



# O *Whistleblowing* em Portugal

## Será que pode ser praticado pelo auditor?

### Auditoria



*Patrick de Pitta Simões*  
AUDITOR INTERNO DO INSTITUTO POLITÉCNICO DE LISBOA.





O presente artigo é um excerto, adaptado, de um capítulo da dissertação de mestrado do autor, subordinada ao tema “Os Limites da Auditoria Interna – o perfil do Auditor e o *Whistleblowing*”. Note-se que foi empregue o Novo Acordo Ortográfico, determinado pela Resolução n.º 8/2011 do Conselho de Ministros, publicada no *Diário da República* (DR), 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.

## Resumo

Após sucessivos escândalos financeiros, nos Estados Unidos da América, enfatizou-se o sistema de denúncias internas, mais conhecido por *Whistleblowing*, um sistema delimitado entre o “procedimento meramente informativo” e o “mais ou menos complexo de investigação interna”.

Em Portugal, a Comissão do Mercado de Valores Mobiliários emitiu recomendações sobre a adoção deste e por sua vez, face ao elevado número de notificações de tratamento de comunicações internas de atos de gestão financeira irregular, a Comissão Nacional de Protecção de Dados deliberou princípios (Linhas de Ética) aplicáveis aos tratamentos de dados pessoais com aquela finalidade, de modo a salvaguardar a privacidade dos intervenientes.

Com este artigo pretende-se fazer um enquadramento teórico e legal sobre o *Whistleblowing* nacional, percebendo se o auditor pode ser um *Whistleblower*.

**Palavras-chave:** Denúncias internas, *Whistleblowing*, Linhas de Ética, Privacidade.

## Abstract

After successive financial scandals in the United States of America, the system of internal denunciations, better known as *Whistleblowing*, was emphasized, as a system delimited between the “merely informative procedure” and the “more or less complex internal investigation”.

In Portugal, the National Securities Market Commission issued recommendations about adopting it and, regarding the high number of notifications concerning the internal communications of irregular financial management acts, the National Data Protection Commission, as deliberated principles (Ethic Lines) applicable to the processing of personal data for that purpose, in order to safeguard the privacy of the interveners.

Concerning the intent of this article is to make a theoretical and legal framework on the national *Whistleblowing*, analyzing if the auditor can be a *Whistleblower*.

**Keywords:** Internal complaints, *Whistleblowing*, Ethical Lines; Privacy.

## 1. Introdução

A análise e reflexão que ora se faz pretende compreender o sentido e alcance do *Whistleblowing* questionando-se se este pode ser praticado por qualquer pessoa, mais concretamente, se o auditor pode ser um *Whistleblower*; e quem deverá gerir e manusear a informação num processo de *Whistleblowing*. São estas as dúvidas que se tenta responder neste artigo, onde se abordam as Linhas de Ética pelas quais se deve pautar a implementação do *Whistleblowing*.

Desde já se explica que, de acordo com a Deliberação n.º 765/2009, da Comissão Nacional de Protecção de Dados (CNPd), aprovada na sessão plenária de 21 de setembro de 2009, «[e]m termos simples, podemos definir o *whistleblowing* como um sistema que se traduz na criação nas empresas de condições para denúncia de comportamentos fraudulentos ou irregulares capazes de afectar seriamente a sua actividade.»<sup>1</sup>

## 2. Enquadramento

Desde o início do século XXI, consecutivos escândalos têm preocupado o mundo financeiro<sup>2</sup>. Pense-se nos casos como do Banco Português de Negócios (BPN)<sup>3</sup>, do Banco Privado Português (BPP)<sup>4</sup> e do Banco Espírito Santo (BES)<sup>5</sup>. Recorrentes, têm provocado quebras de confiança nos mercados financeiros, atribuindo-se a sua ocorrência, na maior parte das vezes, à forma ou falta de controlo interno<sup>6</sup>.

Nunca como nos dias de hoje, se debateu tanto a Auditoria e os métodos que permitam uma maior e melhor eficiência dos sistemas financeiros. Cada vez mais se dá relevo à função e ao perfil do auditor (interno), na medida em que o mesmo apoia a gestão das organizações, alertando para os riscos de negócio.

Nos EUA, após o colapso de algumas empresas, a 30 de julho de 2002, como forma de promover a credibilidade, a responsabilidade, a transparência, a segurança, a prevenção e a deteção de irregularidades e, ou fraudes<sup>7</sup>, através da *SOX*<sup>8</sup>, instituiu-se às sociedades registadas num dos seus mercados bolsistas (incluindo as sociedades estrangeiras ou filiais europeias), um sistema de denúncias de corrupção<sup>9</sup> ou de má administração: o *Whistleblowing*<sup>10</sup>.

---

*“...um sistema de denúncias de corrupção ou de má administração: o Whistleblowing”.*

---

Cerca de três anos depois, a Comissão Europeia aprovou a Recomendação 2005/162/CE, de 15 de fevereiro de 2005, relativa ao papel dos Administradores Não Executivos ou Membros do Conselho de Supervisão de Sociedades Cotadas e aos Comitês do Conselho de Administração ou de Supervisão<sup>11</sup>.

Nesta, são incentivadas as empresas cotadas<sup>12</sup> a criarem comitês de auditoria aos quais incumbe, «[...] controlar o procedimento através do qual a sociedade cumpre as disposições em vigor no que diz respeito à possibilidade de os empregados notificarem irregularidades importantes, alegadamente cometidas na sociedade, [...] e assegurar-se de que existe um dispositivo que prevê uma investigação independente [...], acompanhada de medidas apropriadas.»<sup>13</sup> [sic].

«No texto recomendatório [(**Recomendação 10-A: comunicação de irregularidades**)] de Novembro de 2005[,] a CMVM introduziu uma nova recomendação segundo a qual “a sociedade deve adoptar uma política de comunicação de irregularidades alegadamente ocorridas no seio da sociedade” e que faça menção aos seguintes elementos: “indicação dos meios através dos quais as comunicações de práticas irregulares podem ser feitas internamente, incluindo as pessoas com legitimidade para receber comunicações[;] indicação do tratamento a ser dado às comunicações, incluindo tratamento confidencial, caso assim seja pretendido pelo declarante”. Com esta iniciativa pretendeu-se estimular a utilização adequada ou a criação de meios para comunicar práticas irregulares no seio das sociedades, ressaltando no entanto que a política a seguir dever[ia] ser aplicada coerentemente a cada sociedade de modo a evitar quaisquer comportamentos abusivos ou persecutórios<sup>14</sup>.»

Por sua vez, o grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais, criado pelo art. 29.º da Diretiva 95/46/CE, mais conhecido por Grupo de Protecção de Dados do Artigo 29.º<sup>15</sup>, pronunciou-se, através do Parecer n.º 1/2006, adotado em 1 fevereiro de 2006, sobre a aplicação das normas europeias em matéria de protecção de dados aos sistemas internos de denúncia de infrações nos domínios da contabilidade, dos controlos contabilísticos internos, da auditoria, da luta contra a corrupção e do crime bancário e financeiro.

De acordo com as suas atribuições<sup>16</sup> e tendo em conta as diferenças culturais, os motivos históricos ou sociais<sup>17</sup>, e a especificidade do sistema jurídico de cada país da UE, o parecer limitou-se a uma abordagem formal das regras em matérias de protecção de dados, excluindo-se o direito laboral e penal<sup>18</sup>. Contudo, tentou-se compatibilizar a *SOX*, aplicável às empresas europeias (com sanções no caso do seu incumprimento), com as normas europeias quanto à protecção de dados e às possíveis tentativas de se escamotear a Diretiva 95/46/CE, a coberto de legislação estrangeira.

Em Portugal, a CMVM, em setembro de 2007, emitiu, através do ponto II. 1.4, do seu Código do Governo das Sociedades, recomendações sobre a adoção de uma política de comunicação de irregularidades alegadamente ocorridas no seio das sociedades, concretamente: «[...] i) [a] indicação dos meios através dos quais as comunicações de práticas irregulares podem ser feitas internamente, incluindo as pessoas com legitimidade para receber comunicações; ii) indicação do tratamento a ser dado às comunicações, incluindo tratamento confidencial, caso assim seja pretendido pelo declarante. [...]»

## 3. Linhas de Ética (Whistleblowing)

A CNPD<sup>19</sup>, face ao grande número de notificações de tratamentos de dados pessoais<sup>20</sup> que recebeu com o objetivo de gerir as comunicações internas de práticas irregulares<sup>21</sup>, aprovou, em sessão plenária a 21 de setembro de 2009, a Deliberação n.º 765/2009 (de ora em diante, Deliberação da CNPD)<sup>22</sup>. Esta visa<sup>23</sup> «[d]isponibilizar aos responsáveis dos tratamentos os princípios de protecção de dados aplicáveis [naquelas] situações e estabelecer as regras orientadoras para o correcto cumprimento da Lei de Protecção de Dados; [e d]ar a conhecer aos titulares desses dados os direitos que lhes assistem e os limites estabelecidos para estes tratamentos de dados<sup>24</sup>.» Para o efeito, a CNPD, denomina este tipo de princípios orientadores<sup>25</sup>, de Linhas de Ética<sup>26</sup>.



Mais do que diretrizes de conduta ou parâmetros corretos, genericamente aceites<sup>27</sup>, pelos quais os indivíduos devem pautar o seu modo de atuação (comportamento)<sup>28</sup>, a Deliberação da CNPD tem força obrigatória nos termos do n.º 3, do art. 23º da LPDP<sup>29</sup>, pelo que os seus ditames são para se cumprir<sup>30</sup>.

