



Universitat Autònoma de Barcelona

**ADVERTIMENT.** L'accés als continguts d'aquesta tesi queda condicionat a l'acceptació de les condicions d'ús establertes per la següent llicència Creative Commons:  [http://cat.creativecommons.org/?page\\_id=184](http://cat.creativecommons.org/?page_id=184)

**ADVERTENCIA.** El acceso a los contenidos de esta tesis queda condicionado a la aceptación de las condiciones de uso establecidas por la siguiente licencia Creative Commons:  <http://es.creativecommons.org/blog/licencias/>

**WARNING.** The access to the contents of this doctoral thesis it is limited to the acceptance of the use conditions set by the following Creative Commons license:  <https://creativecommons.org/licenses/?lang=en>



**Universitat Autònoma  
de Barcelona**

Programa de Doctorado en Derecho Público Global

TESIS DOCTORAL

**El Canal de Denuncias Internas en la Actividad Empresarial como  
Instrumento del *Compliance***

Autor: Rosa Espín

Director: Manuel Ballbé

Junio 2017

A mi padre, de quien he aprendido el valor del esfuerzo.

I.	INTRODUCCIÓN.....	13
II.	EL FENÓMENO DEL COMPLIANCE Y LA LUCHA CONTRA LA CORRUPCIÓN .....	19
1.	El fenómeno del Compliance.....	19
1.1	El Compliance y el Buen Gobierno Corporativo .....	26
1.2	El Compliance y la Responsabilidad Social Corporativa.....	30
1.3	El Compliance y la Ética Empresarial.....	35
2.	Directrices internacionales contra la corrupción en el comercio internacional .....	36
2.1	Convención contra el Soborno de la OCDE .....	39
2.2	Recomendación OCDE para fortalecer la lucha contra el cohecho .....	41
2.3	Principios Empresariales para contrarrestar el Soborno, de Transparencia Internacional (TI) .....	42
2.4	Principios Partnering Against Corruption Initiative .....	44
2.5	Convención de las Naciones Unidas contra la Corrupción .....	45
2.6	Reglas de conducta y recomendaciones de la CCI para combatir la extorsión y el soborno .....	45
2.7	Manual de Directrices de la US Sentencing Commission .....	46
2.8	Breve apunte sobre la normativa internacional de compliance en el sector financiero .....	49
	2.8.1 En Estados Unidos .....	49
	2.8.2 En Europa .....	55
III.	PROGRAMAS DE CUMPLIMIENTO.....	61
1.	Definición y Objetivo.....	61
2.	Características y contenido esencial .....	68
2.1	El carácter abierto y dinámico de los programas de cumplimiento.....	68
	2.1.1 El fomento de una cultura organizacional tendiente al cumplimiento de la ley.....	70
	2.1.2 El control y la administración del riesgo .....	74

2.2	Involucración de la alta dirección de la empresa en labores de supervisión y control, y delegación adecuada de funciones de vigilancia.....	76
2.3	Comunicación y formación continua de los integrantes de la empresa.....	80
2.4	Adopción de mecanismos de monitorización y evaluación del programa.....	82
2.5	Sistemas de reporte o denuncia interna.....	84
2.6	Adopción de mecanismos disciplinarios y de incentivos internos.....	85
2.7	Reacción adecuada y actualización permanente del modelo .....	86
3.	Naturaleza y eficacia jurídico-laboral de los programas de cumplimiento .....	87
4.	El cumplimiento normativo en ordenamientos de sociedades especiales.....	90
4.1	El gobierno corporativo, el cumplimiento normativo y el canal de denuncia en la regulación de las sociedades cotizadas.....	90
4.2	El cumplimiento normativo en el ordenamiento de las entidades de crédito .....	96
4.3	El cumplimiento normativo en la regulación de las entidades aseguradoras .....	100
4.4	El cumplimiento normativo en la regulación de las empresas de servicios de inversión.....	106
IV.	EL WHISTLEBLOWING .....	109
1.	Antecedentes y desarrollo histórico del whistleblowing .....	109
1.1	Antecedentes.....	109
1.2	Evolución de la concepción del whistleblower en EEUU.....	110
1.2.1	El whistleblower como caza - recompensas.....	110
1.2.2	El whistleblower como <i>ethical resister</i> .....	111

1.2.3	La era compliance: el whistleblower en el sector privado .....	113
1.3	La importancia del whistleblowing en los escándalos financieros más importantes del último siglo .....	116
2.	El whistleblowing en el Derecho comparado.....	126
2.1	El whistleblowing en el Derecho Internacional .....	126
2.2	El whistleblowing en Estados Unidos .....	128
2.2.1	Breve repaso a la legislación Estadounidense .....	128
2.2.1.1	False Claim Act.....	131
2.2.1.2	La Foreign Corrupt Practices Act (FCPA). 134	
2.2.1.3	Whistleblowers Protection Act (WPA).....	135
2.2.1.4	Códigos Éticos .....	137
2.2.1.5	Sarbanes-Oxley Act 2002 .....	138
2.2.1.6	Dodd-Frank Wall Street Reform and Consumer Protection Act.....	139
2.3	El whistleblowing en la Unión Europea y en la normativa nacional europea .....	149
2.3.1	Unión Europea. Grupo de Trabajo Directiva 95/46/CE .....	149
2.3.2	Normativa en el Reino Unido: la Public Interest Disclosure Act .....	156
2.3.3	Referencia a Francia (Especial referencia a la <i>Commission Nationale de l'informatique des libertes</i> ) 164	
2.3.4	Alemania .....	165
3.	El whistleblowing en el ordenamiento jurídico español .....	165
3.1	Consideraciones generales .....	165
3.2	En la actividad empresarial.....	166
3.2.1	La legislación penal .....	166

3.2.2	Protección de Datos: La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales .....	176
3.2.3	Transparencia: La Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno .....	178
3.2.4	El Mercado de Valores: la notificación de infracciones en las empresas de servicios de inversión (art. 197 TRLMV).....	179
3.2.5	Blanqueo de capitales. Ley 10/2010, de 28 de abril, de Prevención y Blanqueo de Capitales y de la Financiación del Terrorismo.....	180
3.2.6	Defensa de la Competencia. Programas de Clemencia .....	190
3.2.7	Ámbito societario en los Códigos de Buen gobierno .....	193
3.2.8	Derecho Nuclear .....	197
4.	Figuras similares en el sector financiero: los servicios de atención al cliente de las entidades y los servicios de reclamaciones de los organismos reguladores .....	201
5.	Concepto y Naturaleza del whistleblowing y el whistleblower.....	210
V.	LAS DENUNCIAS INTERNAS COMO MANIFESTACIÓN DEL WHISTLEBLOWING.....	216
1.	Las denuncias internas y la responsabilidad penal.....	217
2.	Las denuncias internas y los derechos de los empleados.....	221
2.1	Derecho a la intimidad y la protección de datos.....	222
2.2	Obligación de información previa .....	228
2.3	Protección al denunciante frente a un despido .....	230
2.4	Derecho a fiscalizar a un trabajador .....	232
2.5	La interpretación del deber de denunciar .....	235
3.	El alcance de los procedimientos de denuncia de irregularidades .....	240

4.	Condiciones de eficacia del sistema interno de denuncia.....	243
VI.	EL CANAL INTERNO DE DENUNCIAS.....	249
1.	Consideraciones generales .....	249
2.	Características.....	253
2.1	Consideraciones generales .....	253
2.1.1	Sistema respaldado por la dirección.....	253
2.1.2	Sistema previamente divulgado y que cumpla con la obligación de información.....	254
2.1.3	Sistema fácilmente accesible.....	255
2.1.4	Sistema proporcional .....	256
2.1.5	Sistema documentado .....	257
2.1.6	Sistema en el que los comportamientos irregulares estén expresamente detallados, así como las consecuencias de su incumplimiento.....	257
2.1.7	Sistema que garantice que no habrá represalias para el denunciante.....	258
2.2	Confidencialidad y la protección de datos .....	259
2.2.1	Deberes y derechos de las partes .....	266
2.2.2	Deber de calidad de los datos. Plazos de conservación de la información relacionada con la denuncia.....	271
2.2.3	Derechos de acceso, rectificación, cancelación y oposición (ARCO) .....	273
2.2.4	Sanciones por incumplimiento .....	274
2.2.5	Medidas de seguridad a implantar en el canal de denuncia interna .....	275
2.3	Aceptación de las normas y política de privacidad.....	280
2.4	Ausencia de represalias .....	281
2.4.1	Protección por el Derecho constitucional y laboral .....	282
2.4.2	Protección por el Derecho penal.....	284



2.4.3	Programas de amnistía y otros incentivos.....	286
2.5	Voluntariedad vs. Obligatoriedad.....	288
3.	Delimitación del ámbito del canal de denuncia .....	293
3.1	Delimitación del ámbito material.....	293
3.2	Delimitación del ámbito subjetivo .....	296
3.2.1	Legitimación activa .....	296
3.2.2	Legitimación pasiva .....	302
3.3	Delimitación del ámbito territorial.....	302
4.	Organización .....	303
4.1	Cuestiones básicas.....	303
4.2	Figuras implicadas.....	311
4.3	Ejemplos prácticos de sociedades cotizadas españolas.....	313
5.	Procedimiento.....	321
5.1	Consideraciones generales .....	321
5.2	Procedimiento de denuncia e investigación interna .....	322
6.	Gestión del canal de denuncias internas en un grupo empresarial ....	356
7.	Reacciones de la empresa ante el resultado de la investigación.....	359
VII.	CONCLUSIONES.....	364

## BIBLIOGRAFÍA

## ABREVIATURAS

AA.M.N.	Anales de la Academia Matritense del Notariado
AA.VV.	Autores varios
AD.Con.	Anuario de Derecho Concursal
ADC	Anuario de Derecho Civil
Ant.	Anteproyecto
Apdo.	Apartado
Art.	Artículo
BOCG	Boletín Oficial de las Cortes Generales
BOE	Boletín Oficial de Estado
BORME	Boletín Oficial del Registro Mercantil
C. de c.	Código de Comercio
CBG	Código de buen gobierno de las sociedades cotizadas
CC	Código Civil
CCJC	Cuadernos Cívitas de Jurisprudencia Civil
CD y Com.	Cuadernos de Derecho y Comercio
CDJ	Cuadernos de Derecho Judicial
CE	Constitución Española de 1978
CEE	Comunidad Económica Europea
CNMV	Comisión Nacional del Mercado de Valores
Coord./s	Coordinador/es
CP	LO 10/1995, de 23 de noviembre, del Código Penal
CSPL	Committee on Standards in Public Life
DGRN	Dirección General de los Registros y del Notariado
DGS y FP	Dirección General de seguros y fondos de pensiones
dir./s.	Director/es
disp. ad.	Disposición adicional
disp. de.	Disposición derogatoria
disp. f.	Disposición final
disp. t.	Disposición transitoria

DOCE	Diario Oficial de las Comunidades Europeas
ed.	Edición
edit./s.	Editorial/es
ERA	Employment Rights Act
esp.	Especialmente
ET	Ley 8/1980, de 10 de marzo, del Estatuto de los Trabajadores
Exp. Mot.	Exposición de Motivos
FCPA	Foreign Corrupt Practices Act
ICAC	Instituto de Contabilidad y Auditoría de Cuentas
LAC	Ley 22/2015, de 22 de julio, de Auditoría de Cuentas
LDC	Ley 15/2007, de 3 de julio, de Defensa de la Competencia
LEC	Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil
LO	Ley Orgánica
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
LOSSEAR	Ley 20/2015, de 14 de junio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras
LOSSEC	Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito
LPACAP	Ley 39/2015, de 26 de noviembre, del Procedimiento Administrativo Común de las Administraciones Públicas
LPBC	Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo
LPRL	Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales
LSRL	Ley 2/1995, de 23 de marzo, de Sociedades de Responsabilidad Limitada
nº	Número
ob. cit.	Obra citada

OM	Orden Ministerial
p./ pp.	Página/s
PIDA	Public Interest Disclosure Act 1998
RD	Real Decreto
RDBB	Revista de Derecho Bancario y Bursátil
RDLeg	Real Decreto Legislativo
RDL	Real Decreto Ley
RDM	Revista de Derecho Mercantil
RDN	Revista de Derecho Notarial
RDP	Revista de Derecho Privado
RdS	Revista de Derecho de Sociedades
RJ	Repertorio de Jurisprudencia Aranzadi
RLOPD	Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre aprobado por Real Decreto 1720/2007, de 21 de diciembre
RM	Registro Mercantil
ROSSEAR	Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras
ROSSEC	Real Decreto 84/2015, de 13 de febrero, por el que se desarrolla la Ley 10/2014, de 26 de junio de ordenación, supervisión y solvencia de entidades de crédito
RPBC	Reglamento de la Ley 10/2010, de 28 de abril de 2010, de prevención del blanqueo de capitales y de la financiación del terrorismo, aprobado por Real Decreto 304/2014, de 5 de mayo
RRM	Reglamento del Registro Mercantil, aprobado por RD 1784/1996, de 19 de julio
RSC	Responsabilidad Social Corporativa
S.A.	Sociedad Anónima

SEPBLAC	Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias
S.R.L.	Sociedad de Responsabilidad Limitada
SEC	Securities Exchange Commission
ss.	Siguientes
STC	Sentencia del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
T.	Tomo
TC	Tribunal Constitucional
TRLET	Texto refundido de la Ley del Estatuto de los Trabajadores aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre
TRLMV	Texto refundido de la Ley de Mercado de Valores aprobado por Real Decreto Legislativo 4/2015, de 23 de octubre
TRLSC	Texto refundido de la Ley de Sociedades de Capital aprobado por Real Decreto Legislativo 1/2010 de 2 de julio
TS	Tribunal Supremo
U.E.	Unión Europea
Vid.	Véase
vol.	Volumen

## I. INTRODUCCIÓN

Esta investigación tiene como principal propósito estudiar el canal de denuncias internas en la actividad empresarial. La implantación de tal canal es de candente actualidad en España desde Julio de 2015 con la introducción en el ordenamiento jurídico español del deber de contar con un programa de cumplimiento efectivo como uno de los requisitos que posibilitan atenuar o eximir a las personas jurídicas de una eventual responsabilidad penal.

