspeto temporal relativamente ao denunciado –, ou mesmo a pessoa coletiva, num todo, numa lógica de responsabilidade objetiva), que no decurso da sua atividade profissional ou por causa desta descobre irregularidades ou violações ao direito da União.

¹⁷ Tenha-se em conta que há diplomas legais da UE, relativos à segurança dos transportes que preveem também a proteção dos trabalhadores que denunciem erros por si cometidos de boa-fé contra atos de retaliação (“cultura justa”). Vide considerando 9 da Diretiva.

¹⁸ A Diretiva introduz “figuras jurídicas colaterais”, designadamente o facilitador (pessoa que auxilie – uma testemunha ou “coautor mitigado” – definido na alínea 8) do art. 5.º da Diretiva) ou o terceiro [tais como um colega ou um familiar do denunciante, cf. alínea b) do art. 4.º, ou testemunha, cf. considerando 76 e alínea a) do n.º 1 do art. 9.º da Diretiva] que sabe da denúncia por intermédio daquele ou sofre alguma represália (ato ou omissão), independentemente do seu grau de envolvimento na denúncia ou de conhecimento (o caso claro das entidades jurídicas – cf. identificadas na alínea c) do n. 4 do art. 4.º da Diretiva), por ter algum tipo de relação, pessoal ou profissional com o denunciante. Admitindo que haja prova testemunhal, com diferentes níveis de envolvimento (conhecimento) da testemunha com a denúncia, ou diversas fases em que possa intervir no *Whistleblowing*, não será tão clara a fronteira com as figuras de terceiro, de facilitador ou mesmo de denunciante em coautoría.

¹⁹ “Pessoa visada” que, cf. designado pela alínea 10) do art. 5.º, se define por ser: uma pessoa singular ou coletiva referida na denúncia, ou na divulgação pública, como autora da violação ou que a esta seja associada.

como estabelece regras²⁰ ao responsável pelo tratamento da denúncia, que não deverá ser o visado dos factos²¹, direta ou indiretamente, constantes na denúncia²².

De forma mais simples, o *Whistleblowing* é um conjunto de canais (interno e externo) de reporte ou comunicação (de informações ou de denúncias), que sinalizam ou alertam (chamam atenção) para irregularidades ou violações a regras²³ ou ao Direito da União Europeia (cf. art. 2.º da Diretiva) e de cada Estado-Membro, que pode ser diferente dos demais, cf. n.º 2 do art. 2.º e art. 3.º da Diretiva (*hard law*).

O *Whistleblowing* deve ser também encarado como um dispositivo instrumental (com canais internos e externos) e procedimental (de direitos, deveres e garantias). É no fundo um conjunto de meios técnicos (tendencialmente eletrónicos e informatizados) e jurídicos, proporcionados num ambiente profissional, que devem visar a proteção dos seus intervenientes (denunciante, denunciado e também pessoal responsável pelo tratamento da denúncia, tais como a confidencialidade e um procedimento e processo equitativo e justo – entende-se, como melhor se verá no capítulo 4, que procedimento e processo serão duas fases distintas do sistema de *Whistleblowing*).

E quem será afinal *Whistleblower*? Curiosamente a Diretiva na sua redação em inglês apenas refere esta palavra nos seus considerandos, usando a expressão *reporting person* para aquilo que nós, na versão portuguesa, lemos na alínea 7) do art. 5.º: denunciante.

²⁰ Processuais (nomeadamente, imparcialidade, justiça e rigor) e procedimentais (designadamente, prazos de retorno de informação e de conservação).

²¹ Reais (passados ou presentes) ou potenciais, cf. alínea 2) do art. 5.º da Diretiva.

²² De acordo com alínea 3) do art. 5.º da Diretiva, entende-se por denúncia ou comunicação de informações, denunciar ou comunicar informações: a comunicação verbal ou escrita de informações sobre violações. Os ingleses utilizam a palavra *report*, os espanhóis, *denuncia* ou *denunciar*; os franceses *signalement* ou *signaler*; os italianos *segnalazione* ou *segnalare*; e os romenos *raportare* (cf. alínea 3) do art. 5.º da Diretiva, em cada respetivo idioma). Daqui se observa que não é uniforme a utilização de uma palavra, se se fizer uma tradução, *ipsis verbis*, de cada língua para o português (e destas, se excluirmos o inglês, a família linguística românica, também conhecida por línguas latinas).

²³ Diretrizes (*guidelines*), linhas gerais, linhas estratégicas, padrões ou estruturas de enquadramento (*framework*), melhores práticas do setor (guias de boas práticas) ou, ainda, códigos de conduta. Todos estes instrumentos normativos fazem parte de um leque de autorregulação (*soft law*) que tem sido usado pelas organizações.

Dito isto, recorrendo à definição incita nesta alínea, denunciante é uma pessoa singular que comunica ou divulga publicamente informações sobre violações obtidas no âmbito das suas atividades profissionais.

Podem ser denunciantes: funcionários públicos²⁴, não assalariados, titulares de participações sociais e pessoas pertencentes a órgãos de administração, de gestão ou de supervisão de empresas (incluindo membros não executivos), assim como voluntários e estagiários, remunerados ou não remunerados, ou quaisquer pessoas que trabalhem sob a supervisão e a direção de contratantes, subcontratantes e fornecedores (cf. n.º 1 do art. 4.º, que deve ser conjugado com os arts. 45.º, relativo à circulação de trabalhadores, e 49.º referente à liberdade de estabelecimento, do Tratado de Funcionamento da UE, bem como o capítulo VI – medidas de proteção – da referida Diretiva).

Assim, repara-se que os denunciantes podem denunciar a qualquer momento, antes, durante ou depois da relação profissional ter sido estabelecida, não estando previsto nenhum regime de caducidade ou prescrição para a comunicação (denúncia) ou divulgação da informação.

2. Quem pode ser responsável pelo tratamento do *Whistleblowing*?

Por mais informatizado e auto mecanizado que venha a ser o sistema de *Whistleblowing*, e por isso se defende que estamos já perante uma segunda geração face aos meios mais convencionais já mencionados, este dispositivo que visa garantir a integridade e transparência das entidades, carece que haja uma intervenção humana para organizar e decidir: o responsável pelo mecanismo.

Feito este enquadramento, normativo e conceptual, procurar-se-á agora identificar quem será o responsável pelo tratamento de dados pessoais gerados pelo *Whistleblowing*, isto é, quem deverá manusear e geri-lo.