## 4. Quem pode ser whistleblower?

Feito este enquadramento<sup>31</sup>, encontremos respostas às perguntas colocadas: quem pode ser *whistleblower* (qualquer pessoa, incluindo um auditor)? E quem deverá manusear e gerir a informação num processo de *Whistleblowing*?

A Deliberação da CNPD estabelece direitos para o denunciante<sup>32</sup> e limites de âmbito subjetivo e específicos quanto à entidade responsável pela apreciação das denúncias<sup>33</sup>.

Concretamente, quanto a este último, determina que não se afigura adequado «o estabelecimento de uma linha de denúncia interna, cuja gestão e apreciação compete aos eventuais denunciados.» Todavia, lacuna ou não, não define quem poderá ser denunciante.

Ora, se ao estabelecer limites de âmbito subjetivo delibera que «[a] penas as pessoas que pratiquem actos 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 poderão ser alvo de denúncia», teríamos de excluir a possibilidade de os auditores serem responsáveis pela apreciação das denúncias.

Contudo, não poderá ser esse o sentido (estrito) da Deliberação da CNPD, uma vez que também estabelece 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

cumpra as disposições em vigor no que diz respeito à possibilidade de os empregados notificarem irregularidades.»

Acrescenta ainda que, «[c]umpra, neste particular, efectuar uma distinção de regimes: a) [o]u 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; b) [o]u se verifica o recurso a entidade externa à estrutura societária, caso em que se aplica o regime de subcontratação já descrito na presente Deliberação, nos termos e para os efeitos descritos no artigo 14.º da [LPDP].»

Assim, pela Deliberação da CNPD apenas ficamos a saber que o auditor pode ser alvo de denúncia ou ser responsável, independente, pelo tratamento das denúncias. Portanto, continuamos sem conseguir dar resposta à questão: pode o auditor ser denunciante?

---

**“...auditor pode ser alvo de denúncia ou ser responsável, independente, pelo tratamento das denúncias”.**

---

O RGPD<sup>34</sup>, não se refere especificamente ao *Whistleblowing*<sup>35</sup>, pelo que se prevê que a(s) autoridade(s) de controlo<sup>36</sup> que venha(m) a ser criada(s) ou designada(s), se já existir(em), terá(ão) de se pronunciar sobre este sistema de denúncias internas (havendo aqui a oportunidade de limitar ou não a atuação dos auditores internos) que, inevitavelmente, deverá ser conjugado com os ditames da proteção das pessoas singulares no que respeita ao tratamento de dados pessoais e à livre circulação destes, ainda que seja meramente para aderir às Deliberações da (atual) CNPD<sup>37</sup> e, por ventura, aos pareceres da (atual) Comissão de Acesso aos Documentos Administrativos (CADA)<sup>38</sup>, ou ainda de uma outra entidade com responsabilidades nestas matérias, tais como, eventualmente, os Serviços de

Informações de Segurança (SIS) ou a Entidade Reguladora para a Comunicação Social (ERCS)<sup>39</sup>.

Não obstante o sentido convergente e harmonizador do RGPD<sup>40</sup>, recordando Carrigy (2005:39), «[c]ada legislador [...] determin[ou] o âmbito subjectivo de aplicação das normas de protecção, pelo que o conceito de denunciante protegido varia, da mesma forma que variam os procedimentos de aplicação das normas de protecção e o próprio domínio das normas, que poderão ser de natureza civil, criminal ou administrativa. Importa, apesar das diferenças de regimes, assentar numa noção que sirva de base [...]»

Segundo o dicionário legal *The Free Dictionary by Farlex* (s.d.), podemos saber que o *Whistleblowing* significa a divulgação por uma pessoa, normalmente um trabalhador do Estado ou de uma empresa privada, para o público ou autoridades, de uma situação de má administração, corrupção, ilegalidade ou erro<sup>41</sup>.

Para Kranacher (2006:1), um *Whistleblower* é genericamente definido como um empregado que divulga informações potencialmente danosas sobre um trabalhador, a uma autoridade que pode ser a chefia, a comunicação social ou um funcionário do governo<sup>42</sup>. Enquanto que para Near e Miceli (s.d.), *apud Carrigy* (2005:39) «*whistle blowing* pode ser definido como 'a revelação por membros de uma organização (actuais ou no passado) de práticas ilegais, imorais ou ilegítimas ocorridas dentro da esfera de controlo do empregador, a pessoas ou organizações que poderão intervir'»<sup>43</sup>.

Carrigy (2005:39), refere que «[...] são várias as classificações usadas, atendendo, nomeadamente, à qualidade da pessoa que faz a denúncia, falando-se em denúncias por colaboradores ou por pessoas que o foram ou que estão ligadas à empresa por outro tipo de vínculo (prestação de serviços), aos meios de denúncia disponíveis e às formas de protecção disponíveis.»



De acordo com alguns autores, existem dois tipos de denúncias: as internas, aquelas em que o trabalhador denuncia, dentro da sua organização, uma conduta ou comportamento ilegal de um colega de trabalho ou superior hierárquico; e as externas, aquelas em que o trabalhador denuncia para entidades externas à sua organização, tais como instituições reguladoras ou os meios de comunicação.

Assim, para Latimer e Brown (2008:777), «[...] apenas quando a denúncia interna falhar é que se deve recorrer a agências, entidades ou órgãos externos para efetuar denúncias.»<sup>44</sup>

Berry (2004:1) *apud* Barbosa (2012:14) «refere que apesar de o mecanismo de *whistleblowing* envolver denúncias tanto dentro como fora da organização, existe uma grande vantagem quando os colaboradores escolhem denunciar internamente», pois evitam o constrangimento (escrutínio) público e litígios (incluindo multas) dispendiosos.

Banisar (2006) *apud* Barbosa (2012:15), menciona «que a primeira e a mais apropriada via de efetuar denúncias deve ser a própria organização, tendo em conta que uma [...] bem estruturada quererá saber sobre as condutas erradas, para tomar as medidas necessárias para as corrigir. [...] Banisar (2006) refere também que muitas vezes os *whistleblowers* optam pela via externa, quando se trata de graves problemas, sendo quase certo que se a denúncia for feita internamente existem probabilidades de ocorrer retaliação ou de destruição de provas.»

De acordo com Carrigy (2005:39) estes modos de denúncia (interna e externa) causam impactos diferentes. Na denúncia interna «[...] a empresa poderá actuar e tentar resolver a situação internamente, mantendo algum controlo sobre a informação relativa ao caso; na denúncia exterior e principalmente nas situações em que a entidade exterior não está obrigada a sigilo, a empresa, embora mantendo a possibilidade de actuar no sentido de resolver a situação detectada perdeu a possibilidade de gerir a informação relativa ao caso, sendo certo que a confiança do público em geral e dos *stakeholders*<sup>45</sup> em particular dependem em larga medida do modo como a situação e a informação a ela respeitante é gerida. A denúncia externa, na medida em que representa um maior risco para a empresa, coloca a questão da ponderação do eventual interesse público na informação face ao interesse da empresa e lança a discussão relativa à legitimidade da motivação/actuação do denunciante.»

Perry (1993:81), menciona que o *Whistleblowing* tem mais a ver com os interesses pessoais ao invés de ser propriamente uma atitude altruísta. Este autor tipifica três tipos de queixas: a válida, de acordo com a percepção do denunciante (a mais frequentemente falada por autores); a inválida, de acordo com o que a pessoa apreende, erradamente pois não confirma; e a inválida, mais séria, pois quem denuncia fá-lo para o seu próprio proveito<sup>46</sup>.

Carrigy (2005:46) refere ainda que, «[a] denúncia ao exterior que venha a ser conhecida do público causa sempre prejuízo à empresa, no mínimo, o da má publicidade associada [...], ainda que os [...] dirigentes [...] reconheça[m] a importância de pôr termo à actuação denunciada.»

Por sua vez, «[o] estímulo da denúncia interna, pelo contrário, apesar de poder ser considerado um mecanismo de criação de um clima de suspeita e desconfiança entre colaboradores e entre estes e a direcção, será, no entanto, considerado positivo numa cultura em que a direcção se sente responsável por tudo o que ocorre dentro da



empresa, em que esta actua e espera que se actue de forma responsável e em que se dispõe a investigar e resolver as situações denunciadas de forma célere e justa. A denúncia interna pode, pois, ser um mecanismo que permita a detecção precoce e termo de situações irregulares antes de estas se tornarem gravemente danosas [...]» (ibid.:46).

Park, Blenkinsopp, Oktem e Omurgonulsen (2008:4), tipificam a denúncia em identificada («quando um colaborador que denunciou práticas inapropriadas usa o seu verdadeiro nome, ou de alguma outra forma, fornece informações que possam identificá-lo») ou anónima («quando o colaborador não fornece nenhuma informação sobre si, ou então fornece uma identificação falsa.»)<sup>47</sup>

A Deliberação da CNPD repudia o anonimato a favor de um regime de confidencialidade como forma de salvaguardar os riscos de denúncia caluniosa e de discriminação<sup>48</sup>.