Una primera aproximación a este tema pone en evidencia una contraposición de valoraciones y sentimientos hacia esta clase de instituciones en nuestra sociedad; por un lado, se reconoce su eficacia pero por otro, con cierta habitualidad la figura del denunciante no siempre es siempre adecuadamente valorada. Esta figura de procedencia anglosajona, tradicionalmente no ha sido apreciada moralmente en las culturas latinas, sin embargo el *whistleblower* es uno de los métodos más eficaces para descubrir irregularidades, conductas contrarias al código ético de conducta de la empresa y delitos, especialmente los relativos a corrupción, fraude y blanqueo de capitales. Esta acción de denuncia puede llegar a salvar vidas, a descubrir fraudes en todo tipo de empresas, evita la destrucción de la empresa y de puestos de trabajo, la pérdida del dinero de los inversores, protege la salud de los ciudadanos y el medioambiente. Tienen un fin que es prevenir, evitar, descubrir y actuar frente a los fraudes empresariales y la corrupción nacional e internacional.

Es imposible comprender el origen del compliance sin analizar la obra visionaria de M. BALLBÉ<sup>1</sup> en la que se analiza la globalización jurídica y especialmente la americanización administrativa y reguladora. En ella M. BALLBÉ repasa el modelo norteamericano de Estado administrativo y

---

<sup>1</sup>BALLBÉ, M./ MARTÍNEZ, R., "Law and Globalization: Between the United States and Europe", en AA.VV., Global Administrative Law. Towards a Lex Administrativa, dirs. J. Robalino- Orellana/ J. Rodríguez- Arana, pp. 137 y ss.

regulador, porque- tal y como él afirma de manera pionera- la Unión Europea y la globalización se inspirarán en él. Este es, exactamente, el embrión del fenómeno del Compliance que actualmente ocupa una piedra angular en nuestros ordenamientos europeos.

Los canales internos de denuncias en las empresas o sistemas o procedimientos de whistleblowing, consisten en la creación de cauces dentro de las empresas por los que resulte posible denunciar internamente irregularidades, infracciones legales y de normas internas (códigos éticos, políticas de prevención contra el fraude, corrupción y blanqueo de capitales, políticas de entrega y recepción de regalos, de uso de los sistemas informáticos, risk management control, etc.) cometidas en su seno o en su ámbito de actuación<sup>2</sup>.

Antes de entrar en el análisis de Whistleblowing o más en concreto del canal de denuncias interno de una empresa, he hecho un análisis del fenómeno del Cumplimiento Normativo o también llamado *Compliance*. En particular, he analizado la relación del Compliance con el Buen Gobierno Corporativo, la Responsabilidad Social Corporativa y la Ética Empresarial.

A lo largo del trabajo he utilizado indistintamente la expresión “Cumplimiento Normativo” y el término “Compliance”, ya que a pesar de que considero que Cumplimiento Normativo es más correcto en nuestro ordenamiento y cultura, no se puede negar la importancia y aceptación del término Compliance. Lo mismo he hecho con los términos “denunciante” y “whistleblower”.

A continuación y siguiendo con el análisis del Compliance, he querido resumir la respuesta internacional que se ha dado al fenómeno de la corrupción en el comercio internacional. Para ello he analizado la Convención contra el Soborno de la OCDE, la Recomendación OCDE para fortalecer la lucha

---

<sup>2</sup>MESIA MARTÍNEZ, C., "El procedimiento de denuncia interna o whistleblowing en los códigos de conducta", en AA.VV., *Gobierno corporativo: La estructura del órgano de gobierno y la responsabilidad de los administradores (Adaptado a la Ley 31/2014, de 3 de diciembre)*, dir. A. Martínez-Echevarría y García de Dueñas, Navarra, 2015, p. 1210.

contra el cohecho, los Principios Empresariales para contrarrestar el Soborno de Transparencia International, los Principios Partnering Against Corruption Initiative, Convención de las Naciones Unidas contra la Corrupción, Reglas de conducta y recomendaciones de la Cámara de Comercio Internacional (CCI) para combatir la extorsión y el soborno, y el Manual de Directrices de la US Sentencing Commission. Por último también he considerado interesante para fijar el contexto del fenómeno de la corrupción y el Compliance hacer un análisis de la normativa internacional de Compliance en el sector financiero.

Una vez investigado sobre lo anterior, he creído necesario analizar el programa de cumplimiento, que es el instrumento donde se inserta el canal de denuncias interno de una compañía. Para ello he investigado sobre sus características y contenido esencial, sobre su naturaleza jurídica y sobre su incidencia en ordenamientos de sociedades especiales como son las sociedades cotizadas, las entidades de crédito, las entidades aseguradoras o las empresas de servicios de inversión.

Para estudiar dicho canal he creído necesario analizar primero el fenómeno del *whistleblowing* en la sociedad para luego analizarlo desde el ámbito interno de una empresa. Para todo ello, es imprescindible analizar el origen y la evolución normativa del *whistleblowing*, especialmente la anglosajona, cultura de la que proviene. Asimismo, he estudiado la importancia del *whistleblowing* en los escándalos financieros más importantes del último siglo.

Las primeras regulaciones de los sistemas de denuncias fueron a través de leyes norteamericanas como la False Claims Act (FCA), Sarbanes-Oxley (SOX) y la Dodd Frank Consumers Act que otorgaban incentivos a los denunciantes (*whistleblowers*) y trataban de garantizar protección frente a represalias del empresario.

Una de las primeras normas que incidió sobre la materia, fue la False Claims Act de 1863 (FCA, conocida como Lincoln Law), que fue aprobada durante la Guerra de Secesión norteamericana para combatir el fraude en los



suministros al ejército de la Unión, y sigue actualmente vigente tras diversas modificaciones, fomentando la denuncia de fraude contra el Gobierno Federal de los Estados Unidos, y regulando un sistema de *Qui tam action*<sup>3</sup>, en virtud del cual el denunciante o delator ostenta legitimación para emprender una acción legal en defensa del gobierno. Contempla además como incentivo el derecho a percibir un porcentaje del importe que se consiga recuperar.

La protección legal a los denunciantes, se aborda en dos leyes norteamericanas, la Lloyd-La Follette Act de 1912 y la whistleblower Protection Act de 1989, ambas promulgadas con el fin de blindar laboralmente a los funcionarios que informen sobre irregularidades cometidas en el seno de la Administración.

En la Unión Europea se ha producido recientemente la implantación de los sistemas de cumplimiento normativo y whistleblowing en las empresas cotizadas y de gran dimensión a través del movimiento del Gobierno Corporativo y de las leyes penales nacionales.

A partir de ahí he estudiado el whistleblowing en el ordenamiento jurídico español en sus distintos ámbitos: penal, protección de datos, transparencia y, mercado de valores, blanqueo de capitales y financiación del terrorismo, defensa de la competencia y ámbito societario en los Códigos de Buen Gobierno. Para terminar este bloque de estudio he considerado oportuno hacer una reflexión sobre el concepto del whistleblowing y del whistleblower.

A continuación, he analizado la compatibilidad de los programas de denuncia internos con las normas del empleado, en particular la protección de datos de carácter personal, directamente relacionado con el derecho a la privacidad del denunciante y el denunciado, así como las normas penales, de defensa de la

---

<sup>3</sup>*Qui tam* es la abreviatura de la frase *Qui tam pro domino rege quam pro se ipso in haec parte sequitur* cuya traducción puede ser, “quien presenta la acción al rey también la presenta para su propia causa”. Una “acción qui tam”, es aquella demanda iniciada por un ciudadano denunciado por un desvío o utilización incorrecta de fondos públicos, por la cual el denunciante adquiere un derecho a reclamar un porcentaje del dinero que el Estado recupere si prospera su acción legal. Tiene su origen en la Inglaterra del siglo XIV y es recogido en los ordenamientos anglosajones.

competencia, de represión del blanqueo de capitales y financiación del terrorismo y de la corrupción nacional e internacional. No cabe ninguna duda de que los sistemas de whistleblowing están dentro del ámbito de aplicación de la normativa señalado anteriormente.

Los canales de denuncia internos son mecanismos atractivos desde diferentes perspectivas. Desde el punto de vista de la criminología, interesa analizar el hecho de que, de manera creciente, se pretenda convertir a los trabajadores en vigilantes, y en su caso en delatores, de sus superiores o compañeros. Para los laboristas se plantea la posibilidad de incorporar los deberes de denuncia al contrato de trabajo o la manera más adecuada de realizar las investigaciones internas que resultan de una determinada denuncia. Para los especialistas en protección de datos, les preocupa el tratamiento que debe darse a las bases de información utilizadas para procesar estas denuncias.

Por último he sintetizado lo que creo que debe ser un correcto canal de denuncias de una empresa cumpliendo tanto con los estándares nacionales e internacionales de ética y mejores prácticas, así como con toda la regulación española desde las diferentes materias del derecho que pueden afectar al mismo. Asimismo, he analizado todo el procedimiento de investigación y de reacción de la empresa ante una denuncia.

Finalmente quiero volver a destacar que creo que el tema de esta Tesis resulta sumamente interesante en estos momentos, ya que cada vez más organizaciones son conscientes de la necesidad de implantar sistemas y programas de *Corporate Compliance* que permitan prevenir o, al menos, reducir la comisión de actos ilícitos o indebidos en las mismas. Cada vez se considera más necesario implantar procedimientos internos para que los trabajadores o terceros (como proveedores o clientes) puedan denunciar conductas irregulares de los directivos o empleados de la empresa. Estos mecanismos refuerzan un mejor gobierno corporativo y el fortalecimiento de

una auténtica ética empresarial. Por razones de política criminal, estos sistemas facilitan el descubrimiento y la prevención de los hechos ilícitos que puedan producirse en la actividad empresarial, un entorno de difícil acceso para las investigaciones policiales y judiciales. Por todo ello, espero que este estudio resulte de ayuda e interés para comprender las complejidades del Canal de Denuncias Interno de una compañía desde distintas ópticas.

## II. EL FENÓMENO DEL COMPLIANCE Y LA LUCHA CONTRA LA CORRUPCIÓN

### 1. El fenómeno del Compliance

Para entender el fenómeno del *compliance* o cumplimiento normativo es fundamental conocer su origen e historia y conocer la cultura jurídica y empresarial que lo rodea.

Para muchos autores, la génesis del *compliance* se sitúa en los años setenta en Estados Unidos. En ese momento el regulador norteamericano del mercado de valores<sup>4</sup>, la Securities Exchange Commission (SEC), descubre que más de 400 compañías americanas han participado en pagos ilegales a cargos públicos o a partidos políticos en el extranjero<sup>5</sup>. Como consecuencia de lo anterior, el Senado en diciembre de 1977 aprueba la Foreign Corrupt Practices Act (FCPA), que como analizaremos más adelante prohíbe realizar pagos ilegales a funcionarios extranjeros y exige a las compañías cotizadas registrar todas las transacciones y contar con sistemas de control interno adecuados.