Para o efeito, recorrer-se-á à Deliberação e à Diretiva do *Whistleblowing*, com algumas abordagens ao RGPD, dando por fim, no capítulo seguinte,

²⁴ Terminologia usada pelo art. 386.º do Código Penal português, mas que já não é usada na Lei Geral do Trabalho em Funções Públicas (LGTFP), aprovada pela Lei n.º 35/2014, de 20 de junho e as suas sucessivas alterações. A LGTFP utiliza, simplesmente, o termo trabalhador (em funções públicas). Não obstante, vide considerando 38 da Diretiva, que justifica a *ratio* da utilização da expressão funcionário público.

conta de como eram as entidades autorizadas pela CNPD a implementarem o *Whistleblowing* e como se organizavam, a este respeito, 4 das 5 maiores empresas de auditoria em Portugal.

Antes de mais, convém referir quais são os dados pessoais genericamente sujeitos a tratamento no decurso de uma denúncia em contexto profissional. A Deliberação refere que “(...) [c]onsiderando a finalidade do tratamento em apreço, mostram-se necessárias para o tratamento as seguintes categorias de dados: [i]dentidade e categoria profissional do denunciante; [i]dentidade e categoria profissional do denunciado; [i]dentidade e funções das pessoas que intervêm na recolha e no tratamento; [o]s factos denunciados passíveis de integrarem actividades consideradas suspeitas (...); [o]s elementos de facto recolhidos no âmbito da averiguação; [d]estino da denúncia (...)”.

A Diretiva não detalha como aquela, mas refere, no seu considerando 14, que o respeito pela privacidade e a proteção dos dados pessoais, que são consagrados como direitos fundamentais nos arts. 7.º e 8.º da Carta dos Direitos Fundamentais da UE, constituem por si só um dos domínios do âmbito material da Diretiva [previsto na subalínea x), da alínea a), do n.º 1, do art. 2.º, que deve ser conjugada com o ponto J da Parte I do Anexo, do qual destacamos a alínea ii) relativa à possibilidade de denunciar violações ao RGPD; vide ainda considerando 76, 83, 97, 105, 109, art. 13.º e 17.º da Diretiva].

Os Estados-Membros da UE devem assegurar que a identidade do denunciante não seja divulgada a ninguém, além do pessoal autorizado competente para receber as denúncias ou dar seguimento a estas, sem o consentimento explícito do denunciante. O mesmo se aplica a quaisquer outras informações que permitam deduzir, direta ou indiretamente, a identidade do denunciante (cf. n.º 1 do art. 16.º da Diretiva).

A identidade do denunciante, e quaisquer outras informações que permitam identificá-lo, apenas podem ser divulgadas se tal for uma obrigação necessária e proporcional imposta pelo direito da UE ou nacional no contexto de uma investigação por autoridades nacionais ou de processos judiciais, inclusive com vista a salvaguardar os direitos de defesa da pessoa visada (cf. n.º 2 do art. 16.º da Diretiva).

A divulgação efetuada está sujeita a salvaguardas adequadas nos termos das regras da UE e nacionais. Em especial, os denunciantes devem ser informados antes da divulgação da sua identidade, salvo se tal informação

comprometer as investigações ou processos judiciais relacionados. Ao informar os denunciante, a autoridade competente deve enviar-lhes uma comunicação por escrito explicando os motivos da divulgação dos dados confidenciais em causa (cf. n.º 3 do art. 16.º da Diretiva).

Recorrendo à definição de dados pessoais do RGPD, ficamos a saber que estes são a informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)²⁵, isto é, para a análise em apreço, qualquer informação que identifique as pessoas intervenientes numa situação concreta de *Whistleblowing*.

Como já se referiu, a Deliberação estabeleceu direitos para o denunciante²⁶ e para o denunciado²⁷, bem como limites de âmbito subjetivo²⁸, procedimental²⁹, de autonomia da vontade³⁰ e específicos quanto à entidade responsável pela apreciação das denúncias³¹.

²⁵ 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 (cf alínea 1) do art. 4.º do RGPD).

²⁶ Nomeadamente informação sobre a identidade da entidade responsável; a finalidade prosseguida; os domínios abrangidos pela denúncia; o carácter facultativo do dispositivo; a inexistência de consequência pela não utilização do dispositivo; os destinatários da denúncia, a eventual transferência de dados para Estado exterior à UE; a existência de um direito de acesso e de retificação por parte das pessoas identificadas; e a não divulgação da sua identidade ao denunciado.

²⁷ Designadamente, informação sobre a identidade da entidade responsável; os factos denunciados; a finalidade do tratamento; o direito de acesso aos seus dados pessoais; o direito de requerer a retificação ou supressão dos dados se forem inexatos, incompletos ou equívocos; a confidencialidade no tratamento dos dados que lhe respeitem; a defesa do seu bom nome e privacidade; e o direito de apresentar queixa crime de denúncia caluniosa, nos termos previstos e punidos no Código Penal.

²⁸ Quem pode ser alvo de denúncia.

²⁹ O *Whistleblowing* deve ser um mecanismo complementar da atividade regular das organizações.

³⁰ Deve defender-se um regime de voluntariedade, limitado apenas pela obrigatoriedade de denúncia nos casos em que a lei penal e processual penal determine.

³¹ “(...) [A] gestão e a apreciação preliminar das denúncias apresentadas deve ser adstrita a entidades de auditoria, independentes (...)”. Repare-se que podemos entender o responsável pelo tratamento das denúncias, como um gestor das denúncias.

Circunscreveu ainda que não se afigura adequado “o estabelecimento de uma linha de denúncia interna, cuja gestão e apreciação compete aos eventuais denunciados”. Estes podem ser “(...) pessoas que pratiquem atos de gestão relacionados com os domínios da contabilidade, dos controlos contabilísticos internos, da auditoria, da luta contra a corrupção e do crime bancário e financeiro (...)” – cf. os limites de âmbito subjetivo que prevê.

Tal gerava a dúvida de saber se o *Whistleblowing* poderia ser praticado pelo auditor (no sentido de serem denunciantes ou denunciados) que, simultaneamente, pode ser o responsável pela apreciação das denúncias. Nesse sentido, indagou-se respostas através do recurso a literatura estrangeira, mormente, anglo-saxónica, decompondo os conceitos *Whistleblower* (e as suas classificações: interno e externo) e denúncia (e os seus tipos: interna e externa, identificada ou anónima, autorizada e não autorizada), chegando-se à conclusão que não se poderá excluir a possibilidade de os auditores serem responsáveis pela apreciação das denúncias³², sem prejuízo de também poderem ser denunciantes ou denunciados (desde que não assumam, cumulativamente, dois tipos de intervenção no procedimento e processo)³³.