À pessoa identificada pela denúncia deverão ser assegurados os direitos de informação sobre a entidade responsável, os factos denunciados (salvo a identidade do denunciante) e a finalidade do tratamento<sup>49</sup>, bem como os direitos ao acesso, à retificação e à eliminação dos dados, como também o direito de oposição. Contudo, a Deliberação da CNPD, reconhece «a possibilidade de restrição desses direitos quando os interesses perseguidos pelo sistema, a protecção dos direitos das restantes pessoas envolvidas, em particular do denunciante, e as finalidades da investigação o exijam.»<sup>50</sup>

Por sua vez, Park [et al.] (2008), *apud* Barbosa (2012:12) mencionam ainda que a denúncia pode ser formal quando há «uma forma institucional de comunicar irregularidades, seguindo as linhas padrão de denúncias ou um protocolo da organização para o efeito [...]», e informal quando «é feita pessoalmente pelo colaborador aos outros [...] mais próximos ou alguém na organização, em quem [...] confia [...]».

Jubb (1999:90) *apud* Barbosa (2012:12), refere-se «a este mesmo tipo de denúncia, como autorizada e não autorizada». Tendo em conta o nosso panorama nacional antes do RGPD, podíamos dizer que era o nosso caso, existir um sistema de *Whistleblowing* com ou sem a autorização da CNPD.

Jubb (2000) *apud* Barbosa (2012:60) «refere que os auditores como qualquer outra pessoa podem tornar-se *whistleblowers*, mas a questão é saber se eles ganham esta denominação simplesmente por exercerem a sua profissão.» O(s) autor(es) prossegue(m) afirmando que «[...] a função de auditoria externa possui algumas características que se encaixam na definição de *whistleblowing*. [...] [O]s auditores [...] fazem revelações intencionais sobre ilegalidades, não conformidades regulamentares, ineficiências, violações aos códigos, políticas ou mecanismos de controlo, que ocorrem dentro das organizações, sendo certo que o critério da materialidade pode

ser invocado para seleccionar apenas os erros mais significativos a serem divulgados. Por outro lado, os relatórios de auditoria são destinados aos proprietários, reguladores, gestão, entre outros que, em diferentes graus, podem tomar uma ação corretiva. [...] [M]as [...] constituem-se os auditores *whistleblowers* simplesmente por exercerem a sua profissão, ou melhor dizendo, os auditores tornam-se *whistleblowers* em virtude de denúncias de fraudes efetuadas no exercício de uma auditoria? [...] [Jubb e Barbosa entendem que] não. Pois ao contrário dos clássicos *whistleblowers*, que denunciam condutas erradas de forma livre ou opcional, os auditores possuem responsabilidades legais para o efeito<sup>51</sup> [...]. Nesse sentido, perante fraudes, não se espera outra atitude senão a denúncia das mesmas por parte do auditor.»<sup>52</sup>

«[C]omparativamente aos auditores externos, os auditores internos por serem colaboradores da organização perante uma situação de fraude, enfrentam um maior dilema de lealdade para com a mesma, uma vez que ao efetuarem divulgações de informações (nesse caso às partes externas à organização) podem estar [a infringir] a obediência e a confidencialidade<sup>53</sup>, e dessa forma os riscos que enfrentam são mais imediatos.» (ibid.:2000 *apud* ibid. 2012:63)<sup>54</sup>.

«[...] [A]lguns auditores internos podem optar por denunciar externamente, mas num papel diferente, talvez como simples profissional ou cidadão preocupado. Neste sentido procuram uma entidade externa porque, na sua opinião, a organização deixou de responder adequadamente às suas preocupações. O conhecimento revelado é obtido no âmbito do seu trabalho, mas a sua divulgação pública não faz parte do seu trabalho, neste caso constituem-se *whistleblowers*. [...] De forma conclusiva, [...] os auditores [...] só constituem candidatos a *whistleblowers* se tais divulgações forem feitas externamente (auditor interno) e forem além do propósito do seu papel formal na organização (auditor interno e auditor externo).» (ibid.:2000 *apud* ibid. 2012:64).

## 5. Considerações finais

Verificou-se que, após diversos descalabros financeiros, os EUA, através da SOX, ao implementar alargadamente o *Whistleblowing*, estabeleceu um marco histórico no que respeita às empresas americanas e por arrastamento às europeias (quer estivessem ou não cotadas nas suas bolsas de valores).

A estratégia de combate à corrupção, fraude e irregularidades, passou a ser a procura de uma cultura que fomenta condutas eticamente aceitáveis por parte dos trabalhadores (incluindo os auditores internos) e favoreça atitudes responsáveis e transparentes.

Com o objetivo de assegurar a fiabilidade e a credibilidade da informação financeira, protegendo os *stakeholders*, o *Whistleblowing* traduz-se na criação de condições para a denúncia de comportamentos irregulares capazes de afetar, seriamente, a atividade das organizações. Neste contexto, este mecanismo (muitas vezes, também, apenas e só sinónimo de decisão ética de ação, isto é, de denunciar)<sup>55</sup> pode dar um contributo importante para a adoção de uma conduta profissional eficiente (preventiva) e para um eficaz controlo interno (reativa)<sup>56</sup>.

Nesse sentido, a CNPD deliberou Linhas de Ética, de modo a que seja possível, dando sustento legal (complementando os institutos gerais do direito de trabalho na salvaguarda ao denunciante de re-



presálias do empregador), ao uso subsidiário de um dispositivo adequado de reporte de irregularidades, protegendo a privacidade dos seus intervenientes (denunciado, denunciante e responsável pela recolha, tratamento e conservação dos dados pessoais que, em última análise, é de todos os intervenientes, o mais interessado neste mecanismo).

Se noutros países o *whistleblower* pode ser qualquer indivíduo (trabalhador ou não da organização) que denuncie situações irregulares, podendo optar por fazê-lo interna ou externamente, a nível nacional o *Whistleblowing* apresenta limites específicos (de âmbito objetivo, subjetivo, procedimental, de autonomia da vontade e de entidade responsável pela apreciação de denúncias) que o auditor, como possível responsável pelo tratamento das denúncias (caso não haja uma entidade incumbida pela averiguação das denúncias como, por exemplo, um Comité de Auditoria ou empresa externa de auditoria) deve respeitar.

É possível que o auditor seja *whistleblower*, mas não é desejável por significar que algo na estrutura não está correto ou algo grave carece de ser denunciado. Neste caso a denúncia externa deve ser admissível apesar de indesejável.

Só numa situação de obrigação legal se compreenderá que o auditor possa ser denunciante (*whistleblower*) ainda que possa ser, em simultâneo, responsável pela apreciação das denúncias.

**“...Só numa situação de obrigação legal se compreenderá que o auditor possa ser denunciante (*whistleblower*)”.**

A Auditoria e o *Whistleblowing* estão interligados na medida em que ambos visam a melhor *performance* da entidade.

Cada empresa tem o seu próprio ambiente, pelo que não existe um sistema de denúncias que seja o ideal para todas. As organizações devem, considerando as circunstâncias operacionais e culturais, como refere Carrigy (2005), fomentar uma «cultura de exigência ética» de modo a favorecer atitudes responsáveis em que os colaboradores tomem a iniciativa de denunciar as situações consideradas irregulares, de forma a evitar danos maiores.

O *Whistleblowing* não deve ser tido como um sistema de gestão de reclamações indiscriminadas ou alarmistas. Daí que a CNPD tenha balizado, legalmente, as matérias a serem tratadas e entenda que não se deva aceitar o anonimato (que torna difícil a investigação tanto em termos de clarificação, como de corroboração de factos), mas sim a confidencialidade (protegendo a identidade dos intervenientes).

A aparente vantagem do anonimato que permite aos indivíduos temerários de retaliações divulguem as irregularidades cometidas por outro(s) colega(s), pode gerar um clima de suspeição generalizado, que além de criar um ambiente hostil entre colegas, será “desestabilizador” para quem venha a ser descoberto como delator (inibindo assim a continuidade deste mecanismo) ou contraproducente no dispêndio de recursos em queixas infundadas.

Diferentemente da obrigatoriedade de participação de um crime a um Órgão de Polícia Criminal (OPC), ou dos deveres legais como,



por exemplo, os que impendem sobre o órgão de fiscalização ou o ROC no âmbito do CSC, convém salientar que a denúncia de irregularidades (nos termos das Linhas de Ética) é (e deve ser) feita de forma voluntária, não existindo uma imposição legal por parte da entidade sobre os colaboradores. Ainda que haja regulamentos internos ou códigos de conduta nesse sentido, a Deliberação da CNPD, a *contrario sensu* do regime penal e processual penal que se aplica, subsidiariamente, ao contraordenacional e disciplinar no âmbito das relações de trabalho, pugna pela voluntariedade da denúncia.

O risco de estigmatização ou a pura má-fé manipulando e incriminando condutas corretas, justifica a necessidade de proteção jurídica a todos os intervenientes.

Assim, neste caso concreto, é-se tentado a dizer que o Direito (sentido de justiça) e a Auditoria (tecnicidade apurada), fazem uma parceria perfeita para assunção de responsabilidade pelo tratamento deste sistema de denúncias internas.

Ao contrário do auditor forense<sup>57</sup>, o auditor interno<sup>58</sup>, não procura detetar fraudes, mas se as encontra deve reportar a quem de direito. O auditor interno não é um *whistleblower* por inerência de funções, apenas o é (externamente) por inevitabilidade ocasional, caso a estrutura não disponha, por exemplo, de um Comité de Auditoria ou seja possível (e talvez desejável) o reporte a uma empresa de auditoria externa (responsável pela apreciação das denúncias)<sup>59</sup>, ou se a gravidade do assunto assim o determinar. Apenas e só nesta medida poderemos entender que o auditor (interno) é uma espécie de *whistleblower* qualificado e desde que a denúncia se enquadre no âmbito objetivo deliberado pela CNPD<sup>60</sup>.