Durante los años noventa, con la creciente globalización, queda patente que las políticas nacionales no responden suficientemente al nuevo contexto de libre circulación de capitales. Para adaptarse a esta nueva realidad fue necesaria la firma de distintas iniciativas internacionales contra la corrupción, entre ellas y como pilar fundamental destaca la firma de los miembros de la OCDE (a instancias de Estados Unidos) de la Convención contra el Soborno en 1997. Ratificada en la actualidad por un total de 41 países, los Gobiernos firmantes se comprometen a implementar una legislación que penalice el

---

<sup>4</sup>Para entender el origen de la SEC y la evolución del fenómeno de la “policía” privada de EEUU es fundamental la obra de BALLBÉ, M./ MARTÍNEZ, R., “Law and Globalization: Between the United States and Europe”, ob. Cit pp. 145 y ss.

<sup>5</sup>REMACHA, M., “Compliance, ética y RSC”, Cuadernos de la Cátedra “la Caixa” de *Responsabilidad Social de la Empresa y Gobierno Corporativo*, Julio 2016, pp. 6 y ss., extraído de: [http://www.iese.edu/es/multimedia/catedralaciixa\\_31\\_tcm42-230724.pdf](http://www.iese.edu/es/multimedia/catedralaciixa_31_tcm42-230724.pdf).

soborno de un funcionario público extranjero<sup>6</sup>, similar a las regulaciones de la FCPA.

Asimismo, a partir de los años noventa se irán constituyendo los diferentes códigos e iniciativas que han permitido el desarrollo efectivo del *compliance* hasta su constitución actual<sup>7</sup>. En este sentido, y como ejemplo, la United States Sentencing Commission publicó en 1991 un Manual de Directrices (Guidelines Manual) en el que unificaba criterios que debían seguir los jueces al graduar las penas en los crímenes corporativos, intentando evitar la disparidad de criterios. Entre las distintas medidas, incluía la existencia de un programa de cumplimiento normativo y de acciones para evitar la comisión de delitos como factores que pueden atenuar o evitar la condena de la compañía. Dicha medida tuvo una enorme repercusión: a partir de entonces surge la figura del *Chief Ethics & Compliance Officer* (CECO, director de Ética y Cumplimiento) y muchas compañías adoptaron programas de cumplimiento<sup>8</sup>.

A lo largo de estas dos primeras décadas del nuevo milenio, el fenómeno del *Compliance* ha terminado de establecerse como respuesta necesaria a numerosos escándalos de corrupción, como fueron los casos de Enron, Tyco, Worldcom, Global, TelLink y Adelphia. En este contexto, en el año 2002 se promulgaba en Estados Unidos la ley Sarbanes-Oxley, con el fin de garantizar la veracidad de los informes auditados y evitar falsificación del valor de las empresas en bolsa, los fraudes y los riesgos de bancarrota<sup>9</sup>.

---

<sup>6</sup><http://www.oecd.org/corruption/oecdantibriberyconvention.htm>

<sup>7</sup>En 1992, el Committee of Sponsoring Organizations of the Treadway Commission (COSO), comité formado por cinco asociaciones estadounidenses de auditoría y rendición de cuentas, publicaba Internal Control-Integrated Framework, una guía para el diseño, implementación, seguimiento y evaluación de controles internos. Se trata del manual más extendido en Estados Unidos, así como en la mayoría de las empresas de todo el mundo.

<sup>8</sup>MURPHY, D. E., "The Federal Sentencing Guidelines for Organizations: A Decade of Promoting Compliance and Ethics", *Iowa Law Review*, nº 87, 2002, pp. 697-719.

<sup>9</sup>GILBERT W. J., *Sarbanes-Oxley For Dummies*, 2ª ed., Indianápolis, 2008.

Para acabar de entender el fenómeno en el que estamos inmersos es necesario señalar que en la actualidad nos encontramos ante una ola general de americanización de los ordenamientos jurídicos europeos<sup>10</sup>, y esta nueva corriente norteamericana ha traído también el *compliance*, que actualmente ha pasado también a ser parte esencial de la nueva cultura jurídica y empresarial europea<sup>11</sup>.

En los últimos años, la crisis financiera junto con el descubrimiento de graves casos de corrupción, ha provocado el aumento de presión social (tanto por parte de ciudadanos, como inversores y reguladores) demandando un nuevo marco de transparencia y de ética mucho más elevado. Tal y como afirma M. BALLBÉ *“la fuente de los nuevos derechos, aunque formalmente serán las leyes del Parlamento y los reglamentos de la Administración, materialmente ha sido el activismo de los grupos y la comunidad en detectar los viejos y nuevos riesgos para el derecho a la vida, a la salud y a la seguridad humana”*<sup>12</sup>.

Dicha exigencia se ha traducido en la implantación en las empresas de los programas de *compliance* y en la normalización de la función del cumplimiento normativo en los Consejos de Administración. Asimismo, los Gobiernos y reguladores han contribuido enormemente en estos últimos años al desarrollo de estas nuevas políticas, creando o adaptando la normativa que

---

<sup>10</sup>En este sentido BALLBÉ, M. y MARTÍNEZ; R. señalan la importante influencia que el derecho norteamericano ha ejercido sobre los ordenamientos europeos y también, en particular sobre el nuestro. Como ejemplo de americanización del derecho español y europeo señalan la *Administrative Procedure Act* en 1946 que inspiró la famosa Ley de Procedimiento Administrativo española de 1958. BALLBÉ, M./ MARTÍNEZ, R., “Law and Globalization: Between the United States and Europe”, ob. Cit pp. 158 y ss.

<sup>11</sup>NIETO MARTIN, A., “Cumplimiento normativo”, en AA.VV., *Manual de cumplimiento penal en la empresa*, dir. A. Nieto Martin, Valencia, 2015, p. 27.

<sup>12</sup>BALLBÉ, M. “El futuro del derecho administrativo en la globalización: entre la americanización y la europeización”, *Revista de Administración Pública*, núm. 174, 2007, pp 236.

establece la existencia de un programa de cumplimiento como un imperativo para las empresas<sup>13</sup>.

Daniel S. Lewis ha definido el *Compliance* como el proceso de identificación y gestión de los riesgos regulatorios y de conducta a los que una compañía está expuesta y señala que los riesgos regulatorios y de conducta provienen tanto de la exposición externa de la empresa (las reglas creadas por los reguladores) como de los requisitos internos (los procedimientos y políticas internas autoimpuestas en cada organización)<sup>14</sup>. Respecto a los requisitos internos debe señalarse que esta era de la globalización se caracteriza, entre otras cosas, por utilizar esta nueva forma de autorregulación por medio de la cual las propias compañías se imponen unos estándares que se comprometen a cumplir<sup>15</sup>. Tal y como dicen M. BALLBÉ y R. MARTÍNEZ en el libro *Global Administrative Law “la autorregulación es la base del concepto moderno del Derecho Administrativo”*<sup>16</sup>. Este impulso de la autorregulación, en sus distintas vertientes permite generar normas y procedimientos básicos para el buen funcionamiento del mercado y el interés general<sup>17</sup>.

Tal y como veremos el ámbito de aplicación de lo que se entiende actualmente por *Compliance* es difuso, pero podríamos sostener que la opinión mayoritaria es que abarca, como mínimo, las siguientes materias: la prevención de riesgos laborales, la corrupción en todos sus sentidos, el respeto a la normativa sobre mercado de valores, el abuso de mercado y

---

<sup>13</sup>Entre los ejemplos más notables de ello a nivel internacional, se encuentra la ley anticorrupción del Reino Unido (Bribery Act 2010), que atañe a los delitos cometidos tanto en territorio británico como fuera del mismo por empresas o ciudadanos originarios de este país. La ley, considerada una de las más severas y referente en el ámbito internacional, incluye los pagos de facilitación y el acto de recibir sobornos como delitos sancionables, algo que no incluye su homóloga estadounidense Foreign Corrupt Practices Act (FCPA).

<sup>14</sup>LEWIS, D.S., *Compliance: A concise guide to the role of the Compliance Function in financial services firms*, edit. Create Space Independent Publishing Platform, 2016.

<sup>15</sup>Sobre este tema ESTEVE PARDO, J. “Autoregulación: Génesis y efectos”, Aranzadi. 2012.

<sup>16</sup>BALLBÉ, M. / MARTÍNEZ, R. “Law and Globalization: Between the United States and Europe”, en AA.VV., *Global Administrative Law. Towards a Lex Administrativa*, dirs. J. Robalino-Orellana/ J. Rodríguez-Arana, pp. 137 y ss.

<sup>17</sup>NIETO MARTIN, A., “Cumplimiento normativo”, ob. cit., p. 33.

otros incumplimientos a la normativa de defensa de la competencia, la protección de datos y respeto a la regulación sobre nuevas tecnologías, el blanqueo de capitales y financiación del terrorismo, el respeto al medioambiente, la discriminación positiva, contratación en el sector público, etc. En todas estas áreas, y en muchos casos en otras adicionales, el *compliance* consistiría en asegurar el cumplimiento de la legislación aplicable y políticas de la empresa y establecer mecanismos internos que eviten conductas que pudieran resultar en infracciones de lo anterior.

Como se desarrolla más adelante, el cumplimiento normativo necesariamente se apoya en el buen gobierno corporativo, entendiendo por gobierno corporativo los mecanismos de lucha contra cualquier abuso de poder por parte de los directivos de una compañía.

Asimismo, debe resaltarse que el *compliance* -tanto en un sentido más estricto como en un sentido más amplio- tiene una estrechísima relación con la ética<sup>18</sup>, y se apoya en los llamados códigos éticos, con los que actualmente cuentan todas las grandes compañías y que recogen principios y valores éticos que se comprometen a seguir en la lucha contra la corrupción. Por tanto, esta ética autoimpuesta por las empresas pasa a ser una forma de *soft law*, la cual se comprometen a cumplir las empresas constituyéndose como un mecanismo de control de ciertos delitos en el seno de las organizaciones empresariales. Para su efectividad -y tal y como veremos más adelante- dichos códigos han dejado de ser meras declaraciones o recomendaciones para pasar a constituir verdaderas obligaciones entre los empleados, pudiendo sancionarse disciplinariamente a los mismos si no las cumplieran. La ética de la empresa está indudablemente relacionada con la responsabilidad social corporativa<sup>19</sup>.

---

<sup>18</sup>LEWIS, D.S., *Compliance: A concise guide to the role of the Compliance Function in financial services firms*, edit. Create Space Independent Publishing Platform, 2016.

<sup>19</sup>ALONSO DE ESCAMILLA, A., "La responsabilidad penal de los administradores de sociedades mercantiles. Una aproximación desde la perspectiva del compliance", en AA.VV., *Gobierno*



Sin embargo es evidente que confiar en esta propia autorregulación de las empresas sin establecer unos incentivos o desincentivos legislativos podría convertir a los programas de cumplimiento en papel mojado que sólo sirvan como meros instrumentos de marketing de las empresas frente a la opinión pública. Dicho peligro es evidente tanto en iniciativas nacionales como internacionales<sup>20</sup>, como el Pacto Mundial de Naciones Unidas (Global Compact), cuyos elementos de implementación han sido calificados por algunos autores como muy débiles<sup>21</sup>. O, lo que es peor, puede llevar a movilizar los recursos de la empresa hacia la “apariencia” del cumplimiento: como decía Marx (Groucho), “*el secreto de la vida es la honestidad y el juego limpio; si puedes simular eso, lo has conseguido*”<sup>22</sup>.

Por tanto, puede concluirse que el cumplimiento normativo se ha convertido en un instrumento de *global law* o gobernanza global. En este sentido, la forma más determinante para obligar a las empresas a cumplir con una correcta y eficaz autorregulación es establecer la responsabilidad penal de las personas jurídicas cuyo fin último es forzar a las empresas a que adopten mecanismos internos de control para que traten de evitar la comisión de ilícitos<sup>23</sup> y así además de prevenir y detectar hechos delictivos, exonerando o reduciendo tal responsabilidad<sup>24</sup>. Cabe destacar que en un número significativo de países de nuestro entorno como Alemania, Italia o Austria la

---

*corporativo: la estructura del órgano de gobierno y la responsabilidad de los administradores. Adaptado a la Ley 31/2014, de 3 de diciembre*, dir. A. Martínez-Echevarría, Pamplona, 2015, p. 884.