De acordo com a Deliberação, nos termos da Lei n.º 67/98, de 26 de outubro, alterada pela retificação n.º 22/98, de 28 de novembro, Lei n.º 103/2015, de 24 de agosto, antiga Lei de Proteção de Dados Pessoais (LPDP), alínea d) do art. 3.º: “(...) o responsável pelo tratamento é ‘a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais’”.

A Deliberação, que deverá ser apreendida pela lei nacional que transpõe a *Directiva*, carece de adequação à lei de execução do RGPD (Lei n.º 58/2019, de 8 de agosto, também conhecida por – atual – LPDP) que,

³² Uma vez que a Deliberação diz que “(...) na linha do previsto no Código do Governo das Sociedades CMVM, a gestão e a apreciação preliminar das denúncias apresentadas deve ser adstrita a entidades de auditoria, independentes, às quais cumpre, entre outras funções, controlar o procedimento através do qual a sociedade cumpre as disposições em vigor no que diz respeito à possibilidade de os empregados notificarem irregularidades.”

³³ Para mais desenvolvimentos vide PITTA SIMÕES, Patrick, “O Whistleblowing em Portugal. Será que pode ser praticado pelo auditor?”, *Revisores & Auditores*, revista da Ordem dos Revisores Oficiais de Contas, edição 84, janeiro-março 2019, p. 20-31. Disponível em: <<http://hdl.handle.net/10400.21/11354>>.

por sua vez, deve ser conjugada com a Deliberação 2019/494, da CNPD, de 3 de setembro (referente à desaplicação de algumas normas da Lei de Execução do RGPD).

Ela esclarece que a entidade responsável deve ser individualmente responsável, só se admitindo a corresponsabilidade entre instituições em casos de absoluta impossibilidade de determinar individualmente a responsabilidade pelo tratamento.

De acordo com a mesma, o responsável será a sociedade que adote procedimentos internos e assegure meios que permitam a denúncia e a ulterior investigação de comportamentos contrários à lei ou às políticas da sociedade ou grupo de sociedades e decida, a final, sobre o destino a dar à denúncia apresentada.

Tenha-se em atenção que a Deliberação, não dizendo expressamente que se aplica ao setor privado, nada diz, *a contrario sensu*, que seja aplicável à Administração Pública. Pode presumir-se que não se previa a sua aplicabilidade por desnecessidade, uma vez que a Deliberação no seu enquadramento refere a Lei n.º 19/2008, de 21 de abril, que estabeleceu garantias aos denunciantes que sejam trabalhadores da Administração Pública e de empresas do sector empresarial do Estado. Todavia a sua aplicabilidade ao sector público não é tão clara como a Diretiva (vide prómio do n.º 1 do art. 4.º deste diploma legal).

Para a Deliberação, ao responsável pelo tratamento cumpre estabelecer as regras para implementar a comunicação e o tratamento das denúncias, com indicação das pessoas ou órgãos que no seio da sociedade ou do grupo de sociedades estejam especialmente encarregues da recolha e do tratamento das denúncias, as quais deverão ser em número limitado, com formação técnica adequada e adstritas ao dever de confidencialidade assumido contratualmente.

Estas entidades deverão pautar a sua actuação por princípios de independência e imparcialidade e pelo respeito pelos princípios vigentes no direito interno, em particular no Código do Trabalho e no Código do Processo Penal.

Numa interpretação literal do considerando 74, que pode ser conjugado com o n.º 5 do art. 12.º, somente as autoridades competentes (responsáveis pelos canais de denúncia externa – art. 10.º a 14.º da Diretiva) terão o dever de receber formação profissional, nomeadamente, sobre as normas aplicáveis em matéria de proteção de dados, para tratar das denúncias

e assegurar a comunicação com os respetivos denunciantes, bem como dar o seguimento adequado à denúncia.

No entanto, os responsáveis pelos canais de denúncia interna (art. 7.º a 9.º da Diretiva) também tem os mesmos deveres que os trabalhadores das autoridades competentes (vide considerando 73, 77, alínea 12) do art. 5.º ou arts. 16.º a 18.º da Diretiva), pelo que dever-se-á por isso ter em conta o elemento sistemático da interpretação do considerando.

Assim, faz-se uma interpretação sistemática da necessidade de formação, ainda que a título recomendatório, para todos responsáveis, públicos ou privados, pelo tratamento das denúncias, de canais externos e internos.

Mencione-se ainda que o considerando 59 da Diretiva, referindo-se a informações de esclarecimento que as entidades públicas e privadas que dispõem de procedimentos para a denúncia interna (*Whistleblowing*) devem prestar às pessoas para que ponderem denunciar; deverão incluí-las em cursos e seminários de formação sobre ética e integridade. Deste modo acredita-se que estas matérias estarão incluídas nas ações de formação para responsáveis pelo tratamento das denúncias (internas e externas – autoridades competentes).

Não obstante eventuais regimes de subcontratação, o responsável pelo tratamento está adstrito à verificação do cumprimento das medidas de segurança, sobre quem impende a obrigação legal e a salvaguarda das medidas adequadas.

A Deliberação especifica que medidas de segurança podem ser adotadas, tal como a Diretiva, ainda que esta de forma mais dispersa. Não se vai desenvolver neste texto estas, mas tenha-se presente que a Deliberação refere, a este propósito, que o “(...) responsável pelo tratamento tomará as precauções necessárias para preservar a segurança dos dados, quer na ocasião da recolha, quer na da sua comunicação ou conservação. Independentemente das medidas de segurança adoptadas pelo responsável pelo tratamento, é a este que cabe assegurar o resultado da efetiva segurança da informação.”

Se houver recurso a prestação de serviços para recolher ou tratar os dados, as pessoas especialmente encarregadas dessa missão, no seio do organismo prestador de serviços, só acedem aos dados dentro dos limites das suas competências (no caso de dados pessoais essa matéria é regulada no capítulo IV, mormente secção 1, do RGPD).

O prestador de serviços assume, por via contratual, a responsabilidade de não utilizar os dados para outros fins, assegurar a sua confidencialidade, respeitar o prazo de conservação e proceder à destruição ou à restituição de todos os suportes manuais ou informáticos dos dados pessoais no termo da sua prestação.