Em suma, o *Whistleblowing* pode ser praticado por qualquer pessoa, incluindo o próprio auditor em geral (na qualidade de trabalhador como os demais em situações que pela gravidade deve reportar a um OPC, tornando-se assim num *whistleblower* externo) ou um terceiro (pessoa externa à organização).

1 Mencione-se que a Deliberação refere-se também a este sistema como mecanismo ou dispositivo.

2 Tais como os intitulados: *Adecco, Adelphia, Ahold, AOL, Arthur Andersen, Enron Corporation, Goldman Sachs, Lehman Brothers, Madoff, Nortel, Parmalat, Tyco, Vivendi, WorldCom, a Xerox E*, ou, até mesmo, a Operação *Lava Jato* e o Escândalo da *Mensalão*, ou as divulgações feitas através do *WikiLeaks*, dos *Papéis do Panamá* ou *LuxLeaks*.

3 A 1 de novembro de 2008, «[o] Governo português nacionaliza o [BPN], por receio dos efeitos sistemáticos na banca nacional». A 4 de janeiro de 2010, «[é] publicado o [DL] que aprova o processo de privatização do BPN, nacionalizado em finais de 2008.» *In website* do Observatório sobre Crises e Alternativas – OCA (s.d.), criado pelo Centro de Estudos Sociais, com a colaboração do Instituto para os Estudos Laborais da Organização Internacional do Trabalho, ambos da Universidade de Coimbra.

4 «O Banco de Portugal torn[ou] público que, por deliberação do Conselho de Administração de 15 de Abril de 2010, [...] foi revogada a autorização para o exercício da atividade do [BPP], SA, depois de verificada a inviabilidade dos esforços de recapitalização e recuperação desta instituição desenvolvidos no contexto das providências extraordinárias de saneamento adotadas pelo Banco de Portugal. [...]» *In website* do Banco de Portugal (s.d.).

5 A 3 de agosto de 2014, «[o] Banco de Portugal intervém no [BES], criando duas instituições: o [BES] e o Banco Novo. O governador Carlos Costa menciona práticas fraudulentas levadas a cabo pela administração de Ricardo Salgado.» *In website* do OCA (s.d.).

6 Existem várias definições deste, mas podemos entender que engloba todos os métodos e medidas adotados para providenciar fiabilidade e compreensibilidade à informação (contabilística e não financeira), salvaguardar os ativos, prevenir e detetar erros e fraudes, objetivar a eficiência das operações em conformidade com os normativos aplicáveis, gerar uma maior confiança e garantia de qualidade na organização. A ISA 315 § 4, alínea c), define como «[o] processo concebido, implementado e mantido pelos encarregados da governação, pela gerência e por outro pessoal para proporcionar segurança razoável acerca da consecução dos objetivos de uma entidade com respeito à fiabilidade do relato financeiro, eficácia e eficiência das operações, e cumprimento de leis e regulamentos aplicáveis. [...]». *Mutatis mutandis*, o n.º 2 do art. 2.º do DL n.º 166/98, de 25 de junho, que institui o sistema de controlo interno da administração financeira do Estado, refere que «[o] controlo interno consiste na verificação, acompanhamento, avaliação e informação sobre a legalidade, regularidade e boa gestão, relativamente a actividades, programas, projectos, ou operações de entidades [...]».

7 A ISA 240 (Clarificada), que versa sobre a responsabilidade do auditor ao considerar a fraude numa Auditoria de Demonstrações Financeiras, define na alínea a), do seu § 11, a fraude como «[u]m acto intencional por um ou mais indivíduos entre a gerência, os encarregados da governação, os empregados ou terceiros, envolvendo o uso de enganar para obter uma vantagem injusta ou ilegala». Recorde-se que o Código Civil, aprovado pelo DL n.º 47344, de 25 de novembro de 1966, em vigor, com as devidas alterações, prevê no seu art. 21.º um normativo respeitante a fraude à lei, no qual dispõe que fraude são «[...] as situações de facto ou de direito criadas com o intuito [...] de evitar a aplicabilidade da lei que, noutras circunstâncias, seria competente».

8 Ao abrigo das secções 301 (responsabilidade corporativa da Comissão de Auditoria nas empresas cotadas); 806 (proteção civil contra retaliações em casos de fraude); e 1107 (retaliação contra denunciante). Segundo Carrigy (2005:38), «[a] denúncia, por parte de um colaborador de uma instituição, de supostas ilegalidades ocorridas nessa mesma instituição, foi pela primeira vez especificamente regulamentada nos EUA numa lei de 1863, o *False Claims Act*, estabelecido para combater a fraude de fornecedores do governo federal durante a guerra civil.»

9 De acordo com o Departamento Central de Investigação Penal, do Ministério Público nacional (s.d.), «[d]e um modo geral, a corrupção pode-se definir como o desvio de um poder para fins diferentes daqueles para que foi concedido. [...]»

10 Escrito de forma junta cf. Perry (1993), Jubb (1999) e Viten (2003), e não de forma separada como outros autores escrevem tais como Carrigy (2005), Smith (2010) ou Lavina (2014); não obstante, poderem ser palavras autónomas (na tradução livre do autor: apito e sopro). Barbosa (2012:6) refere que a tradução à letra de *Whistleblowing* será soprar o apito. Fazendo-se alusão à prática antiga de polícias soprar um apito para indicar uma ação ilegal ou ilícita, talvez seja essa a origem desta palavra. Carrigy (2005:39) refere que a tradução, será «pôr a boca no trombone» ou «soar o alarme». Entendemos ser mais adequada esta última.

11 Não iremos analisar documentos europeus antecedentes, tais como a Comunicação da Comissão – concluir o mandato da reforma: relatório intercalar e medidas a aplicar em 2004 – que no seu ponto 4.4, previa a denúncia de irregularidades, e referenciava como sua precedente a Decisão da Comissão de 2 de junho de 1999; sob pena de nos alongarmos em demasia neste enquadramento histórico legal.

12 Cf. o seu considerando 3.º, «[...] [d]efinidas, como sociedades cujos valores mobiliários são admitidos à negociação num mercado regulamentado pela Comunidade. [...]».

13 Cf. n.º 8 do ponto 4.3 do Anexo I da Recomendação.

14 Segundo informação constante no *website* da CMVM [consult. 14 jun. 2018]. Disponível em: [http://www.cmvm.pt/pt/EstatisticasEstudosEPublicacoes/EstudosEWorkingsPapers/Pages/20061023\\_inq6\\_3\\_3.13.aspx](http://www.cmvm.pt/pt/EstatisticasEstudosEPublicacoes/EstudosEWorkingsPapers/Pages/20061023_inq6_3_3.13.aspx).

15 Composto pelas autoridades de proteção de dados dos Estados-Membros.

16 Previstas no art. 30.º da Diretiva 95/46/CE.

17 *Transparency International* (2009) *apud* Barbosa (2012:34), fez um estudo «sobre a proteção dos *whistleblowers* em 10 países da Europa, no que respeita à conotação que é atribuída aos denunciante nestes países [...]». Em alguns, «[...] são vistos como informadores, no sentido negativo da palavra, como traidores ou espíões [...]» [E]m muitos desses países essa percepção negativa de *whistleblowing* é resultado dos vários anos do regime autoritário e da existência de redes de policiais secretas. [...] Noutros casos [...], parece haver uma desconfiança geral das autoridades públicas e uma forte ênfase em não falar contra o vizinho ou colega. [...] De acordo com o *Inter-Active Terminology for Europe* (IATE) - banco de dados, usado pelas instituições e agências da UE, desde 2004, para disseminação, partilha e padronização da terminologia específica da UE – (s.d.), o *whistleblower* pode ser denominado de “alertador”. Um termo sem as conotações negativas que se podem associar a “denunciante» ou a “informador»; fortemente ligadas em Portugal às situações históricas de repressão política. Sob pena de desvio do tema deste artigo, não se abordará o que autores, como Simões e Larguesa (2010), referem como as causas ou motivações para não haver denúncias de irregularidades quando se tem conhecimento da sua existência.

18 Entende-se que não compete neste artigo indagar até que ponto o *Whistleblowing*, ao minimizar e, ou, evitar irregularidades (salvaguardando assim a marca e imagem da empresa, o seu valor intrínseco – o *Goodwill*), não constitui uma desresponsabilidade e, ou despenalização, em sentido lato, do ordenamento jurídico disciplinar (previsto no Código do Trabalho), contraordenacional (previsto em diversas disposições legais avulsas de Autoridades Reguladoras, e, ou, serviços de Inspeção), civil (previstos no Código Civil), comercial (previstos no Código das Sociedades Comerciais - CSC) fiscal (previstos nos diversos Códigos Tributários), financeiro (previstos mormente na legislação referente às instituições de crédito) e penal (previstos no Código Penal e no Código de Processo Penal – CPP –, nomeadamente o regime de denúncia obrigatória previsto no art. 242.º do CPP), sobretudo, se não houver o devido reporte aos órgãos de polícia criminal (OPC – cf. definidos na alínea c) do art. 1.º do CPP). Não se irá pois, numa análise puramente jurídica, tecer considerações sobre “os limites do *Whistleblowing*”, e se há ou não uma perversão dos deveres jurídicos (ainda que os atos processuais não sejam tão céleres quanto desejáveis ou “altruistas”), pelas vicissitudes económicas.

19 De acordo com os arts. 21.º e 22.º da Lei n.º 67/98, de 26 de outubro, alterada pela Retificação n.º 22/98, de 28 de novembro e pela Lei n.º 103/2015, de 24 de agosto, de ora avante Lei da Proteção de Dados Pessoais (LPDP), a CNPD é a Autoridade Nacional de Controlo de Dados Pessoais.