<sup>20</sup>El Pacto Mundial de Naciones Unidas (Global Compact) es una iniciativa internacional que promueve implementar 10 Principios universalmente aceptados para promover la responsabilidad social empresarial (RSE) en las áreas de Derechos Humanos y Empresa, Normas Laborales, Medio Ambiente y Lucha contra la Corrupción en las actividades y la estrategia de negocio de las empresas. Con más 13.000 entidades firmantes en más de 145 países, es la mayor iniciativa voluntaria de responsabilidad social empresarial en el mundo, sin embargo sus elementos de implementación podrían calificarse de muy débiles.

<sup>21</sup>NIETO MARTIN, A., "Cumplimiento normativo", ob. cit., pp. 34-35.

<sup>22</sup>ARGANDOÑA, A., "La compliance en la empresa", extraído de: <http://blog.iese.edu/antonioargandona/2014/02/12/la-compliance-en-la-empresa/>

<sup>23</sup>NIETO MARTIN, A., "El cumplimiento normativo", ob. cit., pp. 34-35.

<sup>24</sup>Vid. NIETO MARTIN, A., "Problemas fundamentales del cumplimiento normativo en el Derecho penal", en *Compliance y teoría del Derecho penal*, Marcial Pons, 2013, pp. 25 y 26.

responsabilidad de la empresa se basa en la culpabilidad por defecto de organización<sup>25</sup>. Consecuentemente, la existencia de programas de cumplimiento efectivos en el seno de las empresas puede servir para que las mismas no respondan penalmente o puedan ver atenuadas la responsabilidad empresarial si uno de sus administradores o trabajadores comete un delito al realizar sus funciones<sup>26</sup>.

Por ello, la elaboración de programas de cumplimiento constituye algo necesario hoy en día<sup>27</sup>. Los sistemas de cumplimiento, que también en ocasiones son llamados *corporate codes*, *compliance programs*, *codes of conduct*, *corporate social responsibility*, *risk management*, *value management*, *corporate governance*, *business ethics* o *integrity codes*, entre otras acepciones, constituyen mecanismos de control social empresarial para controlar y evitar la comisión de ilícitos penales por parte de las empresas<sup>28</sup>.

Tal y como veremos a continuación, el cumplimiento normativo convive en el entorno empresarial con una serie de movimientos o de fenómenos conexos que están interrelacionados. Por un lado, una cultura empresarial ética<sup>29</sup> es un presupuesto básico para que exista la responsabilidad social corporativa, lo cual también es un presupuesto fundamental para poder cumplir con el buen gobierno en la empresa. Por otro lado, la autorregulación con la gestión

---

<sup>25</sup>En España, el compliance es una función en auge desde el año 2010, cuando la reforma del Código Penal introdujo la responsabilidad penal de las personas jurídicas. Anteriormente, solo las empresas que operaban junto a compañías británicas o americanas, o en estos territorios, se habían visto obligadas a desarrollar la función de cumplimiento normativo, ya que la legislación de estos países (por ejemplo, la Bribery Act 2010 o la Foreign Corrupt Practices Act) también les era de aplicación. A partir de la reforma de 2010, la función se ha generalizado a la práctica totalidad de las grandes corporaciones españolas, tengan o no actividad en el extranjero.

<sup>26</sup>ALONSO DE ESCAMILLA, A., "La responsabilidad penal...", ob. cit., pp. 885-886.

<sup>27</sup>Sobre la necesidad de los Programas de Cumplimiento es imprescindible la obra de VILLEGAS GARCIA, M.A., ENCINAR, M.A. "*Compliance Programs y DPA: Una nueva etapa en el camino hacia un derecho anticorrupción sin fronteras*", 2016.

<sup>28</sup>ALONSO DE ESCAMILLA, A., "La responsabilidad penal...", ob. cit., pp. 883-884.

<sup>29</sup>La ética empresarial puede ser definida como el descubrimiento y aplicación de los valores y normas compartidos por una sociedad pluralista al ámbito peculiar de la empresa, lo cual requiere entenderla según un modelo comunitario. CORTINA, A., *Ética De La Empresa. Claves Para Una Nueva Cultura Empresarial (Estructuras y Procesos. Filosofía)*, 7ª ed., Trotta, Madrid, 2013.

de riesgos, la estandarización y la auditoría son conceptos complementarios para conseguir los fines que establece el cumplimiento normativo. Las interrelaciones entre estos contenidos afectan lógicamente a la definición de tareas y competencias en la empresa para lograrlos<sup>30</sup>.

## 1.1 El Compliance y el Buen Gobierno Corporativo

Es evidente que los conceptos de *Compliance* y Buen Gobierno Corporativo coinciden en muchas de sus áreas. El Buen Gobierno Corporativo es también un concepto en continua evolución al menos si pensamos en la “sociedad” como un concepto que incluye a la *société anonyme* en países de habla francesa, la *Gesellschaft mit beschränkter Haftung* y *Aktiengesellschaft* en países de habla alemana, la sociedad anónima en España, y la *società per azioni* en Italia, o la insistente demanda en todo en el mundo corporativo por implantar el buen gobierno corporativo.<sup>31</sup>

Hay autores que también han considerado el Buen Gobierno Corporativo como una subcategoría de la Ética, ya que las decisiones del Consejo de Administración muchas veces versan sobre las áreas no reguladas por la Ley y tienen un componente ético muy fuerte. Todo esto hace imposible definir el Buen Gobierno al margen del *Compliance*, la Ética o la Responsabilidad Social Corporativa<sup>32</sup>.

El Buen Gobierno corporativo tiene como fin último evitar el abuso de poder en su sentido más amplio- dentro de las empresas por parte de los directivos que las gestionan. Esta herramienta es especialmente necesaria en las empresas cotizadas donde existe una clara separación entre los dueños del capital y los directivos que gestionan la empresa. El gobierno corporativo trata de proteger, mediante el establecimiento de una serie de medidas, a los

---

<sup>30</sup>NIETO MARTIN, A., "El cumplimiento normativo", ob. cit., pp. 35-36.

<sup>31</sup>NORDBERG, D., *Corporate Governance: Principles and Issues*, SAGE Publications Ltd, London, 2011, pp. 2 y ss.

<sup>32</sup>NORDBERG, D., *Corporate Governance...*, ob. cit., pp. 2 y ss.

socios de la compañía (*shareholders*), así como a determinadas personas que podrían resultar afectadas por la actividad de la sociedad (*stakeholders*). La definición clásica de stakeholders de FREEMAN es “*un grupo o individuos que pueden influir o que es influido por los logros y objetivos de una empresa*”<sup>33</sup>. El gobierno corporativo tiene en cuenta que la actividad de una empresa y su buena gestión no sólo afectan a sus socios sino también a otros círculos de personas.<sup>34</sup>

Es necesario destacar que el buen gobierno influye enormemente en la reputación de la compañía, genera confianza en su liderazgo, fomenta las inversiones, y tiene un impacto positivo en el precio de las acciones<sup>35</sup>.

Teniendo en cuenta la similitud de materias y objetivos que comparten las áreas de cumplimiento normativo y de buen gobierno en una empresa es frecuente y, además, conveniente, que los encargados de ambos departamentos tengan también una estrecha relación institucional, llegando a veces incluso a solaparse. Actualmente la importancia del buen gobierno ha conducido a que existan comisiones del Consejo en las sociedades cotizadas (tal y como es el caso de la Comisión de Auditoría, de Responsabilidad Social, Comisión del Código Ético, *controlling*, etc.) cuya función es garantizar la calidad de la información financiera y el control de riesgos, o el cumplimiento de las políticas internas asumidas por la entidad.

Dentro de esta interrelación que existe entre el Buen Gobierno y el *Compliance*, debemos de destacar que ambas herramientas responden a la misma técnica de intervención administrativa: la autorregulación incentivada o coaccionada. En cada país se han publicado Códigos de Buen Gobierno, en los cuales se hacen recomendaciones sobre cómo organizar la gestión o el

---

<sup>33</sup>FREEMAN, R.E., *Strategic Management: A Stakeholder Approach*, Pitman Press, Boston, 1984.

<sup>34</sup>FRIEDMAN, A.L./ MILES, S., *Stakeholders: Theory and Practice*, Oxford University Press, 2006, pp. 1 y ss

<sup>35</sup>KOTZ, H. D., *Financial Regulation and Compliance. How to manage Competing and Overlapping Regulatory Oversight*, Edit. John Wiley & Sons, Inc, New York, 2015, pp. 23 y ss.

gobierno de las sociedades cotizadas, dichas recomendaciones quedan sujetas al principio de "cumplir o explicar"<sup>36</sup>. Es importante resaltar que la falsedad en el informe de buen gobierno corporativo en muchos ordenamientos constituye una infracción penal<sup>37</sup> o administrativa<sup>38</sup>, así que teniendo en cuenta que el sistema de cumplimiento forma parte del sistema de buen gobierno, la información falsa relativa a dicho sistema podría considerarse constitutivo de alguna de estas infracciones. En ciertos países, como es el caso de Alemania, los programas de cumplimiento han adquirido relevancia penal a través de estos delitos. Este tipo de formas, son una alternativa al uso del derecho penal a través de la responsabilidad penal de las personas jurídicas para incitar a la autorregulación de las empresas que constituye el *compliance*<sup>39</sup>.

Tal y como quedó expuesto anteriormente, el Gobierno Corporativo tiene como objetivo que en la gestión de las empresas se tenga en cuenta además de los derechos de los socios, los intereses y derechos de los *stakeholders*.

Así el Código del buen gobierno de las sociedades cotizadas, señala como Principio 9: *"El consejo de administración asumirá, colectiva y unitariamente, la responsabilidad directa sobre la administración social y la supervisión de la dirección de la sociedad, con el propósito común de promover el interés social"*. Así mismo se recomienda *"que en la búsqueda del interés social, además del respeto de las leyes y reglamentos y de un comportamiento basado en la buena fe, la ética y el respeto a los usos y a las buenas prácticas comúnmente aceptadas, procure conciliar el propio interés social con, según corresponda, los legítimos intereses de sus empleados, sus proveedores, sus clientes y los de los restantes grupos de interés que puedan*

---

<sup>36</sup>Código del buen gobierno de las sociedades cotizadas, CNMV, 18 de febrero de 2015, disponible en [https://www.cnmv.es/docportal/publicaciones/codigogov/codigo\\_buen\\_gobierno.pdf](https://www.cnmv.es/docportal/publicaciones/codigogov/codigo_buen_gobierno.pdf), y art. 540.4.g TRLSC.

<sup>37</sup>Arts. 282 bis y 290 del CP.

<sup>38</sup>Art. 540.5 TRLSC y art. 296.1 TRLMV.

<sup>39</sup>NIETO MARTIN, A., "El cumplimiento normativo", ob. cit., pp. 39-40.

*verse afectados, así como el impacto de las actividades de la compañía en la comunidad en su conjunto y en el medio ambiente” (Recomendación 12).*

Otro punto importante en el que convergen el Cumplimiento Normativo y el Buen Gobierno Corporativo es en la política de gestión de riesgos. Una infracción normativa puede conllevar un potencial riesgo económico o reputacional que puede ser crucial para la empresa (multas; la interdicción de contratar con la administración o de recibir ayudas públicas; revocación de licencias...). En este sentido, los Códigos de Buen Gobierno establecen que una de las facultades indelegables del Consejo es aprobar la política de gestión de riesgos, así como el seguimiento periódico de los sistemas internos de información y control. Los sistemas de cumplimiento son parte de la administración diligente en las sociedades cotizadas. En el caso del ordenamiento jurídico alemán, la legislación societaria incluye de manera expresa la gestión de riesgos como una de las funciones del Consejo de Administración<sup>40</sup>, de manera paralela el Código de Buen Gobierno alemán considera fundamental para dicha gestión el cumplimiento normativo<sup>41</sup>.

Por último cabe destacar que el gobierno corporativo también sirve (tal y como hace el *compliance*) para prevenir determinados delitos societarios<sup>42</sup>. Asimismo, los códigos de buen gobierno tienen como premisa potenciar la transparencia en la gestión y, por tanto, la calidad y la fiabilidad de la información societaria<sup>43</sup>.

---

<sup>40</sup>§ 91.2 Aktiengesetz (Ley Alemana de Sociedades Anónimas), dispone que la dirección ha de adoptar *“las medidas necesarias, en particular, la organización de un sistema de vigilancia, para conocer lo antes posible los desarrollos peligrosos para la subsistencia de la sociedad”*.

<sup>41</sup>NIETO MARTIN, A., "El cumplimiento normativo", ob. cit., pp. 38-39.