Não obstante as obrigações contratuais descritas, sempre haverá a realçar a obrigação de resultado que impende sobre o responsável pelo tratamento na salvaguarda da qualidade e da segurança dos dados³⁴.

A Deliberação esclarece ainda, relativamente à entidade responsável pela apreciação das denúncias, que ou esta entidade se encontra prevista na estrutura societária, sem prejuízo do exercício das funções descritas com independência e com salvaguarda da confidencialidade, não se verificando recurso à figura da subcontratação, aplicando-se-lhe o regime do responsável pelo tratamento; ou se verifica o recurso a entidade externa à estrutura societária, caso em que se aplica o regime de subcontratação.

Deste modo, se observa que a Deliberação permite que o auditor, interno ou externo, possa ser denunciado, como todo e qualquer trabalhador (ou se preferirmos colaborador)³⁵, e ser responsável por tratar as denúncias³⁶.

Independentemente da interpretação que se possa fazer da Deliberação, relativamente à natureza (interna ou externa) da entidade (de auditoria) responsável pela apreciação (tratamento) das denúncias, crê-se que as dúvidas quanto a esses profissionais (auditores) se dissiparam, no sentido que antecipadamente se indicou³⁷, com a publicação da Diretiva.

A Diretiva esclarece no considerando 54 que terceiros (fornecedores de plataformas de denúncias externas, consultores externos, auditores,

³⁴ Para uma reflexão complementar do exposto na Deliberação, vide MENEZES CORDEIRO, A. Barreto, *Direito da Proteção de Dados – à luz do RGPD e da Lei n.º 58/2019*, Edições Almedina, 2020, p. 307-317, 391-393.

³⁵ Não se desenvolverão as questões doutrinárias terminológicas tais como trabalhador, empregado ou funcionário. Parta-se do pressuposto que colaborador engloba todo o tipo de relação profissional.

³⁶ Não se olvide que um auditor subcontratado, apesar de ser externo à estrutura da organização, pode ser considerado interno se desempenhar tarefas de auditoria interna.

³⁷ Cf. PITTA SIMÕES, Patrick, *Os limites da Auditoria Interna – O perfil do Auditor e o Whistleblowing*, dissertação de mestrado defendida no ISCAL, 2017. Disponível em: <<http://hdl.handle.net/10400.21/8921>>.

representantes sindicais ou representantes dos trabalhadores) podem ser igualmente autorizados a receber denúncias em nome de entidades dos setores privado e público, desde que ofereçam as devidas garantias de independência, confidencialidade, proteção de dados e sigilo. Os canais de denúncia podem ser operados internamente por pessoas ou serviços designados para o efeito ou disponibilizados externamente por terceiros (cf. n.º 5 do art. 8.º da Diretiva).

Não obstante, igualmente, é possível que uma pessoa (responsável operacional)³⁸, serviço imparcial competente ou departamento, possa receber as denúncias e manter comunicação com o denunciante (dar retorno de informação)³⁹.

A escolha das pessoas ou dos departamentos de uma entidade do setor privado para receber e dar seguimento às denúncias varia em função da estrutura da entidade, mas, em qualquer caso, o desempenho da função deverá assegurar a independência e a ausência de conflitos de interesses. Nas pequenas entidades, aquela poderá corresponder a uma segunda tarefa de um empregado da empresa, bem posicionado para comunicar diretamente com o dirigente da organização, tais como o chefe do gabinete de conformidade (vulgo *Compliance Officer*), o responsável pelos recursos humanos, o responsável pela integridade, o responsável por questões jurídicas ou de privacidade, o diretor financeiro, o auditor-chefe ou um membro do conselho de administração (cf. considerando 56 da Diretiva).

Se se observar a sistemática da Diretiva, que diferencia denúncias internas de externas e ambas de divulgação pública, pode entender-se que existirão diferentes responsáveis pelo tratamento de denúncias internas (das entidades do setor privado e público) e externas (das autoridades competentes). Tenha-se em conta que a Deliberação nunca referiu a possibilidade de a divulgação pública poder ser protegida pelo sistema de *Whistleblowing*.

Ainda relacionado com o responsável pelo tratamento do *Whistleblowing*, como se tem vindo a mencionar, há que ter em conta a autoridade competente, ou seja, qualquer autoridade nacional designada para receber

³⁸ Cf. se extrai da parte final do n.º 5 do art. 8.º da Diretiva.

³⁹ Cf. alínea c) do n.º 1.º do art. 9.º da Diretiva.

denúncias externas e dar aos denunciantes retorno de informação⁴⁰ (seguimento)⁴¹; que é diferente da figura de responsável pelo tratamento da denúncia (interno).

Caberá aos Estados-Membros designar as autoridades competentes para receber e para dar o devido seguimento às denúncias. Estas poderão ser autoridades judiciais, organismos reguladores ou de supervisão competentes nos domínios específicos em causa, ou autoridades com competências mais gerais a nível central num Estado-Membro, autoridades de aplicação da lei, organismos de luta contra a corrupção ou provedores de justiça (cf. considerando 64 da Diretiva).

Como já defendido⁴², julga-se que fará sentido haver autoridades competentes por setores⁴³, com diferentes níveis de responsabilidade, cf. se depreende do considerando 77. Muito provavelmente, estas serão os Serviços de Inspeção Geral, Autoridades ou Entidades Reguladoras⁴⁴, a Comissão do Mercado de Valores Mobiliários, a CNPD, as Ordens Profissionais ou mesmo o Provedor de Justiça. Mencione-se que as instituições, órgãos ou organismo da União, são tidos como entidades externas à autoridade competente (que é sempre nacional) para efeitos de denúncia.

Por último, não se crê que o responsável pelo tratamento da denúncia, que será o responsável máximo pela organização e por isso o maior interessado na eficiência e eficácia do *Whistleblowing*, não delegue, sobretudo em organizações de significativa dimensão, competências de apreciação preliminar ou instrutória a um trabalhador, deixando para si apenas o poder de decisão final (vide considerando 55 e 56).

⁴⁰ Definida na alínea 13) do art. 5.º da Diretiva.

⁴¹ E, ou, designada para desempenhar as funções previstas na Diretiva (cf. definição prevista na alínea 14) do art. 5.º).

⁴² Em PITTA SIMÕES, Patrick, “O Whistleblowing é um caso de polícia(s)?”, in *Polícia(s) e Segurança Pública: História e Perspetivas Contemporâneas*. MUP – Museu da Polícia, p. 482-483.