20 Nos termos do art. 3.º, alínea a) da LPDP, entende-se por dados pessoais: «qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social». Definições («dados pessoais» e «titular dos dados») ligeiramente reformuladas pela alínea 1) do art. 4.º do Regulamento (UE) 2016/679, do Parlamento Europeu do Conselho, de 27 de abril.

21 Sousa e Matos (2010:55), elucida que «[a] irregularidade é a consequência reservada pela ordem jurídica para os actos que padeçam de ilegalidades pouco graves e, como tal, tidas como insusceptíveis de afectar de forma essencial a produção de efeitos estáveis pelos actos viciados em causa. Subjacentes aos casos de irregularidade podem estar apenas vícios competenciais e formais e nunca vícios materiais ou funcionais.»

22 A Deliberação da CNPD, de carácter geral, teve em conta, entre outros diplomas legais, o disposto no art. 4.º da Lei n.º 19/2008, de 21 de abril, posteriormente, alterada pela Lei n.º 30/2015, de 22 de abril, que aprovou as medidas de combate à corrupção e prevê garantias para os denunciante, a saber: «1 – [o]s trabalhadores da Administração Pública e de empresas do sector empresarial do Estado, assim como os trabalhadores do sector privado, que denunciem o cometimento de infrações de que tiverem conhecimento no exercício das suas funções ou por causa delas não podem, sob qualquer forma, incluindo a transferência não voluntária ou o despedimento, ser prejudicados. 2 – [p]resume-se abusiva, até prova em contrário, a aplicação de sanção disciplinar aos trabalhadores referidos no número anterior, quando tenha lugar até um ano após a respectiva denúncia. 3 – [o]s trabalhadores referidos nos números anteriores têm direito a: a) [a]nonimato, excepto para os investigadores, até à dedução de acusação; b) [t]ransferência a seu pedido, sem faculdade de recusa, após dedução de acusação; c) [b]eneficiário, com as devidas adaptações, das medidas previstas na Lei n.º 93/99, de 14 de julho, que regula a aplicação de medidas para a proteção de testemunhas em processo penal, alterada pela Lei n.º 29/2008, de 4 de julho, e pela Lei n.º 42/2010, de 3 de setembro.»

23 Note-se que a finalidade é a gestão das comunicações internas de práticas irregulares, destinadas a prevenir e, ou a reprimir irregularidades no seio das sociedades, nos domínios da contabilidade, auditoria, luta contra a corrupção e do crime bancário e financeiro. Ao contrário do regime do Reino Unido (previsto pela *Public Interest Disclosure Act*), ou dos EUA (previsto pela *SOX*) que são mais amplos e abarcam ilícitos criminais, mormente a fraude. A CNPD estabelece limites específicos de âmbito objetivo (considerando que as relações no local de trabalho se devem pautar por princípios da boa-fé, lealdade e confiança, restringe o sistema de denúncia aos domínios já referidos), subjetivo (apenas as pessoas que pratiquem atos de gestão relacionados com os tais domínios poderão ser alvo de denúncia, uma vez que este mecanismo não deverá servir de suporte a um regime de denúncia geral), procedimental (a utilização do sistema deve ser complementar à atividade regular da entidade, limitando a casos onde não seja objetivamente justificável o uso dos demais mecanismos de comunicação interna ou decorrentes da ordem jurídica nacional, revestindo a natureza de dispositivo subsidiário) e autonomia da vontade (questão controversa ao nível da eticidade do dispositivo, isto

é, o carácter impositivo ou facultativo da denúncia; todavia a CNPD toma a posição de entender que só nos casos em que a lei penal e processual penal o determine se justifica um regime de obrigatoriedade). Refira-se que estes regimes em geral são menos positivistas (legalistas), dos que os regimes continentais europeus, pelo que não será de estranhar que alguns âmbitos, designadamente o penal, estejam englobados. Aliás, como realça Schmidt (s.d.), *apud* Carrigy (2005:47), «o contexto juslaboral dos EUA e do [Reino Unido] é muito diverso daquele da tradição jurídica continental, onde os mecanismos legais de defesa do trabalhador estão mais aperfeiçoados, nomeadamente na exigência do procedimento de despedimento e aplicação de sanções.»

24 Dados esses que, cf. a Deliberação da CNPD «[...] devem ser adequados, pertinentes e não excessivos relativamente à finalidade da recolha [...]».

25 Cf. denomina no seu relatório de atividades de 2009. CNPD (2009:11).

26 Barbosa (2012:1), não obstante identificar no seu trabalho a Deliberação da CNPD (repeita-se, de carácter geral), de 2009, afirmou que «[e]m Portugal, [...] apenas exist[ia] uma recomendação da [...] CMVM [relativa] às empresas cotadas, sobre a adoção de uma política de denúncias [...]» e que «[a] denúncia de ilegalidades no seio da empresa por trabalhadores ou outras pessoas ligadas à atividade, não est[ava] especificamente regulada na legislação portuguesa». A autora cita, concordando, Carrigy que, em 2005, poderia dizer isso ainda que fizesse uma interpretação positivista (restritiva ou literalista) do ordenamento jurídico nacional num todo, nomeadamente penal, contra-denunciação e laboral (disciplinar), embora esta autora refira estes (dizendo (2005:45), contudo, que «[o] problema é, no entanto, que dificilmente poderá o trabalhador ter sucesso na impugnação de despedimento causado por denúncia, quando tenha sido outro, legítimo, o motivo invocado para o despedimento [...]»); bem como ainda que a CNPD tenha deliberado casuisticamente sobre a protecção de dados para o cumprimento dos requisitos da SOX (a título de exemplo, o processo n.º 2595/2003). Todavia, Barbosa (2012) sabendo que a CNPD já tinha deliberado sobre o assunto (em 2009), não deveria afirmar tal.

27 Há quem chame às Linhas de Ética, "Política Anti-Fraude", por exemplo a Açoreana Seguros ([em linha] s.d.). [Consult. 10 Set. 2018]. Disponível em: [https://www.ageas.pt/documents/11601/1239505/Politica\\_anti-fraude\\_20\\_04\\_17.pdf/03d65a9c-513e-405c-8720-84cc43d1014d](https://www.ageas.pt/documents/11601/1239505/Politica_anti-fraude_20_04_17.pdf/03d65a9c-513e-405c-8720-84cc43d1014d), Ageas Seguros ([em linha] s.d.). [Consult. 10 Set. 2018]. Disponível em: [https://www.acoreanaseguros.pt/institucional/politica\\_anti-fraude/](https://www.acoreanaseguros.pt/institucional/politica_anti-fraude/), Groupama Seguros ([em linha] s.d.). [Consult. 10 Set. 2018]. Disponível em: <http://www.groupama.pt/fundo-pens-es/pol-tica-anti-fraude/pol-tica-anti-fraude-@/article.jsp?zid=37755>), ou a Tranquilidade ([em linha] s.d.). [Consult. 10 Set. 2018]. Disponível em: <https://www.tranquilidade.pt/pt/cstinter242>; ou denomine "Linhas de alerta", como o Grupo Auchan ([em linha] s.d.). [Consult. 10 Set. 2018]. Disponível em: [https://www.unglobalcompact.org/system/attachments/cop\\_2016/345551/original/RelatorioSustentabilidadeJUMBO\\_2015web.pdf?1481305456](https://www.unglobalcompact.org/system/attachments/cop_2016/345551/original/RelatorioSustentabilidadeJUMBO_2015web.pdf?1481305456)). Ou ainda, Comunicação de Irregularidades como o Banco Comercial Português, S.A. ([em linha] s.d.). [Consult. 10 Set. 2018]. Disponível em: [https://ind.millenniumbcp.pt/pt/Institucional/governacao/Documents/Reg\\_Comunicacao\\_lreg\\_25022015.pdf](https://ind.millenniumbcp.pt/pt/Institucional/governacao/Documents/Reg_Comunicacao_lreg_25022015.pdf)

28 Orientações para um julgamento ético-moral introspectivo (sobretudo em torno da lealdade), mas também cívico, do dever de comunicar o incorreto ou incorreto, sendo muitas vezes uma linha de fronteira muito tênue entre a bravura de denunciar e o receio de represálias ou de ser considerado traidor. Segundo Berry (2004:1), *apud* Barbosa (2012:23), «*Whistleblowing is the voice of conscience.*»

29 Apesar dos dados com a finalidade de gerir as comunicações internas de práticas irregulares de âmbito financeiro não serem classificados como sensíveis (cf. previstos no art. 7.º da LPDP), são especialmente protegidos (cf. n.º 2 do art. 8.º da LPDP).

30 Antes do Regulamento (UE) 2016/679, do Parlamento Europeu do Conselho, de 27 de abril, relativo à protecção das pessoas singulares no que respeita ao tratamento de dados pessoais e à livre circulação dos mesmos, mais conhecido por Regulamento Geral sobre a Protecção de Dados (RGPD), de acordo com a alínea a), do n.º 1, do art. 28.º da LPDP, o tratamento deste tipo de dados era legalmente sujeito a uma protecção especial que obrigava à existência de controlo prévio da CNPD, pelo que não se podia iniciar aquele antes desta o autorizar. A CNPD tinha de apreciar «se o tratamento est[ava] em conformidade com os princípios de protecção de dados, designadamente quanto à qualidade dos dados e quanto ao âmbito e admissibilidade do tratamento. [...]» (cf. Deliberação). Com o RGPD deixou de haver autorização prévia porque as entidades são agora responsáveis pela aplicação daquele.