<sup>42</sup>En este sentido se debe recordar que los códigos de buen gobierno tratan de las retribuciones de los consejeros e impiden los conflictos de interés, lo que ayuda a la prevención de delitos (como el de administración desleal).

<sup>43</sup>Por tanto, es evidente que un sistema de gobierno corporativo eficiente ayuda a prever los delitos societarios.

## 1.2 El Compliance y la Responsabilidad Social Corporativa

La Responsabilidad Social Corporativa implica un cambio de visión respecto a la empresa que pasa a convertirse en una suerte de ciudadano responsable (*good citizens corporations*), el cual actúa con una responsabilidad no sólo económica, sino social, política y moral hacia su comunidad.<sup>44</sup>

Esta concepción de la persona jurídica como co-responsable en cuanto al cumplimiento con sus obligaciones tiene su origen en la regulación americana de la era Roosevelt, tal y como ya señaló M. BALLBÉ “*esta reforma puede considerarse trascendental porque vino a cambiar los parámetros del Derecho Administrativo y de las tradicionales formas de intervención e inspección administrativas*”<sup>45</sup>.

Actualmente y de manera global, la política de responsabilidad social empresarial emerge como una nueva ratio de las empresas para contrarrestar el reproche social a una gestión empresarial incívica e insostenible practicada por algunas entidades, que ha dañado la imagen colectiva, y con el objetivo de reforzar la reputación de la entidad.<sup>46</sup> Determinadas legislaciones incluso conceden a las compañías derechos de ciudadanía<sup>47</sup> como la libertad de expresión o la posibilidad de financiar partidos políticos<sup>48</sup>. La empresa, especialmente las grandes multinacionales,

---

<sup>44</sup>NIETO MARTIN, A., "El cumplimiento normativo", ob. cit., p. 40.

<sup>45</sup>BALLBÉ, M. “*El futuro del derecho administrativo en la globalización: entre la americanización y la europeización*”, Revista de Administración Pública, núm. 174, 2007, pp 230.

<sup>46</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial (Compliance programs): aspectos laborales", en AA.VV., *Responsabilidad de la Empresa y Compliance. Programas de prevención, detección y reacción penal*, dirs. S. Mir, M. Corcoy y V. Gómez, Madrid, 2014, ob. cit., p. 379.

<sup>47</sup>Tal y como dice M. BALLBÉ “*al regular el comportamiento de empresas y ciudadanos y traspasarles la responsabilidad a ellos, se convierten prácticamente en protagonistas activos de la implementación de los valores y principios de esta regulación*”. BALLBÉ, M. “*El futuro del derecho administrativo en la globalización: entre la americanización y la europeización*”, ob. cit., pp 231.

<sup>48</sup>Realmente, el entendimiento de la empresa como ciudadano, con una responsabilidad social y moral hacia la sociedad que le rodea, conecta también con la responsabilidad penal de la persona

en una economía global tienen un poder cada vez mayor que puede llegar a afectar a personas que no tienen ningún vínculo contractual con ella. Como contrapartida, dicho poder debe suponer una determinada responsabilidad en el ejercicio de la actividad de la empresa.

Esta nueva forma de concebir a la empresa comprende que éstas son más eficientes cuando se dirigen de acuerdo con determinados principios y respetando su entorno. Asimismo, podría argumentarse que el respeto a principios e intereses comunes, al medio ambiente y a los derechos humanos, son un mínimo exigido como respuesta a que los individuos puedan actuar bajo una forma societaria con el beneficio implícito de la limitación de responsabilidad.

La Responsabilidad Social Corporativa (RSC) que entiende a las empresas como *good citizen corporations* también influye en la forma de entender por parte de la empresa el buen gobierno. Porque aunque, tal como muestra el Código de Buen Gobierno español, el interés de los socios es el fin principal, también el respeto a las leyes y los principios éticos básicos deben ser un objetivo prioritario de los directivos<sup>49</sup>.

Por tanto, aunque el *Compliance* y la RSC compartan muchos aspectos, es necesario señalar también su principal diferencia: la obligatoriedad de la primera frente a la voluntariedad de la segunda. El *compliance*, en efecto, logra que la empresa se gestione con responsabilidad y siguiendo una normativa cuyo fin último es posibilitar la convivencia social. Pero esto no es suficiente para la RSC, cuyo fin último es que la empresa sobrepase los mínimos de cumplimiento (obligatorios) y alcance los máximos de excelencia (voluntarios).<sup>50</sup> Este carácter voluntario de la RSC deriva de su estrecha relación con la ética, y es sin duda su mayor grandeza y al mismo tiempo su

---

jurídica que trataremos más adelante y podría llevar a justificar el concepto de culpabilidad de empresa.

<sup>49</sup>NIETO MARTIN, A., "El cumplimiento normativo", ob. cit., pp. 41 y 43.

<sup>50</sup>REMACHA, M., "Compliance, ética y RSC", ob. cit., pp. 6 y ss.



principal flaqueza. Los objetivos de la RSC no son obligatorios y no existen medios coercitivos para imponer su cumplimiento lo que puede llevar a una cierta utilización de la misma con un interés reputacional<sup>51</sup>.

Por todo lo anterior, el *Compliance* debe entenderse como un instrumento de la RSC, dentro del área de cumplimiento con la legalidad, pero no como su esencia misma<sup>52</sup>, aunque también es cierto que poco a poco cada vez más Estados y organizaciones internacionales tratan de aprobar normas o programas que favorezcan la exigibilidad de la RSC.

La Unión Europea está interesada en la responsabilidad social de las empresas en la medida en que puede contribuir positivamente al objetivo estratégico establecido en Lisboa: *“convertirse en la economía basada en el conocimiento más competitiva y dinámica del mundo, capaz de crecer económicamente de manera sostenible con más y mejores empleos y con mayor cohesión social”*. Tal como señala por ejemplo el Libro Verde de la UE para fomentar un marco europeo para la responsabilidad social de las empresas ésta es necesaria para un crecimiento económico continuado y para atraer inversores. De acuerdo con dicho Libro Verde *“La responsabilidad social de las empresas es, esencialmente, un concepto con arreglo al cual las empresas deciden voluntariamente contribuir al logro de una sociedad mejor y un medio ambiente más limpio”*<sup>53</sup>.

En Europa las primeras manifestaciones de la RSC han sido la preocupación por el medio ambiente y la sostenibilidad en todos sus sentidos. De manera progresiva la RSC también ha ido incorporando otro tipo de valores sociales, como la lucha anticorrupción, el respeto a los derechos humanos, o que se respete el marco legal dentro de la actividad empresarial. Actualmente, el

---

<sup>51</sup> NAVARRO GARCÍA, F., *Responsabilidad Social Corporativa: Teoría y práctica*, 2ª ed., ESIC, Madrid, 2012, pp. 2 y ss.

<sup>52</sup> ARGANDOÑA, A., "Compliance + ética, ¿por qué? (II)", *Economía, Ética y RSE*, IESE Blog Network, 8 de mayo de 2015. Extraído de: <http://blog.iese.edu/antonioargandona/2015/05/08/compliance-etica-por-que-i/>

<sup>53</sup> Extraído de: <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52001DC0366&from=ES>

buen ambiente en el trabajo también se considera un factor a proteger y determinante para aumentar la productividad de la empresa (*human resources approach*)<sup>54</sup>. Sobre este tema, es imprescindible destacar la gran obra de R. MARTÍNEZ<sup>55</sup>. Tal y como afirma, algunas empresas que han infringido el ordenamiento han quedado obligadas por parte de los Tribunales o Administración a disponer de un “*director público especial*”.

Para algunos autores, la RSC significa un nuevo enfoque estratégico para la gestión empresarial, basado en una visión relacional de la misma. Es, en definitiva, la innovación para la sostenibilidad corporativa de la empresa (sostenibilidad corporativa) y del entorno social al que afecta<sup>56</sup>.

La iniciativa con más éxito en relación a la RSC ha sido el ya citado Pacto Mundial de Naciones Unidas el cual goza de un consenso universal y contiene 10 principios que derivan de las declaraciones de las Naciones Unidas en materia de derechos humanos, trabajo, medioambiente y anticorrupción<sup>57</sup>. Actualmente el Pacto Mundial cuenta con 13.000 entidades firmantes en más de 145 países<sup>58</sup>. Las entidades firmantes deben realizar anualmente una Comunicación de Progreso en la que expongan las medidas

---

<sup>54</sup>NIETO MARTIN, A., "El cumplimiento normativo", ob. cit., pp. 40 a 42.

<sup>55</sup>MARTÍNEZ, R. “*El Delegado de Prevención de Riesgos Ambientales*”. Trabajo original de investigación para la oposición a Profesor Titular de Derecho Administrativo UAB, convocada por la Resolución de 8 de noviembre de 2001 (BOE 26 de noviembre de 2001).

<sup>56</sup>PERRINI, F./ TENCATI, A., *Corporate Social Responsibility: Un nuovo approccio strategico alla gestione d'impresa (Cultura di impresa)*, Ed. Egea, Milano, 2011, pp 1-2.

<sup>57</sup>Los 10 Principios del Pacto Mundial son los siguientes: Principio 1: Las empresas deben apoyar y respetar la protección de los derechos humanos fundamentales, reconocidos internacionalmente, dentro de su ámbito de influencia. Principio 2: Las empresas deben asegurarse de que sus empresas no son cómplices en la vulneración de los Derechos Humanos. Principio 3: Las empresas deben apoyar la libertad de afiliación y el reconocimiento efectivo al derecho de la negociación colectiva. Principio 4: Las empresas deben apoyar la eliminación de toda forma de trabajo forzoso o realizado bajo coacción. Principio 5: Las empresas deben apoyar la erradicación del trabajo infantil. Principio 6: Las empresas deben apoyar la abolición de las prácticas de discriminación en el empleo y la ocupación. Principio 7: Las empresas deben mantener un enfoque preventivo que favorezca al medioambiente. Principio 8: Las empresas deben fomentar las iniciativas que promuevan una mayor responsabilidad ambiental. Principio 9: Las empresas deben favorecer el desarrollo y la difusión de las tecnologías respetuosas con el medioambiente. Principio 10: Las empresas deben trabajar contra la corrupción en todas sus formas, incluidas la exclusión y el soborno. Extraído de <http://www.pactomundial.org/category/aprendizaje/10-principios/>

<sup>58</sup><http://www.pactomundial.org/global-compact/>

adoptadas para cumplir los diez principios del Pacto Mundial. No enviar dicha Comunicación implica quedar excluidas de la lista de participantes activos del Pacto Mundial.

En este mismo sentido, las Líneas Directrices de la OCDE para Empresas Multinacionales (*Guidelines for Multinational Enterprises* de la OCDE)<sup>59</sup> consideran que las empresas deben desarrollar sistemas de cumplimiento, implementar canales de denuncia para empleados, formación, gestión de riesgos con el fin de identificar, mitigar y prevenir infracciones, etc.<sup>60</sup> Las Líneas Directrices de la OCDE para Empresas Multinacionales son recomendaciones dirigidas por los gobiernos a las empresas multinacionales que operan en países adherentes o que tienen su sede en ellos. Contienen principios y normas no vinculantes para una conducta empresarial responsable dentro del contexto global, conformes con las leyes aplicables y las normas reconocidas internacionalmente. Las Directrices constituyen el único código de conducta empresarial responsable, exhaustivo y acordado multilateralmente, que los gobiernos se han comprometido a promover<sup>61</sup>.

Algunos ordenamientos también han establecido medidas para incentivar el cumplimiento de la RSC. En particular en España, la Ley 2/2011, de 4 de marzo, de Economía Sostenible (en su capítulo V del Título I: Promoción de la Responsabilidad Social de las Empresas) establece que las *“Administraciones Públicas mantendrán una política de promoción de la responsabilidad social difundiendo su conocimiento y las mejores prácticas existentes y estimulando el estudio y análisis sobre los efectos en materia de competitividad empresarial de las políticas de responsabilidad social”*<sup>62</sup> y que

---

<sup>59</sup><http://www.oecd.org/corporate/mne/>

<sup>60</sup>NIETO MARTIN, A., "El cumplimiento normativo", ob. cit., pp. 42-43.

<sup>61</sup>Las *Directrices* actualizadas y la Decisión conexas fueron adoptadas por los 42 gobiernos adherentes el 25 de mayo de 2011 en la Reunión Ministerial conmemorativa del 50 Aniversario de la OCDE.

<sup>62</sup>Artículo 39 de la Ley 2/2011, de 4 de marzo, de Economía Sostenible.

pondrán a disposición de las empresas un sistema de autoevaluación, y "*modelos de referencia o reporte*".