⁴³ Por exemplo o considerando 21, referindo o art. 11.º da Diretiva 89/391/CEE do Conselho, de 12 de junho de 1989, refere a existência de uma Autoridade para a área de Saúde e Segurança no Trabalho.

⁴⁴ Algumas destas previstas no DL n.º 276/2007, de 31 de julho, alterado pelo DL n.º 32/2012, de 13 de fevereiro e pela Lei n.º 114/2017, de 29 de dezembro.

3. Da teoria ao *Whistleblowing* autorizado

Analisado o porquê de existir o *Whistleblowing*, o que é, e quem são os seus intervenientes, com destaque para quem pode ser responsável pelo seu tratamento, vejamos agora, da teoria à prática, quantas, de onde e como eram as entidades que foram autorizadas pela CNPD a implementá-lo em Portugal, e ainda quem era responsável pelo tratamento de dados gerados pelo *Whistleblowing* em 4 das 5 maiores empresas de auditoria, a que se chamou de “*Four Big Five*”⁴⁵.

Para o efeito, utiliza-se, com as devidas adaptações, o estudo efetuado aquando da realização da dissertação de mestrado em que se solicitou à CNPD o acesso à sua base de dados, de modo a analisar-se as informações disponibilizadas pelas instituições que a tivessem notificado para a autorização de um tratamento de dados pessoais, com a finalidade de gestão das comunicações internas de atos de gestão financeira irregular.

Entendeu-se que se devia pedir diretamente à Autoridade Nacional de Controlo de Dados Pessoais, legítima e competente para, à data (cf. arts. 27.º e 28.º da antiga LPDP), autorizar previamente a implementação do sistema de denúncias internas, daí que o nome escolhido para este capítulo seja: *Whistleblowing autorizado* (oficialmente declarado e em conformidade com a Deliberação)⁴⁶.

Mencione-se também que, honrando o compromisso, previamente assumido, com a CNPD e com todas as SROC que se interpelaram, independentemente de terem ou não colaborado, entendeu-se como uma legítima limitação de âmbito do estudo empírico realizado na dissertação, não se correlacionar as informações recolhidas junto daquela

⁴⁵ As quatro das cinco maiores empresas de Auditoria, que colaboraram no estudo empírico foram: a BDO & Associados, Sociedade de Revisores Oficiais de Contas (SROC), Lda.; a Deloitte & Associados, SROC S.A.; a Ernst & Young Audit & Associados, SROC, S.A. e a KPMG & Associados, SROC, S.A.

⁴⁶ Uma forma alternativa de identificarmos organizações que implementaram o *Whistleblowing*, seria analisar os relatórios de governo das sociedades, conjugados com regulamentos de comunicação de irregularidades das empresas que disponibilizassem os mesmos nos seus *websites*. Porém, correr-se-ia o risco de ser uma informação dispersa, não uniforme e de dificuldades acrescidas face à maior ou menor pública destas informações.

com a identificação destas, incluindo as respostas obtidas pelas “*Four Big Five*”.

Refira-se ainda que se ponderou apurar até que ponto o *Whistleblowing* se revela eficiente e, ou, (des)vantajoso e dispendioso⁴⁷; porém, para além dessa avaliação qualitativa que poderia ser encarada como uma intromissão na gestão de informação financeira e por isso um trabalho estéril; considerando, que o setor empresarial está saturado de inquéritos⁴⁸; achou-se que, numa relação de custo-benefício, não se seria tão produtivo e se afastaria do propósito da dissertação de mestrado.

Por fim, ressalva-se que, relativamente à data a que se reportam as autorizações analisadas, a base de dados eletrónica que foi facultada pela CNPD não permitia saber, *ab initio*, detalhes de todos os processos (autorizações solicitadas) por não estarem informatizados os anteriores ao ano de 2011, o que limitou o tratamento ou a profundidade de algumas questões tratadas.

Feita esta clarificação, balizou-se a amostra às 131 entidades a quem foi autorizado, de acordo com a Deliberação, o tratamento de dados⁴⁹, desde janeiro de 2011 até 31 de agosto de 2015⁵⁰. Assim, em termos evolutivos, cf. ilustra a figura 1, verificou-se que entre os anos civis completos de 2012 e 2014, houve uma tendência crescente de autorizações de *Whistleblowing*, o que pode ser indiciador de que este sistema foi sendo cada vez mais utilizado. Ideia reforçada pelos dados de 2015 que, apesar de serem referentes ao final do mês de agosto, portanto a pouco mais de metade do ano, já superavam as 19 autorizações atribuídas em 2012.

⁴⁷ Em abono da verdade, em grande parte o *Whistleblowing* é um assunto “melindroso” para que nos fosse facultado algumas informações, tais como quantas situações foram detetadas ao seu abrigo.

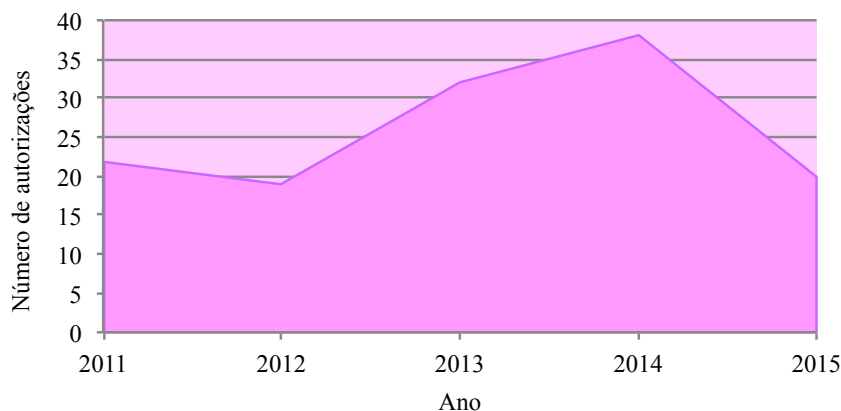
⁴⁸ Nomeadamente os que permitiriam aferir estatística e qualitativamente a eficácia e, ou, eficiência dos serviços.

⁴⁹ Alguns dos 174 processos identificados, distintos em número, eram referentes à mesma entidade. Seriam os casos em que a organização requerente tivesse mudado algum dos dados fornecidos no formulário de notificação geral, à data disponível no *website* da CNPD, e por isso deu origem a um novo número de processo, ou ainda nas situações em que inicialmente se arquivou o processo, por insuficiência de garantias ou inconformidade com a Deliberação, e depois foi reaberto com um outro número.