31 No qual não falámos, sob pena de nos alongarmos, sobre a *Dodd-Frank Act.*, assinada em 21 de julho de 2010, que, sucintamente, surgiu na sequência do caso *Madoff* e da crise financeira de 2008, incentivando o *Whistleblowing* nos EUA, através de recompensa monetária aos *whistleblowers*.

32 Nomeadamente «[...] [o]s utilizadores do dispositivo serão informados sobre a identidade da entidade responsável, finalidade prosseguida, domínios abrangidos pela denúncia, carácter facultativo do dispositivo, inexistência de consequência pela não utilização do dispositivo, destinatários da denúncia, eventual transferência de dados para Estado exterior à UE e sobre a existência de um direito de acesso e de rectificação por parte das pessoas identificadas no quadro do dispositivo. Serão ainda advertidos de que a utilização abusiva e de má-fé do dispositivo pode expor o seu autor a sanções disciplinares e a procedimento judicial. Com estes limites, ao denunciante serão dadas garantias de confidencialidade no tratamento dos dados que lhe respeitem.»

33 Entendida por pessoa singular ou colectiva, autoridade pública, serviço ou qualquer organismo (individual ou em conjunto), cf. alínea d) do art. 3.º da LPDP. Definição idêntica ao art. 4.º, alínea 7), do RGPD. A Deliberação estatui que a entidade responsável deve

ser individualmente indicada, só se admitindo a co-responsabilidade entre instituições em casos de absoluta impossibilidade de determinar individualmente a responsabilidade pelo tratamento. Ao responsável pelo tratamento cumpre assegurar os meios e indicar as pessoas ou órgãos que estejam especialmente encarregadas da recolha, do tratamento e destino das denúncias, as quais deverão ser em número limitado, com formação técnica adequada e adstritas ao dever de confidencialidade assumido contratualmente. 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. 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. Matéria regulada no capítulo IV, momento secção 1, do RGPD. Tenha-se ainda em linha de conta, nos termos da secção 4 do capítulo IV do RGPD, a figura jurídica do encarregado da protecção de dados.

34 Que revogou a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro. O RGPD, com 173 considerandos, obrigatório em todos os seus elementos e diretamente aplicável aos Estados-Membros, entrou em vigor no dia 25 de maio de 2016 e previu um período transitório de dois anos para a sua total aplicação (a partir de 25 de maio de 2018). Por ventura, da sua análise geral, o RGPD, mais do que uma mudança legal (entre outras certamente, Lopes (2016:42) defende que a aplicabilidade do RGPD gera a necessidade de alterar a redação do art. 35.º da CRP) ou procedimental (com, por exemplo, evidentes alterações a nível informático), tendo como pano de fundo a análise de risco, mudará comportamentos sociais.

35 Ainda que o Regulamento (UE) n.º 537/2014, do Parlamento Europeu e do Conselho, de 16 de abril de 2014 (relativo aos requisitos específicos para a revisão legal de contas das entidades de interesse público, e que revoga a Decisão 2005/909/CE da Comissão, de 14 de dezembro), no seu art. 7.º preveja a forma de atuação (divulgar informações) de um Revisor Oficial de Contas (ROC) em caso de deteção de irregularidades (incluindo fraude) sem que isso constitua uma violação a qualquer restrição contratual ou jurídica; e a Diretiva 2014/56/UE, do Parlamento Europeu e do Conselho, de 16 de abril (que altera, insere e suprime disposições legais da Diretiva 2006/43/CE), mencione, também, no seu considerando 17, sem grande explicação sobre quem poderão ser os indivíduos em causa ou mesmo a correlação com os considerandos anteriores, que: «[o]s denunciantes podem fornecer às autoridades competentes novas informações que as ajudem a detetar e a impor sanções por irregularidades, incluindo a fraude. Contudo, os denunciantes podem ser dissuadidos de prestar essa assistência por receio de retaliação ou por não terem incentivos para tal. Os Estados-Membros deverão por conseguinte assegurar a existência de mecanismos adequados para incentivar os denunciantes a alertarem as autoridades para possíveis infrações à [...] [D]iretiva ou ao Regulamento (UE) n.º 537/2014 e para os proteger de retaliações. Os Estados-Membros deverão também poder oferecer incentivos aos informadores internos, mas estes só deverão poder beneficiar desses incentivos se divulgarem novas informações que não sejam já obrigados por lei a comunicar e se essas informações resultarem numa sanção por infração à [...] [D]iretiva ou ao Regulamento (UE) n.º 537/2014 [(temos dúvidas de como se pode concretizar este incentivo, sem que decorra previamente de um dever legal a denúncia)]. Todavia, os Estados-Membros deverão também garantir que os mecanismos de denúncia aplicados incluam disposições que assegurem a protecção adequada das pessoas denunciadas, sobretudo no que respeita ao direito à protecção dos seus dados pessoais, e a procedimentos que garantam os seus direitos de defesa e de audição antes da adoção de qualquer decisão que lhes diga respeito, bem como ao direito de recurso judicial de tal decisão. Os mecanismos instituídos deverão também assegurar a protecção adequada dos denunciantes, não só no que toca à protecção dos dados pessoais, mas também à garantia de que não sejam vítimas de retaliações indevidas.»

36 Cf. entendido pela alínea 21) do art. 4.º do RGPD «uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 51.º [do mesmo diploma legal]».

37 No seu plano de atividade para o ano de 2017, a CNPD (2017:2) refere que «[n]a verdade o novo regime jurídico altera radicalmente a matriz da atividade de supervisão dos tratamentos de dados, com a transformação da função de controlo prévio numa tarefa excecional, que será substituída pela função de orientação, passando o essencial da intervenção da CNPD a centrar-se na fiscalização e aplicação de sanções. Com evidentes consequências em três planos: organizacional, o procedimental e substancial ou material.» Nestes termos, presumimos que a CNPD está convicta na sua continuidade pós RGPD, ainda que com radicais alterações. Cremos que o seu *know-how*, insubstituível por si só, justifica a sua manutenção, ainda que com nova "roupagem".

38 Poderá ser esta uma boa oportunidade do legislador nacional pôr fim a alguns diferendos entre a CNPD e a CADA, tais como os manifestados na Deliberação n.º 241/2014, da CNPD, de 28 de janeiro, não obstante o legislador comunitário admitir a coexistência de mais do que uma autoridade pública independente, responsável pela fiscalização da aplicação da protecção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (cf. capítulo VI do RGPD).

39 *WeMove.EU*, um movimento de cidadãos, que têm como missão zelar por uma União Europeia comprometida com a justiça social e económica, a sustentabilidade ambiental e a democracia liderada pelos cidadãos, refere que apenas cinco Estados-Membros da UE deram protecção específica aos *whistleblowers*. Por isso, fazendo alusão ao caso *LuxLeaks*, peticionam a existência de uma lei a nível da UE que proteja os denunciante.

40 Ainda que respeitando a particularidade de cada Estado-Membro, cf. considerando 10 do RGPD.

41 Tradução livre do autor. No original: «[t]he disclosure by a person, usually an employee in a government agency or private enterprise, to the public or to those in authority, of mismanagement, corruption, illegality, or some other wrongdoing.»

42 Tradução livre do autor. No original: «A whistleblower is generally defined as an employee who discloses potentially damaging information about their employer to an authority figure, such as their boss, the media, or a government official.»

43 Moeller (2009:549) diz que «[t]he whole concept behind these programs is that any employee or other stakeholder who observes some work environment matter that is wrong and independently "blow the whistle", or report the matter to senior management, without any fear of recrimination.»

44 Tradução livre do autor. No original: «[o]nly if internal disclosure fails should there be disclosure to external agencies, entities or regulators.»

45 Isto é, desde clientes, utilizadores de informação (consultores, intermediários, trabalhadores) e investidores (sócios ou acionistas), passando por "concorrentes", fornecedores, até entidades reguladoras ou fiscalizadoras.

46 Tradução livre do autor. No original: «[c]laims are likely to be of three types. The type that is most often assumed in the literature involves the reporting of wrongdoing that is accurately perceived by the whistleblower. At least two other types of claims, however, are likely to manifest themselves. One type of invalid complaint arises when he whistleblower's action is grounded in erroneous perceptions or incomplete information about an activity. another, more serious, instance involves whistleblowing grounded in opportunistic self-interest, where the whistleblower fabricates a problem for self-protection or gain.»

47 Tradução livre do autor. No original: Park [et al.] (2008:4) «Identified versus anonymous: Identified whistleblowing is an employee's reporting of a wrongdoing using his or her real name (or in some other form giving information which might identify him or her) whereas in anonymous whistleblowing the employee gives no information about himself or herself, and may use an assumed name.»