Asimismo en España existe el Consejo Estatal de Responsabilidad Social Empresarial<sup>63</sup> que entre sus funciones están las de estandarizar los modelos de informe de responsabilidad social corporativa, comprobar el seguimiento de las políticas de RSC de las sociedades anónimas de más de 1.000 empleados y expedir acreditaciones de empresas socialmente responsables a aquellas que lo soliciten<sup>64</sup>.

Existe en definitiva una función cada vez más social de la empresa, a la que contribuye claramente la normativa y procedimientos en materia de *compliance*. Una tendencia a la socialización a través de la empresa, tendente a una función no exclusivamente económica. Dicha tendencia encuentra un paralelismo en otros ámbitos de ordenamiento jurídico. En lo que respecta al Derecho Penal (al que el *compliance* está ligado de una forma tan estrecha dada su naturaleza), éste fue adaptándose asimismo con el tiempo a ejercer también un función socializadora respecto de la ejecución de las pena y su régimen sancionador con vocación de reinserción del individuo, y eminentemente respecto en los casos de menores, en lugar de tener una función (como era históricamente) eminentemente de represión y exclusión social en cuanto a su carácter sancionador, tal y como muestran las prestigiosas obras de E. GIMÉNEZ- SALINAS<sup>65</sup>.

### **1.3 El Compliance y la Ética Empresarial**

La ética empresarial constituye otro fenómeno muy cercano al cumplimiento normativo y a la RSC.

---

<sup>63</sup>[http://www.empleo.gob.es/es/sec\\_trabajo/autonomos/economia-soc/RespoSocEmpresas/consejo\\_rse/](http://www.empleo.gob.es/es/sec_trabajo/autonomos/economia-soc/RespoSocEmpresas/consejo_rse/)

<sup>64</sup>Real Decreto 221/2008, de 15 de febrero, por el que se crea y regula el Consejo Estatal de Responsabilidad Social de las Empresas.

<sup>65</sup>GIMÉNEZ-SALINAS COLOMER, E. "Delincuencia juvenil y control social". Barcelona, 1981.

La empresa debe estar gestionada de manera que los comportamientos dentro de la misma respondan a los mismos valores que ha decidido autoimponerse (*value driven management*), para ello resulta muy operativo tener recogidos dichos valores empresariales en un código ético. Lo óptimo para que todo funcione de acuerdo con la ética empresarial es que haya coherencia entre los valores de las personas que la integran y los de la empresa. La ética de una organización se refleja en los comportamientos diarios de cada uno de sus integrantes, y no sólo nos referimos a los directivos, aunque para que los valores éticos queden integrados en los programas de cumplimiento es fundamental que los directivos estén implicados en la implementación del programa de manera activa, lo que se ha llamado el *tone from the top*<sup>66</sup>. Los valores de los empleados de una empresa son fundamentales para el éxito del comportamiento ético de la misma<sup>67</sup>.

Cumplimiento normativo y ético son fenómenos conexos que en cierta medida también se solapan. En una entidad que valore la importancia de la RSC y que asuma la ética, el diseño del plan de cumplimiento normativo debe basarse en los valores éticos de la entidad, la falta de coherencia entre dicho plan y los valores éticos de la empresa tendría consecuencias muy perjudiciales perdiendo ambas herramientas sentido<sup>68</sup>.

## **2. Directrices internacionales contra la corrupción en el comercio internacional**

La corrupción en el comercio es uno de los mayores obstáculos para un desarrollo ético del mismo. El Secretario de las Naciones Unidas Kofi A. Annan en su Prefacio a la Convención de las Naciones Unidas contra la

---

<sup>66</sup>NIETO MARTIN, A., "El cumplimiento normativo", ob. cit., pp. 44-45.

<sup>67</sup>WARNER, J.C., *Corporate Ethics (Rapid Skill Builder Series)*, Ed. Ready To Manage Inc, 2012.

<sup>68</sup>NIETO MARTIN, A., "El cumplimiento normativo", ob. cit., p. 44.

corrupción de octubre de 2003<sup>69</sup> señaló que *"la corrupción es una plaga insidiosa que tiene un amplio espectro de consecuencias corrosivas para la sociedad. Socava la democracia y el estado de derecho, da pie a violaciones de los derechos humanos, distorsiona los mercados, menoscaba la calidad de vida y permite el florecimiento de la delincuencia organizada, el terrorismo y otras amenazas a la seguridad humana."* Hoy en día la corrupción es contemplada como uno de los mayores males globales<sup>70</sup>, y hay importantes iniciativas internacionales para luchar contra ella<sup>71</sup>.

Debido a la gran importancia de la corrupción en el comercio internacional, existen numerosos textos que ofrecen guías y directrices de cumplimiento. De estos textos internacionales se pueden extraer principios comunes sobre los que se han basado normas posteriores de distinta naturaleza<sup>72</sup>. Es indudable que la referencia global más importante son las directrices emitidas por la *US Sentencing Commission*, consideradas por el *Ethics Resource Center*<sup>73</sup> como un modelo idóneo para generar una *cultura ética en las organizaciones*.

Estas normativas nacionales deben ser conocidas por compañías multinacionales, en especial cuando se están incrementando los supuestos

---

<sup>69</sup>NACIONES UNIDAS, Oficina contra la Droga y el Delito: *"Convención de las Naciones Unidas contra la Corrupción"*, aprobada por la Resolución 58/4 de la Asamblea General de 31 de octubre de 2003.

<sup>70</sup>El 31 de octubre del 2003, en la Resolución 58/4, la Asamblea General de las Naciones Unidas *"decide que, a fin de aumentar la sensibilización respecto de la corrupción, así como del papel que puede desempeñar la Convención para combatirla y prevenirla, se proclame el 9 de diciembre Día Internacional contra la Corrupción"*.

<sup>71</sup>La iniciativa Global Compact de las Naciones Unidas propone un compromiso formal de las organizaciones frente a principios universales. <http://www.unglobalcompact.org>.

<sup>72</sup>CASANOVAS YSLA, A., *Legal compliance. Principios de cumplimiento generalmente aceptados*, Madrid, 2012, p. 95.

<sup>73</sup>ETHICS RESOURCE CENTER: *"2011 National Business Ethics Survey"*, disponible en <http://www.ethics.org>. El *Ethics Resource Center* es una organización norteamericana que desde 1922 está comprometida con la ética en los negocios.

de responsabilidad prácticamente objetiva ("*strict liability*") y los pasivos de naturaleza penal pueden ser objeto de sucesión entre empresas<sup>74</sup>.

Tal y como matiza A.Casanovas "*procede, pues, diferenciar entre textos que se proyectan sobre algunos comportamientos criminales<sup>75</sup> respecto de los que lo hacen sobre su generalidad: aunque de los primeros se pueden extraer conclusiones útiles para los segundos, no es técnicamente correcto considerar que un modelo de prevención contra la corrupción, por ejemplo, sea adecuado para prevenir y detectar otras conductas criminales<sup>76</sup>*".

Es necesario subrayar que el cumplimiento en materia penal no sólo es tratado en textos internacionales, sino que cada vez se regula en más normas nacionales, un dato evidente es que cada vez hay más países que han incorporado a su ordenamiento la responsabilidad penal de la persona jurídica, como es el caso de España<sup>77</sup>.

En este sentido debe también destacarse el conocido *Corruptum Perceptions Index* anual que publica la organización *Transparency International*<sup>78</sup>. Su mapa mundial, coloreado según las percepciones de corrupción, nos proporciona una visión alarmante acerca de la extensión de esta lacra en el comercio internacional: en el año 2016 ninguna región o país de los 176 analizados se podía considerar inmune a la corrupción en el sector público, y 86 de ellos eran percibidos como altamente corruptos<sup>79</sup>. Tal y como señala A. Casanovas "*es difícil alegar ignorancia y no disponer medidas de prevención*".

---

<sup>74</sup>Tal circunstancia, que es el caso por ejemplo de la regulación establecida en el 2015 en el Código Penal español, hace necesario revisar las posibles reclamaciones penales de un negocio antes de asumirlo.

<sup>75</sup>Por ejemplo acerca de la corrupción, soborno, blanqueo de capitales, terrorismo, narcotráfico, etc.

<sup>76</sup>CASANOVAS YSLA, A., *Legal compliance...*, ob. cit., pp. 95-96.

<sup>77</sup>En la página web de la OCDE (<http://www.oecd.org>) se hace referencia a 39 regulaciones nacionales relacionadas de algún modo con su Convención contra el Soborno, aunque se incluyen marcos de responsabilidad en un sentido más amplio que el de la mera corrupción.

<sup>78</sup><http://www.transparency.org>

<sup>79</sup>[http://issuu.com/transparencyinternational/docs/2016\\_cpireport\\_en?e=2496456/43483458](http://issuu.com/transparencyinternational/docs/2016_cpireport_en?e=2496456/43483458)

penal cuando se opera en jurisdicciones donde cualquier persona puede formarse un juicio sobre el riesgo de prácticas inadecuadas en ellas. Y no olvidemos que entre los países con una percepción de corrupción más elevada figuran economías emergentes habituales en los planes de expansión internacional de muchas organizaciones”<sup>80</sup>.

Las Líneas Directrices de la OCDE para Empresas Multinacionales<sup>81</sup> incluyen la corrupción como uno de los aspectos a considerar, mostrándose intolerantes frente a este tipo de conductas tanto en el ámbito público como en el privado y exigiendo el desarrollo de un *Ethics and Compliance Programme*, en el contexto de las medidas para prevenir y detectar estos comportamientos<sup>82</sup>.

A continuación se hace un breve repaso a los textos con más relevancia en materia de cumplimiento penal, algunos aplican a Estados y otros directamente a organizaciones, y de todos se extraen principios que son muy comunes en el ámbito del cumplimiento normativo<sup>83</sup>.

## **2.1 Convención contra el Soborno de la OCDE**

La OCDE adoptó en 1997 la Convención para Combatir el Soborno de Funcionarios Públicos Extranjeros en Transacciones Comerciales Internacionales (*Convention on Combating Bribery of Foreign Public Officials in International Business Transactions*), más conocida como la Convención contra el Soborno de la OCDE (*OECD Anti-Bribery Convention*), la cual entró en vigor el 26 de julio de 1999.

---

<sup>80</sup>CASANOVAS YSLA, A., *Legal compliance...*, ob. cit., pp. 96.

<sup>81</sup>OCDE: "Líneas Directrices de la OCDE para Empresas Multinacionales", revisión del año 2011([http:// www.oecd.org](http://www.oecd.org)).

<sup>82</sup>Tal y como sostiene A. CASANOVAS, la diligencia debida no sólo supone vigilar las conductas del personal de la organización, sino también supervisar la de terceros que se relacionan de manera estable con ella, recomendación que concurre en muchos de los textos sobre cumplimiento con la voluntad de impedir la comisión indirecta de ilícitos o la simple permisividad respecto de los mismos. CASANOVAS YSLA, A., *Legal compliance...*, ob. cit., p. 98.

<sup>83</sup>CASANOVAS YSLA, A., *Legal compliance...*, ob. cit., pp. 98-99.



La OCDE señala que *“el cohecho de servidores públicos para obtener ventajas en transacciones comerciales internacionales conlleva grandes consideraciones morales y políticas, socavando la gobernabilidad y el desarrollo económico sostenible y distorsionando la competencia. La corrupción en la adjudicación de contratos tiene costos sociales, políticos, ambientales y económicos, que ningún país puede ignorar. Existen serias consecuencias cuando los servidores públicos toman sobornos al adjudicar contratos a negocios extranjeros para servicios públicos como caminos, agua o electricidad. Un cohecho de un millón de dólares puede escalar a una pérdida de cien millones de dólares en un país asolado por la pobreza, porque los proyectos arruinados e inadecuada inversión socavan los planes de desarrollo”*<sup>84</sup>.

Esta Convención busca prevenir la comisión de actos de cohecho en transacciones comerciales internacionales de los países signatarios y promueve el establecimiento e imposición de sanciones a funcionarios públicos, personas, empresas y profesionales que encubran o participen en un acto de esta naturaleza. A través de ella se define el delito, la base jurisdiccional, las disposiciones secundarias y la organización de la cooperación mutua entre los estados miembros en asuntos de apoyo y extradición.

La Convención contra el Soborno de la OCDE es un acuerdo legalmente vinculante; los países que se unen a la Convención acuerdan establecer como delito el cohecho de un servidor público extranjero en su legislación nacional e implementar políticas efectivas para evitar, detectar, investigar y sancionar el cohecho internacional.