⁵⁰ Data a partir da qual as autorizações ficaram suspensas cf. se irá ver de seguida.

Possivelmente o número de autorizações seria maior se o austríaco *Maximilian Schrems* não tivesse movido, junto do Tribunal de Justiça Europeu, uma ação de reenvio prejudicial contra a *Data Protection Commissioner*, por não ter investigado a sua queixa contra a filial do *Facebook* na Irlanda (a *Digital Rights Ireland Ltd.*), em virtude de esta violar as leis de proteção de dados pessoais europeus.

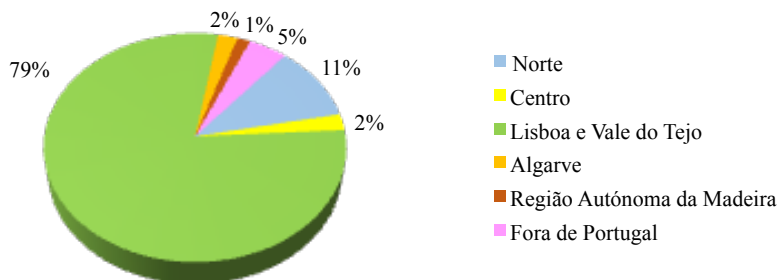
Figura 1 – Notificações autorizadas por ano.



Fonte: CNPD. Elaboração própria.

No que diz respeito à origem geográfica das entidades, observando a Figura 2, ficou-se a saber que a esmagadora maioria (79%, correspondente a 103 empresas), se localizava na região de Lisboa e Vale do Tejo, seguida da Região Norte (11%). As restantes regiões, juntas, apenas representavam 10%. Refira-se ainda que duas entidades que notificaram um tratamento de dados no âmbito das Linhas de Ética, eram da Região Autónoma da Madeira. Nenhuma das 131 entidades é da Região Autónoma dos Açores ou do Alentejo. Curiosamente, sete (5%) declaravam estar sediadas fora de Portugal.

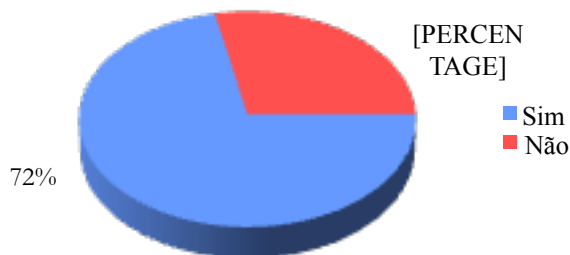
Figura 2 – Incidência geográfica do *Whistleblowing*, entre 2011 e meados de 2015, por Nomenclatura de Unidade Territoriais para Fins Estatísticos (NUT) II⁵¹.



Fonte: CNPD. Elaboração própria.

Destas empresas sabemos também, cf. a Figura 3, que a maioria (94), representando 72% do total, subcontratava uma entidade externa para tratar dos dados decorrentes das denúncias, garantindo assim a sua imparcialidade⁵², e apenas 28% não o fazia.

Figura 3 – Subcontratação do tratamento.



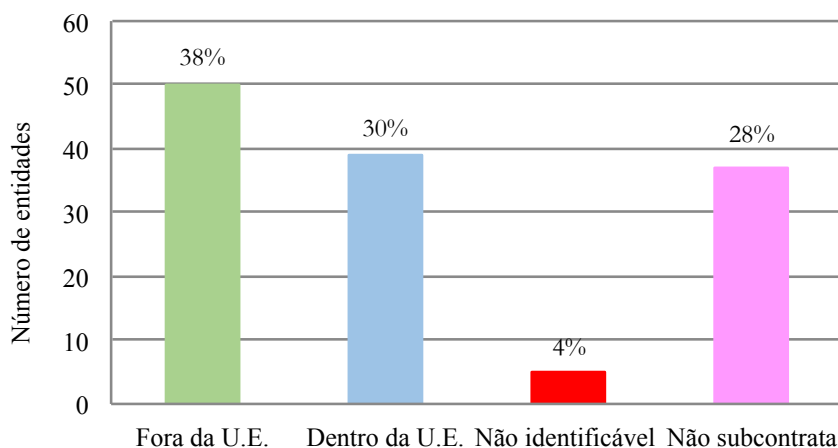
Fonte: CNPD. Elaboração própria.

⁵¹ Matrizes de delimitação geográfica, designadas por NUT, foram aprovadas pelo DL n.º 46/89, de 15 de fevereiro; alterado pelo DL n.º 163/99, de 13 de maio; pelo DL n.º 317/99, de 11 de agosto; pelo DL n.º 244/2002, de 5 de novembro; e pela Lei n.º 21/2010, de 23 de agosto.

⁵² O tratamento por subcontratante devia respeitar o disposto nos arts. 14.º e 16.º da antiga LPDP. Vide art. 28.º do RGPD.

Daquelas, 39 entidades subcontratavam empresas europeias e 50 subcontratavam empresas não europeias, concretamente dos EUA, conforme se ilustra na figura 4.

Figura 4 – Origem da entidade que processa.



Fonte: CNPD. Elaboração própria.

Esclareça-se que as empresas norte-americanas tinham de assegurar a melhor proteção possível dos dados pessoais (quando eram exportados), respeitando os normativos da UE, nomeadamente quando a transferência de dados pessoais era efetuada para fora da UE devia respeitar-se os arts. 19.º e 20.º da antiga LPDP⁵³.

A CNPD manifestou, através das suas autorizações (por exemplo a n.º 2717/2017, de 7 de março), que não estava em condições de decidir de forma definitiva sobre a transferência de dados pessoais para o território

⁵³ Vide art. 22.º da atual LPDP e arts. 44.º a 50.º do RGPD. Não se abordará as transferências de dados pessoais gerados pelo *Whistleblowing*, entre Estados-Membros e entre estes e um país terceiro, no entanto, retenha-se que se no primeiro caso o RGPD, aplicável diretamente, assegura um nível de proteção de dados adequado, no segundo caso é necessário ter a certeza que o país terceiro respeita requisitos de segurança.

dos EUA, uma vez que, por força do acórdão do Tribunal de Justiça da União de Europeia, de 6 de outubro de 2015, relativo ao processo C-362/14, já referido, foi declarada inválida a Decisão 2000/520/CE, da Comissão Europeia, de 26 de julho de 2000, que no seu anexo I estabelecia princípios internacionais de auto-certificação, que deveriam garantir que as entidades norte-americanas respeitavam a privacidade e a segurança das informações pessoais dos cidadãos da UE e Suíça, aquando de fluxos de dados transatlânticos designados por *Safe Harbor*.