48 O Parecer do Grupo do Artigo 29.º diz que «[o] anonimato pode não ser a solução adequada, tanto para o denunciante como para a organização, por várias razões: - o anonimato não impede que se venha a identificar o denunciante; - a impossibilidade de prosseguir abertamente o inquérito dificulta a investigação; - é mais fácil organizar a protecção do denunciante contra retaliações, especialmente se a protecção estiver prevista na lei, se as preocupações forem levantadas abertamente; - as denúncias anónimas podem levar a concentrar a atenção no denunciante e pensar que este agiu de má-fé; - a organização corre o risco de desenvolver uma cultura da denúncia anónima e malevolente; - o clima social na organização pode deteriorar-se se os trabalhadores souberem que podem ser denunciados anonimamente em qualquer altura através do sistema previsto para o efeito. No que toca às regras de protecção de dados, as denúncias anónimas levantam um problema específico quanto ao requisito essencial segundo o qual os dados pessoais só devem ser recolhidos lealmente. Regra geral, o Grupo de Trabalho considera que só as denúncias identificadas deveriam ser comunicadas pelo sistema para poderem respeitar este requisito. Contudo, o Grupo de Trabalho sabe que algumas pessoas não terão condições para apresentar denúncias identificadas ou não estarão predispostas a isso. Sabe ainda que as denúncias anónimas são uma realidade que existe, sobretudo e especialmente quando não existem sistemas organizados de denúncia, e que essa realidade não pode ser ignorada. Assim, o Grupo de Trabalho considera que os sistemas de denúncia podem aceitar receber informações anónimas e tomar medidas em consequência, mas como excepção à regra e quando estejam reunidas determinadas condições.»

49 Cf. n.º 3 do art. 10.º da LPDP.

50 Como refere a Deliberação da CNPD, «[r]elacionado com a tutela jurídica do denunciado, sempre cumprirá, todavia, não escamotear os direitos gerais que lhe assiste, nomeadamente, a defesa do seu bom nome e privacidade e, em particular, o direito de apresentar queixa por crime de denúncia caluniosa, nos termos previstos e punidos no artigo

51 Tais como as vertidas nos arts. 420.º-A; 422.º, n.º 3 do CSC para os ROC; ou mesmo 423.º-G, n.º 3 do CSC para o presidente da Comissão de Auditoria.

52 Talvez a situação mais evidente seja a do auditor forense. Roque (s.d.:15) recorda «[s]e, num primeiro momento, a investigação da fraude era uma actividade que estava essencialmente reservada às polícias e entidades oficiais de investigação, nos últimos anos tem vindo a crescer e a ganhar importância a investigação da fraude por entidades privadas, os auditores forenses. Quando um auditor forense é chamado a intervir num processo de fraude, procede à investigação da fraude, de forma independente, com vista ao apuramento dos factos e, consequentemente, da prova.»

53 Tais como os previstos no capítulo 2, secção 3, § 2.3.5 e secção 7; e capítulo 3, secção 3 do CEOROC.

54 As tarefas a desenvolver pela Auditoria Interna podem incluir a monitorização dos sistemas de controlo interno identificando falhas ou desvios potenciais (analisar a sua operacionalidade: adequação, integridade, custos e segurança), examinar a informação financeira e operacional (determinar a eficácia dos meios usados para a identificar, mensurar, classificar e relatar), rever as operações do ponto de vista da economia, eficácia e eficiência (incluindo as actividades não financeiras) e verificar o cumprimento de regras e de políticas estabelecidas. Um auditor interno é, por inerência, salvo quando se trata de prestação de serviços de auditoria interna por uma entidade externa, um operacional (um trabalhador no terreno) – on the job, o que lhe confere uma posição única no seio da organização, por ser conhecedor, tanto da envolvente geral, como da específica (inerente a cada departamento ou área). Por sua vez, no que concerne à

função de auditoria interna esta deve estar inserida organicamente num lugar de topo da organização, ser independente de todos os outros departamentos, áreas ou setores, mas capaz de construir canais de comunicação entre elas e funcionar como apoio à gestão, reportando (conformidades e não conformidades), preferencialmente, a uma superestrutura consultiva (por exemplo, um órgão consultivo de supervisão constituído por todos os dirigentes, designado por Conselho Geral de Supervisão ou Comissão ou Comité de Auditoria) ou ao cargo mais elevado da organização.

55 Ele não deve ser encarado apenas e só como uma comunicação, mas sim como um conjunto de operações que envolve a análise e ponderação de juízos de valor sobre as consequências da denúncia, e esta propriamente dita.

56 O Whistleblowing pode ser entendido como um mecanismo preventivo e de controlo interno, de deteção de erros e, ou, irregularidades (mitigando e, ou, reprimindo irregularidades).

57 Recorde-se que a Auditoria Forense é aquela que, como Costa (2014:124) sintetiza, «[...]pretende detectar possíveis fraudes [...] confirmando não apenas o que está contabilizado, apresentado e divulgado nas demonstrações financeiras mas tentado, sobretudo, detectar o que não está evidenciado nestes documentos e que devia estar. É pois um verdadeiro trabalho de investigação ou de peritagem altamente especializado [...].»

58 A Auditoria Interna deve ser entendida como uma atividade independente que acrescenta valor às operações de uma determinada organização, auxiliando-a proativamente na monitorização e realização dos seus objetivos, a partir de uma abordagem sistemática (regrada e planeada) e sistémica (multidisciplinar). Como forma de credibilizar as atividades desenvolvidas, melhorar a performance dos recursos financeiros, humanos e materiais, bem como a gestão de riscos e o controlo interno, a Auditoria Interna deve posicionar-se, organicamente, ao mais alto nível e assumir um papel preponderante (muitas vezes de conselheira privilegiada por pertencer "ao terreno").

59 A transferência de dados pessoais para fora da UE deve respeitar os arts. 19.º e 20.º da LPDP, bem como, desde já se sabe, por estarem em vigor, os arts. 44.º a 50.º do RGPD. A CNPD continua a manifestar, através das suas autorizações (por exemplo a n.º 2717/2017, de 7 de março), que não está em condições de decidir de forma definitiva sobre a transferência de dados pessoais para o território 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 (no qual o austríaco Maximilian Schrems moveu uma acção de reenvio prejudicial, junto do Tribunal de Justiça Europeu – que permite a uma jurisdição nacional interrogar o Tribunal Europeu sobre a interpretação ou a validade do direito europeu, garantindo assim a segurança jurídica através de uma aplicação uniforme do direito da União Europeia –, contra a Data Protection Commissioner, sendo interveniente a Digital Rights Ireland Ltd., por aquela não ter investigado a sua queixa contra a filial do Facebook na Irlanda, por esta violar as leis de protecção de dados europeus), 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 supostamente garantiam a privacidade e a segurança de que as entidades norte-americanas respeitavam as informações pessoais dos cidadãos da UE e Suíça, aquando de fluxos de dados transatlânticos designados por «Porto Seguro», ou mais conhecidos 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 sobrepõe de modo desnecessário e desproporcionado às cláusulas contratuais (cláusulas contratuais-tipo, contratos entre empresas do mesmo grupo – acordos intragrupo – ou outros contratos ad-hoc) adequadas que o responsável e os destinatários da informação subscrevem, apenas emite autorizações provisórias (cf. seu comunicado de 23/10/2015, in [https://www.cnpd.pt/bin/relacoes/comunicados/Comunicado\\_CNPD\\_SafeHarbor.pdf](https://www.cnpd.pt/bin/relacoes/comunicados/Comunicado_CNPD_SafeHarbor.pdf)).

60 Atente-se que num culto de integridade, transparência e consideração, não obstante a sua intrínseca independência (que lhe dá jus ao nome), o auditor interno deverá sempre informar ao(s) órgão(s) de gestão ou ao seu superior hierárquico, como por exemplo o Presidente da organização (se não for o visado), que irá proceder a uma denúncia externa.

## REFERÊNCIAS BIBLIOGRÁFICAS

- BANCO de Portugal (s.d). [Em linha]. [Consult. 13 set. 2018]. Disponível em: <https://www.bportugal.pt/comunicado/revogacao-da-autorizacao-do-bpp-sa>.
- BANISAR, David – *Whistleblowing: International Standards and Developments* [Em linha]. (2006). [Consult. 25 set. 2018]. Disponível em: [http://www.corruption.unam.mx/documentos/investigaciones/banisar\\_paper.pdf](http://www.corruption.unam.mx/documentos/investigaciones/banisar_paper.pdf).
- BARBOSA, Carmencita – *Mecanismo de Whistleblowing nas organizações: o caso das empresas cotadas na Euro Next Lisboa*. Lisboa: Instituto Superior de Contabilidade e Administração de Lisboa do Instituto Politécnico de Lisboa. 2012. Dissertação de Mestrado.
- BERRY, Benisa - Organizational Culture: A Framework and Strategies for Facilitating Employee Whistleblowing. In *Employee Responsibilities and Rights Journal*. 2004. ISSN 0892-7545 p. 1.
- CARRIGY, Celina – *Denúncia de Irregularidades no Seio das Empresas (Corporate Whistleblowing)* [Em linha]. (2005) [Consult. 27 abr. 2018] Disponível em: <http://www.cmvvm.pt/pt/EstatisticasEstudosEPublicacoes/CadernosDoMercadoDeValoresMobiliarios/Documentos/7c55e782cd6743fbb2320e72021a6335CelinaCarrigy.pdf>.

COLAÇO, Luísa; ARAÚJO, Maria da Luz – *Regras de Legística a Observar na Elaboração de Actos Normativos da Assembleia da República*. Edição: Divisão de Edições da Assembleia da República. Lisboa, outubro de 2008. ISBN: 978-972-556-499-8.

COMISSÃO do Mercado de Valores Mobiliários [Em linha]. [Consult. 15 jan. 2018]. Disponível em: [http://www.cmvv.pt/pt/EstatisticasEstudosEPublicacoes/EstudosEWorkingPapers/Pages/20061023\\_inq6\\_3\\_3.13.aspx](http://www.cmvv.pt/pt/EstatisticasEstudosEPublicacoes/EstudosEWorkingPapers/Pages/20061023_inq6_3_3.13.aspx).