La Convención contra el Soborno de la OCDE es el primer y único instrumento internacional anticorrupción que se enfoca en el lado “oferente” de la corrupción, es decir la persona o entidad que ofrece, promete u otorga

---

<sup>84</sup><https://www.oecd.org/>

una dádiva. Este enfoque ha permitido a la OCDE convertirse en la autoridad más destacada del mundo contra el cohecho en transacciones comerciales internacionales.

Esta Convención exige que las leyes de soborno de los países signatarios se apliquen no sólo a particulares, sino también a las empresas, lo cual es clave para que éstas tengan responsabilidad ante las leyes de los actos de corrupción que se lleven a cabo en su beneficio. Además, los Estados miembros tienen la obligación de tipificar el soborno internacional en las legislaciones nacionales y se comprometen a establecer sanciones efectivas, proporcionadas y disuasorias para el delito de soborno a funcionarios extranjeros las cuales deben ser, al menos, comparables a las sanciones por soborno de funcionarios públicos nacionales.

La Convención también exige incluir jurisdicción sobre actos de corrupción cometidos en el país y en el extranjero y tomar medidas para garantizar que las decisiones para investigar o juzgar los casos de cohecho no estén influenciadas por consideraciones de interés económico. En este sentido, se deben prohibir las prácticas de contabilidad y auditoría que facilitan el ocultamiento de prácticas corruptas, requisitos cuyo cumplimiento puede considerarse, precisamente, parte de los cometidos de un programa de prevención penal. Al igual que las otras convenciones, la Convención de la OCDE insta a proporcionar asistencia técnica jurídica a los demás Estados parte para investigar y perseguir los actos de cohecho en el extranjero.

## **2.2 Recomendación OCDE para fortalecer la lucha contra el cohecho**

De la Convención contra el Soborno de la OCDE se deriva la Recomendación OCDE para fortalecer la lucha contra el cohecho<sup>85</sup> (*Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in*

---

<sup>85</sup> Texto accesible en <http://www.oecd.org/daf/anti-bribery/44176910.pdf> con los cambios introducidos el 18 de febrero de 2010.

*International Business Transactions*), adoptada el 26 de noviembre de 2009 que, a diferencia de lo que sucedía con la Convención, sí incorpora *recomendaciones concretas* en cuanto a controles internos y buenas prácticas para la prevención del cohecho<sup>86</sup>.

En particular, el Anexo II de dicho texto, que se actualizó el 18 de febrero de 2010, constituye una *Guía de Buenas Prácticas Sobre Controles, Ética y Cumplimiento*, sin carácter vinculante dirigida a las empresas (en particular pequeña y mediana empresa) con la finalidad de establecer y garantizar la efectividad de los controles internos, los programas de cumplimiento normativo y los códigos éticos o las medidas para prevenir y detectar el cohecho de funcionarios públicos en sus transacciones internacionales. La guía reconoce que para que las medidas y programas de una compañía sean efectivos deben de estar interconectados con la política de cumplimiento general.

### **2.3 Principios Empresariales para contrarrestar el Soborno, de Transparencia Internacional (TI)**

La ya citada *Transparency International*<sup>87</sup> es una organización mundial no gubernamental sin ánimo de lucro que se constituyó en 1993 con la finalidad de promover la lucha contra la corrupción, ya que en la práctica conlleva la vulneración de derechos humanos. Sus opiniones y recomendaciones son muy valoradas tanto por Estados como por organizaciones privadas.

Junto con la también organización no gubernamental *Social Accountability International*<sup>88</sup>, y con el apoyo de un grupo de empresas internacionales,

---

<sup>86</sup>CASANOVAS YSLA, A., *Legal compliance...*, ob. cit., pp. 100-101.

<sup>87</sup><http://www.transparency.org>

<sup>88</sup>Organización no gubernamental sin ánimo de lucro fundada en 1997, que procura mejorar los lugares de trabajo y comunidades alrededor del mundo, promoviendo estándares de aplicación voluntaria.

redactó en 2002 los Principios Empresariales para Contrarrestar el Soborno<sup>89</sup>, que conforman un marco de referencia para que las empresas de cualquier tamaño promuevan prácticas éticas en la lucha contra el soborno, tanto en las operaciones con funcionarios públicos como en las transacciones privadas, habiendo sido reconocidas como un entorno específico para la gestión del cumplimiento. Los principios que establece se basan en el compromiso de las empresas en la lucha contra la corrupción, prohibiendo cualquier forma de soborno, y estableciendo un programa para combatirlo. Estos dos principios, aparentemente simples, dan lugar a una elaborada construcción acerca de las acciones en que se traducen y aplican en la práctica, generando una Guía de gran utilidad así como un cuadro esquemático, que se elabora el año siguiente, y que ilustran los seis pasos a seguir para implementar de forma práctica los indicados principios. Para cada paso no sólo se apunta su objetivo, sino quién debe responsabilizarse de su ejecución, el proceso a seguir a tales efectos y el tiempo que normalmente se precisa para ello<sup>90</sup>.

Transparencia Internacional también ha publicado la edición para pequeñas y medianas empresas de los Principios Empresariales para Contrarrestar el Soborno, y señala que *“Son las pequeñas y medianas empresas las que dirigen gran parte de los negocios en todo el mundo, en particular en las economías emergentes. Esta edición de los Principios parte del principio de que las PYMES, en muchas sociedades del mundo, se enfrentan a menudo al problema del soborno. Tratándose de empresas más pequeñas y con recursos limitados, resistir y luchar contra tales presiones constituye para las PYMES un gran desafío. Además, las grandes empresas internacionales imponen cada vez más requisitos a sus proveedores para que presenten pruebas de que disponen de políticas y sistemas contra el soborno. Esta edición se propone exponer, de un modo claro y directo, el proceso mediante*

---

<sup>89</sup>Tanto el documento con los Principios, como la Guía sobre los mismos y los pasos para su implementación se pueden descargar de su página web <http://www.transparency.org>.

<sup>90</sup>CASANOVAS YSLA, A., *Legal compliance...*, ob. cit., pp. 103-104.

*el cual las empresas pequeñas y medianas pueden desarrollar un programa adecuado para luchar contra el soborno, en función de su tamaño y recursos. Combatir el soborno es una buena práctica comercial. Puede ayudar a forjar la reputación, en especial de cara a los clientes, y también puede reducir riesgos. Construyendo una cultura antisoborno fuerte, las PYMES lograrán desafiar y resistir con éxito al soborno*<sup>91</sup>.

## **2.4 Principios Partnering Against Corruption Initiative**

Los Principios *Partnering Against Corruption Initiative* (PACI)<sup>92</sup> nacen de la iniciativa de tres organizaciones de gran prestigio en materia de promoción de buenas prácticas empresariales a nivel internacional: el *World Economic Forum* en asociación con *Transparency International* y el *Basel Institute on Governance*. Puesto que la Convención contra el Soborno de la OCDE (1997) no establecía directrices concretas en materia de cumplimiento y antes de que dicha organización emitiese sus Recomendaciones contra el Soborno (2009), PACI quiso facilitar unas directrices más concretas que permitiesen a las empresas aplicar de forma efectiva las recomendaciones para luchar contra la corrupción que provenían tanto de dicho entorno como de tantas otras iniciativas privadas.

Estos principios se emitieron inicialmente en el año 2004, proyectándose sobre el sector de la ingeniería y construcción, aunque más tarde se extendieron para empresas de cualquier sector e industria y se enmarcaron formalmente en la iniciativa que se denominó PACI. Se resumen en un programa que implica que la organización declare tolerancia cero respecto a actos de soborno y que desarrolle programas efectivos de cumplimiento que garanticen dicha máxima<sup>93</sup>. El objetivo de los principios PACI es proporcionar un marco de buenas prácticas empresariales y estrategias de gestión de

---

<sup>91</sup>[https://www.transparency.org/whatwedo/publication/principios\\_empresariales\\_para\\_contrarrestar\\_el\\_soborno\\_edicion\\_para\\_pequena](https://www.transparency.org/whatwedo/publication/principios_empresariales_para_contrarrestar_el_soborno_edicion_para_pequena)

<sup>92</sup><http://www.weforum.org/issues/partnering-against-corruption-initiative>

<sup>93</sup>CASANOVAS YSLA, A., *Legal compliance...*, ob. cit., pp. 106-107.

riesgos para combatir el soborno. Su objetivo es ayudar a las empresas a: eliminar el soborno, demostrar su compromiso para combatir el soborno, aportar una contribución positiva a la mejora de la integridad empresarial y transparencia donde quieran que operen las compañías<sup>94</sup>.

## **2.5 Convención de las Naciones Unidas contra la Corrupción**

Tal y como señala Alain Casanovas la Convención de las Naciones Unidas Contra la Corrupción (*United Nations Convention Against Corruption/UNCAC*) por su gran relevancia en la comunidad internacional, es una norma que, aunque no incorpora directrices de cumplimiento detalladas, tiene un gran valor interpretativo<sup>95</sup>.

La UNCAC<sup>96</sup>, firmada en el año 2003, es el primer instrumento internacional con vocación global para prevenir y luchar no sólo contra el cohecho, sino contra diferentes conductas en las que se traduce la corrupción. Apremia a los Estados parte que adopten una serie de medidas que se proyectan sobre el sector privado, incluyendo la promoción de códigos de conducta para el correcto y debido ejercicio de las actividades comerciales. Asimismo, insta a velar por que las empresas privadas dispongan de suficientes controles contables internos para ayudar a prevenir y detectar eventuales actos de corrupción.

## **2.6 Reglas de conducta y recomendaciones de la CCI para combatir la extorsión y el soborno**

La CCI fue la primera asociación de negocios en emitir un marco de reglas anticorrupción con la publicación en 1977 de las Reglas de Conducta para el Combate a la Extorsión y al Soborno. Dichas Reglas pretenden ser un método de autorregulación por parte de los negocios internacionales y

---

<sup>94</sup>[http://www3.weforum.org/docs/WEF\\_PACI\\_Principles\\_2009.pdf](http://www3.weforum.org/docs/WEF_PACI_Principles_2009.pdf)

<sup>95</sup>CASANOVAS YSLA, A., *Legal compliance...*, ob. cit., pp. 107-108.

<sup>96</sup>Texto accesible en <http://www.unodc.org>

constituir lo que se considera una buena práctica comercial en la lucha contra la corrupción. Estas reglas de la CCI responden directamente a la llamada del G-20 y al requerimiento de la UNCAC para que las empresas aumentaran sus esfuerzos para luchar contra la corrupción.

En el año 2011<sup>97</sup> han sido revisadas y actualizadas. Las reglas proporcionan un modelo de cumplimiento que es aplicable a empresas grandes, medianas y pequeñas, y están construidas sobre la base de otros documentos preparados por la CCI como el “Manual de Combate a la Corrupción, Prácticas Corporativas” y varios documentos sobre temas específicos de integridad.

## **2.7 Manual de Directrices de la US Sentencing Commission**

La *United States Sentencing Commission*<sup>98</sup> es una agencia independiente dentro del poder judicial norteamericano, cuyo propósito es establecer políticas y prácticas para dictar sentencias en los tribunales federales, incluyendo ciertas pautas con respecto a la graduación de la sanción por delitos federales<sup>99</sup>; asesorar y asistir al Congreso para desarrollar una política criminal eficaz y eficiente; y recopilar, analizar, investigar y distribuir una información detallada sobre delitos federales y cuestiones relativas a sus sentencias, sirviendo como un recurso de información para el Congreso, el Poder Ejecutivo, los tribunales, los profesionales de la justicia penal, y la comunidad en general.

Por medio de un Manual de Directrices (*Guidelines Manual*) que revisa y publica anualmente, difunde los criterios destinados a dotar de uniformidad a

---

<sup>97</sup>La Edición de 2011 está basada en numerosas contribuciones hechas por los comités nacionales de la ICC, compañías miembro, y expertos de la Comisión de Responsabilidad Corporativa y Anticorrupción.

<sup>98</sup><http://www.ussc.gov>

<sup>99</sup>ZYSMAN BERNALDO DE QUIRÓS, D., *Castigo y determinación de la pena en los Estados Unidos: Un estudio sobre las United States Sentencing Guidelines*, ed. Marcial Pons Ediciones Jurídicas y Sociales, S.A., Madrid, 2013, pp 13 y ss.

las resoluciones emitidas ante supuestos similares. Su capítulo 8, destinado a las sentencias sobre organizaciones, comprende la descripción de un *Effective Compliance and Ethics Program*, que actúa como factor a considerar para calcular el llamado *culpability score* de una organización. A pesar de que el sistema de responsabilidad penal norteamericano se declara abiertamente vicarial, vinculando el nacimiento de la responsabilidad criminal de la organización a las conductas ilícitas que hayan cometido sus personas físicas, la existencia de un programa de cumplimiento impacta notablemente en sus consecuencias en términos de graduación de la pena. El *Effective Compliance and Ethics Program* de la *US Sentencing Commission* se considera un importante referente para empresas nacionales y extranjeras, de aplicación no sólo para la prevención penal sino también para crear una cultura ética en las organizaciones<sup>100</sup>.