Nestes termos, tendo a CNPD que proceder a uma análise aprofundada da legislação vigente nos EUA, com vista a apurar se aquela se sobrepunha, de modo desnecessário e desproporcionado, às cláusulas contratuais⁵⁴ adequadas que o responsável e os destinatários da informação subscreviam, apenas emitiu autorizações provisórias (cf. seu Comunicado de 23 de outubro de 2015).

Feita esta explanação e prosseguindo, da teoria à prática, interrogou-se as “*Four Big Five*” no sentido de saber se dispunham de algum sistema que se traduzia na criação de condições para a denúncia de comportamentos fraudulentos ou irregulares (*Whistleblowing*). Todas responderam que sim, exceto uma que não chamava de sistema de denúncias⁵⁵.

Neste último caso, em particular, existiam três áreas diferentes, não divididas por gabinetes, mas sim por sócios responsáveis: pela transparência, sistema interno de controlo da qualidade e ética. “Todas as pessoas [tinham] trimestralmente um conselheiro, exceto os sócios, a quem reporta[va]m todas as questões de análise de *performance*, funcionando como um canal de informação que sai[a] da hierarquia operacional. Qualquer questão relativa ao seu superior hierárquico pod[ia] ser reportada ao seu Conselheiro”.

Refira-se também que uma das SROC reportava que ajudavam “empresas a montar o sistema”. Porventura os auditores internos seriam os mais bem preparados para auxiliarem nesta tarefa.

⁵⁴ Cláusulas contratuais-tipo, contratos entre empresas do mesmo grupo – acordos intragrupo – ou outros contratos *ad-hoc*.

⁵⁵ Repita-se que as informações que ora se mencionam foram obtidas no âmbito da dissertação de mestrado, pelo que se desconhece se ainda se mantem os factos ou procedimentos relatados pelos entrevistados.

Em seguida, perguntou-se a quem ficava a carga a análise e a gestão do *Whistleblowing*. Começando pela entidade que tinha aquela particularidade, o Conselheiro podia ser um dos sócios ou um dos diretores, mas nunca seria o superior hierárquico direto do trabalhador. Ao Conselheiro competia perceber as situações em que o trabalhador entendia revelar o que não estava bem, ou se estava satisfeito com a sua hierarquia operacional. «O Conselheiro dev[ia] comunicar, em função da gravidade, aos sócios executivos (...)»

Outra das “*Four Big Five*”, respondeu que «[n]uma primeira fase [era] cometida ao Diretor de Ética (cargo desempenhado por um sócio), que far[ia] a triagem do assunto e reportar[ia] ao Diretor de Risco e Reputação (cargo também desempenhado por um sócio). Por sua vez, numa segunda fase, este direcionar[ia] a denúncia para outros Diretores, tais como o de Auditoria Interna ou de Independência».

Uma outra SROC inquirida replicou-nos, sucintamente, que quem analisava e fazia a gestão do *Whistleblowing* era a “empresa mãe” e outra específica”.

Por fim, uma quarta entidade afirmava ter “uma área independente da estrutura onde pod[ia] ser comunicada a situação” mencionando ser dever do órgão de fiscalização receber as irregularidades apresentadas por acionistas, colaboradores ou outros [cf. alínea j) do n.º 1 do art. 420.º e f) do n.º 1 do art. 422.º do CSC; se fosse o Fiscal Único ou o Conselho Fiscal; alínea j) do n.º 1 art. 423.º-F do CSC; se fosse a Comissão de Auditoria; ou alínea j) do n.º 1 do art. 441.º do CSC se fosse o Conselho Geral de Supervisão].

4. Responsabilidades intrínsecas ao *Whistleblowing*

Entende-se que esta temática mais do que interessar ao investigador ou à academia, deve interessar à sociedade de forma transversal, uma vez que qualquer pessoa pode ser envolvida num assunto de *Whistleblowing*, mesmo que não queira ou faça, no seu entender, algo passível de tal “enredo”.

Viu-se que os denunciantes podem denunciar a qualquer momento, desde que tenham alguma relação profissional com a entidade a quem reportam a irregularidade ou violação ao Direito; bem como o responsável pelo tratamento, de canais de denúncias internas e externas, é diferente

da autoridade competente, entidade externa que será responsável pelo canal de denúncias externo.

Considera-se que a lei que venha a transpor a Diretiva, deverá ter em conta que a Deliberação não foi revogada e as suas Linhas de Ética deverão estar em conformidade com o RGPD. O que parece não ser o caso da Lei de Execução do RGPD, atual LPDP, cf. Deliberação 2019/494, da CNPD, de 3 de setembro.

Para o gestor (ou responsável pelo tratamento) do *Whistleblowing*, as informações produzidas deverão ser protegidas por técnicas de codificação ou encriptação, o que as tornam logo *a priori* informações classificadas⁵⁶, ainda que devam ser entendidas como diferentes das mencionadas na alínea a) do n.º 3 do art. 3.º da Diretiva.

Haverá matérias cujo conteúdo será sensível e que carecem de ser vedadas a um “*Whistleblowing* mais amplo”, nesses casos o legislador europeu contemplou que a Diretiva não afeta a aplicação do direito nacional ou da União nesses temas.

Poder-se-á subdividir e classificar o *Whistleblowing* como procedimento, isto é, a sequência funcional de atos conducentes à identificação dos intervenientes e dos factos; e como processo, ou seja, o apuramento da veracidade dos factos e assunção do direito.

O primeiro impulso procedimental por parte de um denunciante será dar a conhecer a um responsável pelo tratamento da denúncia a informação que dispõe (preferencialmente suportada em evidências/provas). A tarefa do responsável pelo tratamento das denúncias inicia-se com a denúncia (informação que deve ficar documentada)⁵⁷, incide sobre a mesma (a que não estiver documentada não tem evidências de que foi efetuada) e finda com a elaboração e aprovação de um parecer, relatório ou decisão final (informação documentada). Ser responsável pelo tratamento das denúncias é ser também guardião da documentação produzida no âmbito do *Whistleblowing*.