COMISSÃO Nacional de Protecção de Dados – *10 Medidas para preparar a aplicação do Regulamento Europeu de Protecção de Dados*. [Em linha]. [Consult. 27 jun. 2018]. Disponível em: [https://www.cnpd.pt/bin/rgpd/10\\_Medidas\\_para\\_preparar\\_RGPD\\_CNPD.pdf](https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf).

COMISSÃO Nacional de Protecção de Dados – *Plano de atividades CNPD 2016*. Lisboa. Comissão Nacional de Protecção de Dados. [Em linha]. [Consult. 20 mai. 2018]. Disponível em: [https://www.cnpd.pt/bin/Docs\\_news/PLANO\\_ACTIVIDADES\\_2016.pdf](https://www.cnpd.pt/bin/Docs_news/PLANO_ACTIVIDADES_2016.pdf).

COMISSÃO Nacional de Protecção de Dados – *Plano de atividades CNPD 2017*. Lisboa. Comissão Nacional de Protecção de Dados. [Em linha]. [Consult. 20 Mai. 2018]. Disponível em: [https://www.cnpd.pt/bin/cnpd/planos/PLANO\\_ACTIVIDADES\\_2017.pdf](https://www.cnpd.pt/bin/cnpd/planos/PLANO_ACTIVIDADES_2017.pdf).

COMISSÃO Nacional de Protecção de Dados – *Relatório de atividades da Comissão Nacional de Protecção de Dados 2009*. Lisboa. CNPD [Em linha]. [Consult. 20 mai. 2018]. Disponível em: <https://www.cnpd.pt/bin/relatorios/anos/relat2009.pdf>.

COSTA, Carlos Baptista – *Auditoria Financeira*. 10ª Ed. Lisboa: Reis dos Livros, 2014. ISBN: 978-989-8305-64-0.

DEPARTAMENTO Central de Investigação Penal, do Ministério Público (s.d.). [Em linha]. [Consult. 13 set. 2018]. Disponível em: <https://simp.pgr.pt/dciap/denuncias/index2.php>.

INTER-ACTIVE Terminology for Europe (s.d.) [Consult. 15 jan. 2018]. Disponível em <http://iate.europa.eu/FindTermsByLilId.do?lilId=2201493&langId=pt>.

JUBB, Peter B. – Auditors as Whistleblowers. In *International Journal of Auditing*. 2000. ISSN 51090-6738. 4 pp. 153-167.

JUBB, Peter B. – Whistleblowing: A Restrictive Definition and Interpretation. In *Journal of Business Ethics*. 1999. Pp 77-94.

KRANACHER, Mary-Jo – *The Devil Is in the Details* [Em linha]. 2006. [Consult. 26 fev. 2018]. Disponível em <http://www.nysscpa.org/cpajournal/2006/706/essentials/p80.htm>.

LATIMER, Paul; BROWN, J. – *Whistleblower Laws: International Best Practice*. [Em linha]. (2008). [Consult. 20 fev. 2018]. Disponível em <http://www.austlii.edu.au/au/journals/UNSWLJ/2008/40.pdf>.

LAVENA, Cecilia Florencia – Whistle-Blowing: Individual and Organizational Determinants of the Decision to Report Wrongdoing in the Federal Government. In *The American Review of Public Administration*. 2014. Pp. 1-24.

LOPES, Joaquim de Seabra – O artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível. *Forum de Protecção de Dados*. N.º 2, Editor Comissão Nacional de Protecção de Dados, janeiro de 2016. ISSN 2183-5977 p. 42.

MOELLER, Robert R., *Brink's Modern Internal Auditing – A Common Body of Knowledge* – John Wiley & Sons, Inc., Hoboken, 7ª Ed., 2009, New Jersey.

OBSERVATÓRIO sobre Crises e Alternativas (s.d.) [Em linha]. [Consult. 13 set. 2018]. Disponível em: <http://www.ces.uc.pt/observatorios/crisalt/cronologia.php>.

PARK, Heungsik; BLENKINSOPP, John; OKTEM, Kemal M.; OMURGONULSEN, Ugur - *Cultural Orientation and Attitudes Toward Different Forms of Whistleblowing: A Comparison of South Korea, Turkey, and the U.K.* *Journal of Business Ethics*. ISSN 10551-007-9603-1. 82 (2008) 929-939.

PERRY, James L. – "Whistleblowing, Organizational Performance, and Organizational Control". In *Ethics and Public Administration with a forewords*, Editor H. George Frederickson; 1993 pp. 73-99. Armonk, NY: M.E. Sharpe.

ROQUE, Pedro – *Auditor Forense – Contributo para a definição de uma nova profissão em Portugal*. [Em linha]. (s.d) [Consult. 27 abr. 2018] Disponível em: <https://www.occ.pt/news/comcontabaudit/pdf/128.pdf>.

SCHMIDT, Matthias (s.d.) "Whistle Blowing" Regulation and Accounting Standards Enforcement in Germany and Europe – an Economic Perspective, cit.

SIMÕES, Bruno; LARGUESA, António, – *Combate à corrupção deve passar pela delação? Jornal de Negócios*. (abr. 2010). [Em linha]. [Consult. 15 jan. 2018]. Disponível em: [http://www.migts.pt/xms/files/Comunicacao/Imprensa/2010/o\\_papel\\_da\\_delacao\\_no\\_combate\\_a\\_corupcao.pdf](http://www.migts.pt/xms/files/Comunicacao/Imprensa/2010/o_papel_da_delacao_no_combate_a_corupcao.pdf).

SIMÕES, Bruno; LARGUESA, António, Sindicato dos Magistrados do Ministério Público – *JNEG - "Bufos"? Nem para o combate à corrupção servem*. (2010) [Em linha]. [Consult. 15 jan. 2018]. Disponível em: <http://www.smp.pt/?p=8088>.

SMITH, Rodney – The Role of Whistle-Blowing in Governing Wel: Evidence From the Australian Public Sector. In *The American Review of Public Administration*. 2010. Pp. 704-721.

SOUZA, Marcelo Rebelo de; e MATOS, André Salgado de Matos – *Direito Administrativo Geral – Tomo III, Dom Quixote*, Reimpressão da 2ª edição, julho de 2010, ISBN: 978-972-20-3879-9.

THE FREE DICTIONARY by Farlex – (s.d.) [Em linha] [Consult. 15 Jul. 2018]. Disponível em: <http://www.thefreedictionary.com/whistle-blowing>.

VINTEN, Gerald – Whistleblowing: the UK experience. Part 1. In *Management Decision* Vol. 41. 2003. Pp. 935-943.

## DOCUMENTOS NORMATIVOS

Comunicação da Comissão – concluir o mandato da reforma: relatório intercalar e medidas a aplicar em 2004, Comissão das Comunidades Europeias, Bruxelas, de 10 de fevereiro de 2004.

Decisão 2005/909/CE da Comissão, de 14 de dezembro.

Decreto-Lei n.º 47344, de 25 de novembro de 1966 (e as suas sucessivas alterações) – diploma legal que aprovou o Código Civil.

Decreto-Lei n.º 262/86, de 2 de setembro (e as suas sucessivas alterações) – diploma legal que aprovou o Código das Sociedades Comerciais.

Decreto-Lei n.º 166/98, de 25 de junho.

Deliberação n.º 765/2009, da CNPD, aprovada em 21 de setembro.

Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro.

Diretiva 2006/43/CE, do Parlamento Europeu e do Conselho, de 17 de maio.

Diretiva 2014/56/UE, do Parlamento Europeu e do Conselho, de 16 de abril.

*International Standard on Auditing* 240 (Clarificada) – As Responsabilidades do Auditor Relativas a Fraude numa Auditoria de Demonstrações Financeiras.

*International Standard on Auditing* 315 (Clarificada) – Identificar e Avaliar os Riscos de Distorção por Meio da Compreensão da Entidade e do Seu Ambiente.

Parecer n.º 1/2006, do Grupo de Protecção de Dados do Artigo 29º, adoptado em 1 fevereiro de 2006 – [Em linha]. [Consult. 13 set. 2018]. Disponível em: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117\\_pt.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_pt.pdf).

Recomendação 10-A, de novembro de 2005, da CMVM.

Regulamento (UE) n.º 537/2014, do Parlamento Europeu e do Conselho, de 16 de abril de 2014.

Regulamento (UE) 2016/679, do Parlamento Europeu do Conselho, de 27 de abril de 2016.



**SIPTA**  
Sistema Informático de Papéis de Trabalho de Auditoria

Português

## O SOFTWARE DE AUDITORIA

**A auditoria pode agora ser efetuada de forma mais simples, mais rigorosa, mais rápida e mais eficaz!**

Com o SIPTA, promova a:

- ✓ Produtividade das suas equipas
- ✓ Eficiência e eficácia dos processos

Cumprindo com as ISAs (Normas Internacionais de Auditoria), utilize processos automatizados:

- ✓ Planeamento
- ✓ Programas de trabalho
- ✓ Amostragem estatística
- ✓ Análises substantivas e de conformidade
- ✓ Circularização
- ✓ Demonstrações financeiras
- ✓ e outros...

Descubra mais as potencialidades que temos para lhe oferecer em [www.sipta.pt](http://www.sipta.pt) e solicite já a sua apresentação.

[www.sipta.pt](http://www.sipta.pt)  [geral@sipta.pt](mailto:geral@sipta.pt)  
☎ 239 918 214 • 962 466 048 • 964 197 617

**WIS4**  
Web Integrated Systems, Lda

Em parceria com:  DOGNÆDIS A PRODUCER COMPANY 