O procedimento de denúncia tem sempre de ter uma iniciativa e apreciação preliminar, por sua vez o processo de denúncia terá de ter

⁵⁶ Por serem classificadas devem ser protegidas dessa forma. Estas informações podem englobar segredos comerciais, como diversas vezes referido na Diretiva (vide por exemplo o n.º 4 do art. 16.º).

⁵⁷ Vide art. 18.º da Diretiva.

uma instrução e uma decisão final, que poderá conter a formulação de recomendações pelo representante (máximo) legal da organização, responsável final pelo tratamento das denúncias.

Se houver uma separação de tarefas, o que se considera aconselhável, haverá um responsável pelo tratamento das denúncias (inicial) que fará um relatório ou parecer, com uma proposta de decisão, contendo ou não recomendações, conforme a configuração da situação justifique.

As organizações públicas e privadas devem ter em conta, o que não é explícito na legislação nacional e europeia, a adequada proteção do responsável pelo tratamento das denúncias que, tal como os outros intervenientes no sistema de *Whistleblowing*, também está sujeito a retaliações, quer pela informação que passa a ter conhecimento, quer pela(s) decisão(ões) que toma ou poderá tomar.

O responsável pelo tratamento das denúncias pode também ser alvo de assédio moral (já para não falar de crimes contra a sua honra), designadamente destrato, perseguição ou devassa da sua vida pessoal (escrutínio não legítimo), de modo a ser corrompida a sua idoneidade e imparcialidade ou a ser pressionada em determinado sentido, através de coação, alguma decisão instrutória ou final.

Criar um mecanismo de *Whistleblowing* olvidando este pilar estrutural, pensando apenas na salvaguarda de direitos, liberdades e garantias do denunciante e denunciado, não só torna menos atrativo e mais árido o trabalho subjacente à tarefa do responsável pelo tratamento das denúncias, como pode pôr em causa a integridade e fiabilidade de todo sistema.

Se não forem pensadas medidas para acautelar eventuais incidentes relativos aos responsáveis pelo tratamento das denúncias, tais como a sua proteção jurídica caso venham a ser notificados num processo judicial em consequência de um assunto de *Whistleblowing* que estejam a tratar ou tenham tratado, esta função não será tida como apaziguadora em si mesma.

O *Whistleblowing* não deve ser entendido apenas como um mecanismo de prevenção e, ou, combate à corrupção. Ele engloba também a melhoria de condutas não corruptivas, fraudulentas ou que indiciam sobre a prática de outro crime e, ou, infração conexa. Este sistema deve permitir a prevenção e correção de *performances* laborais, de modo a melhorar a economia, eficiência e eficácia das organizações públicas e privadas.

O responsável pelo tratamento das denúncias deve garantir a proteção de dados pessoais (informação sobre a identidade da entidade responsável);

a finalidade prosseguida; os domínios abrangidos pela denúncia; o carácter facultativo do dispositivo; a inexistência de consequências pela não utilização do dispositivo; a transparência do processo aos destinatários da denúncia; a eventual transferência de dados para Estado exterior à UE em conformidade com a legislação europeia sobre proteção de dados; a existência de um direito de acesso e de retificação por parte das pessoas identificadas; e a não divulgação das suas identidades; deveres de confidencialidade; tratamento de dados apenas relevantes; conservação das denúncias, incluindo “conservação alheia” (isto é, não intromissão ou modificação de uma denúncia dirigida a pessoa não competente para a apreciação da mesma); proibição de retaliação; medidas de apoio para denunciadores e para denunciados; e a irrenunciabilidade dos direitos e das vias de recurso.

Ainda que a denúncia, anónima ou não, deva ser voluntária, os Estados-Membros devem: assegurar que as entidades jurídicas dos setores privado e público estabeleçam canais e procedimentos para denúncia interna; designar as autoridades competentes para receber, dar retorno de informação e dar seguimento a denúncias, dotando-as dos recursos adequados; e assegurar que as autoridades competentes revejam regularmente os procedimentos para a receção de denúncias e o seu seguimento.

Considerações finais

A temática do *Whistleblowing* em Portugal, que para alguns poderá significar o ato de denunciar ou, de uma forma abrangente (e correta), todo o procedimento e processo gerado pela denúncia, tem ganho importância acrescida, passando de recomendações, a artigos de leis até à publicação de uma Diretiva (de *soft* para *hard law*) que, por seu turno, em breve, deverá ser transposta para o ordenamento jurídico nacional.

Quando isso acontecer as organizações vão deparar-se com uma pergunta crucial: e agora, quem pode ser o responsável pelo tratamento das denúncias?

Com este texto pretendeu-se, em primeiro lugar, alertar a sociedade, em geral, e a comunidade científica, em particular, para este assunto e, em segundo lugar, asseverar, dentro do que é possível, a resposta de quem poderá ser o responsável pelo tratamento da denúncia.

A legislação existente e a que venha a existir terá de estar, forçosamente, em conformidade com o RGPD que é de aplicação direta, ainda que não seja totalmente uniforme, face a várias possibilidades que deixa ao legislador de cada Estado-Membro.

Existem direitos, mas também deveres, para todos os intervenientes no mecanismo do *Whistleblowing*, e todos os participantes no sistema devem ter a obrigação e garantia de defesa da confidencialidade dos dados pessoais.

Anseia-se por ver qual será a relação profissional entre *Compliance Officers*, Auditores, Encarregados de Proteção de Dados e responsáveis pelo tratamento das denúncias (se estes não forem os dois primeiros), ou destes com outros profissionais, e verificar se haverá uma articulação ou separação de competências relativamente ao *Whistleblowing* de modo a não haver um conflito positivo ou mesmo negativo no tratamento destas competências sobreposta. Ou, ainda, ninguém especificamente responsável, de modo a gerar um circuito vicioso de não competência direta sobre o sistema de *Whistleblowing*, ou de não decisão tempestiva.

De igual modo, acompanhar-se-á o desenvolvimento da atuação das Autoridades Competentes que venham assim ser denominadas ou eventualmente criadas. Como supervisionarão o *Whistleblowing*? Haverá alguma com atribuições ou competências para agregar e coordenar a informação estatística sobre as denúncias externas, as destinadas às autoridades competentes, a serem apresentadas anualmente à Comissão Europeia (cf. n.º 2 do art. 27.º da Diretiva)? Aguardar-se-á para ver quem serão os responsáveis pelo tratamento das denúncias internas e externas; quem serão os responsáveis pelo tratamento do *Whistleblowing*.