Para la *US Sentencing Commission*, un *Effective Ethics and Compliance Program* debe permitir ejercer la debida vigilancia para *prevenir y detectar* conductas criminales. Además, debe promover una cultura organizativa que facilite las conductas éticas y el compromiso con el cumplimiento de la Ley. Sin embargo, el hecho de que el programa falle en prevenir o detectar determinada conducta penal no significa que sea inefectivo en términos generales, aunque también es cierto que la reiteración de conductas criminales de la misma naturaleza cuestiona la adecuación del modelo.

Partiendo de estas nociones, la *US Sentencing Commission* describe los *siete requisitos* que debe cumplir un programa de prevención penal para que se considere un *Effective Ethics and Compliance Program*. A continuación paso a reproducir los comentarios a cada requisito del experto en la materia Alain Casanovas<sup>101</sup>:

---

<sup>100</sup>ZYSMAN BERNALDO DE QUIRÓS, D., *Castigo y determinación...*, ob. cit., pp. 168 y ss.

<sup>101</sup>CASANOVAS YSLA, A., *Legal compliance...*, ob. cit., pp. 110 a 112.



- Patrones y Procesos: La organización se dotará de patrones de conductas (normalmente en lo que otros textos clasifican como políticas) y procesos para prevenir y detectar la conducta criminal.
- Involucración de alto nivel: El órgano de gobierno social debe conocer el programa de cumplimiento y ejercer una supervisión razonable respecto de su desarrollo y efectividad. El personal de alto nivel se asegurará de que la organización disponga del programa y designará responsables, también de alto nivel, con responsabilidad general respecto del mismo. Sin perjuicio de ello, se delegarán a otras personas las actividades diarias que resulten del programa de cumplimiento penal, que reportarán sobre su efectividad a los responsables de alto nivel y, cuando sea adecuado, incluso al órgano de gobierno o comisión específica al efecto. Para ello, a estas personas delegadas se les facilitarán los recursos y autoridad adecuados, incluyendo acceso directo al órgano de gobierno o comisión específica al efecto.
- Diligencia debida en la elección de personas: Se evitará designar como empleados con cierto nivel de responsabilidades a personas de las que se conozca o debiera conocerse, que han estado involucradas en actividades ilegales o incompatibles con el programa de *compliance*.
- Comunicación y formación: La organización debe cuidarse en comunicar de forma periódica y práctica los patrones de conducta, procesos y otros elementos que conformen el programa de ética y cumplimiento a todo el personal de la organización (incluyendo administradores y empleados) así como a terceros que actúan en nombre de la organización. Se conseguirá este objetivo impartiendo formación o difundiendo información adecuada sobre funciones y responsabilidades.
- Monitorización: Para asegurarse de que el programa de ética y cumplimiento es observado, se hará un seguimiento del mismo y auditorías para detectar conductas criminales. Se evaluará periódicamente la efectividad del modelo y

se dará publicidad a un mecanismo que permita a empleados y terceros que trabajan para la organización pedir consejo o denunciar comportamientos ilícitos de forma anónima y confidencial.

- Régimen disciplinario: Se establecerá un mecanismo de incentivos respecto del cumplimiento del programa de *compliance*, así como las medidas disciplinarias oportunas tanto por desarrollar actividades ilegales como por no actuar razonablemente en la prevención y detección de conductas criminales.
- Respuesta ante el delito: Tras detectarse alguna conducta ilícita, se adoptarán los pasos adecuados tanto para responder a ella como para prevenir en el futuro otras conductas similares.

La *US Sentencing Commission* establece diferencias respecto del modo en que las empresas pueden dar cumplimiento a sus directrices dependiendo del tamaño ya que es comprensible que sus requisitos pueden resultar demasiado gravosos para las pequeñas empresas. De este modo, en grandes organizaciones cabe esperar una dedicación mayor de recursos y también mayores formalismos, así como que motiven a las pequeñas empresas con las que se relacionan para que dispongan de un *Effective Compliance and Ethics Program*. De una organización grande se espera, pues, *cierto compromiso de ejemplo y difusión*<sup>102</sup>.

## **2.8 Breve apunte sobre la normativa internacional de compliance en el sector financiero**

### **2.8.1 En Estados Unidos**

A comienzos del siglo XXI, la sociedad empezó a tomar conciencia sobre la importancia de que existiese un control sobre las operaciones realizadas por sociedades financieras cotizadas como consecuencia de los conocidos

---

<sup>102</sup>CASANOVAS YSLA, A., *Legal compliance...*, ob. cit., p. 113.

escándalos financieros de la época (Enron<sup>103</sup>, WorldCom, Parmalat, Royal Dutch Shell, o Peregrine Systems entre otras) que conllevaron unas cuantiosas pérdidas económicas, la destrucción de miles de puestos de trabajo y un impacto tremendamente negativo en la reputación de las empresas involucradas, de la propia nación estadounidense e incluso del sistema económico de mercado.<sup>104</sup> Pues bien, es a partir de esta ola de corrupción y de malas prácticas en el sector de los mercados de valores por parte de algunos profesionales y ejecutivos, quienes engañaron a socios, empleados y grupos de interés; cuando el gobierno norteamericano se ve forzado a promulgar la Ley<sup>105</sup> Sarbanes-Oxley Act of 2002, y a fortalecer la SEC, para la regulación financiera y la actividad contable pública<sup>106</sup>.

En este contexto, se promulga la SOX con el objetivo de proteger al inversor y controlar las empresas que cotizan en la bolsa de valores de Nueva York y sus filiales, y evitar fraudes y riesgo de bancarrota, protegiendo al inversor.

Tal y como dice M. BALLBÉ *“Ciertamente, la Sarbanes- Oxley Act de 2002 se ha valorado como una eficaz regulación administrativa para atajar las prácticas fraudulentas. Esta Ley viene a reforzar los organismos watchdog y la responsabilidad de los directivos, contables y abogados”*<sup>107</sup>. Esta ley establece importantes obligaciones de reporte que aplican a todas las

---

<sup>103</sup>Algunos autores aseguran que diez años después, las lecciones del caso Enron han impactado más que la Propia Ley Sarbanes-Oxley Act promulgada en 2002. PEREGRINE, M.W., “Another View: Sarbanes-Oxley and the Legacy of Enron”, November 25, 2011, NY, extraído de: [https://dealbook.nytimes.com/2011/11/25/another-view-sarbanes-oxley-and-the-legacy-of-enron/?\\_r=0](https://dealbook.nytimes.com/2011/11/25/another-view-sarbanes-oxley-and-the-legacy-of-enron/?_r=0)

<sup>104</sup>CALDERÓN MARTÍN, J., “Compliance en la normativa sectorial”, AA.VV., *Compliance. Cómo gestionar los riesgos normativos en la empresa*, coord. C.A. Sáiz Peña, Pamplona, 2015, ob. cit., p. 484.

<sup>105</sup>La SOX entró en vigor en 2002 e introdujo grandes cambios a la regulación financiera y de gobierno corporativo. Nombrado después del senador Paul Sarbanes y del representante Michael Oxley, que eran sus principales arquitectos, también fijó una serie de plazos para el cumplimiento.

The Sarbanes-Oxley Act is arranged into eleven titles. As far as compliance is concerned, the most important sections within these are often considered to be 302, 401, 404, 409, 802 and 906. Una guía <http://www.soxlaw.com/>

<sup>106</sup><https://www.auditool.org/blog/control-interno/2651-lo-que-todo-auditor-debe-conocer-de-sox>

<sup>107</sup>BALLBÉ, M. *“El futuro del derecho administrativo en la globalización: entre la americanización y la europeización”*, ob. cit., pp 232.

entidades que coticen en bolsas de Estados Unidos, con total independencia de la nacionalidad de dichas sociedades<sup>108</sup>.

La Ley garantiza la integridad y precisión de los informes financieros de las empresas cotizadas incrementando el nivel y los controles internos de las compañías<sup>109</sup>, mediante su monitorización y control y la implementación de medidas preventivas que garanticen la integridad y precisión de sus informes financieros. Asimismo regula las funciones financieras contables y de auditoría, y penaliza el crimen corporativo. La SOX ha regulado en Estados Unidos diversos controles para mejorar la calidad de la información financiera, teniendo como base las normas de contabilidad, control interno, gobierno corporativo, independencia de las auditorías y el aumento de las sanciones por delitos financieros.<sup>110</sup>

A grandes rasgos dichos controles deben cumplir con las siguientes obligaciones:

- Deben establecer un método de evaluación de su estado financiero que asegure unas condiciones de veracidad y eficiencia.
- Debe formarse un comité interno de auditoría que supervise y verifique el estado financiero de la compañía. De igual manera la empresa debe someterse a auditorías externas independientes que garanticen la veracidad de los resultados de la aplicación de los controles internos.
- Se imponen límites a los beneficios que puedan otorgarse a los directivos de dichas empresas, como por ejemplo la prohibición de que la empresa pueda conceder préstamos personales.

---

<sup>108</sup>UNITED STATES CONGRESS HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES, *Sarbanes-oxley: Two Years Of Market And Investor Recovery*, Ulan Press, 2011, pp. 3 y ss.

<sup>109</sup>ESPINO GARCÍA, M.G., *Fundamentos de la Ley Sarbanes-Oxley*, Ed. IMCP, 2017, p. 20.

<sup>110</sup><https://www.auditool.org/blog/control-interno/2651-lo-que-todo-auditor-debe-conocer-de-sox>

- Se establece la obligación de implantar un sistema que garantice la transparencia de la información en relación con las acciones u opciones que tienen, principalmente, los directivos de la sociedad.
- Deben redactarse informes periódicos en relación con el estado financiero de la entidad que deben quedar sujetos a revisión por parte de las auditorías establecidas<sup>111</sup>.

Las consecuencias del incumplimiento de lo anterior conllevan una responsabilidad civil con importantes sanciones económicas. Asimismo, se establece un sistema de responsabilidad penal, que incluye penas de prisión y cuantiosas multas que se aplicarán a los ejecutivos que hayan incurrido en dichos incumplimientos o que hayan permitido que se incurriese en los mismos<sup>112</sup>.

Unos años después del Informe Final de la Comisión Nacional de las Causas de la Crisis Financiera y Económica en Estados Unidos elaborado por la Comisión de Investigación sobre la Crisis Financiera<sup>113</sup> ("FCIC") en enero de 2011, la FCIC concluyó que la crisis financiera era "*el resultado del fracaso de las instituciones financieras en preguntar, entender, y gestionar la evolución de los riesgos en un sistema esencial para el bienestar del público Americano*"<sup>114</sup>.

El análisis más detallado de la FCIC reveló lo que se describe como "*casos impresionantes de fallos en el gobierno corporativo e irresponsabilidad*" proporcionando ejemplos como la ignorancia de los altos gestores de AIG respecto de los términos y de los riesgos de la compañía en productos

---

<sup>111</sup>CALDERÓN MARTÍN, J., "Compliance en la normativa sectorial", ob. cit., p. 485.

<sup>112</sup>Los inversores internacionales indican claramente que los riesgos regulatorios asociados con la SOX son un impedimento severo para invertir en el mercado de capitales americano. CHAN, S., *Sarbanes Oxley*, Edt. Risk Books, 2006, pp. 1 y ss.

<sup>113</sup>*Financial Crisis Inquiry Commission*.

<sup>114</sup>Ver *Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States*, Comisión de Investigación sobre la Crisis Financiera, enero de 2011 en <http://www.gpo.gov/fgsys/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf>.

derivados de valores relacionados con hipotecas por un importe de \$79 mil millones, la búsqueda de mayor cuota de mercado de Fannies Mae, beneficios, y bonificaciones, que tuvieron como consecuencia una exposición en préstamos y valores arriesgados cuando el mercado de la vivienda estaba en su nivel más alto o el descubrimiento de la alta dirección de Merrill Lynch en el último momento en que la compañía tenía \$55 mil millones en valores supuestamente “*súper-seguros*” relacionados con hipotecas que dieron lugar a pérdidas de miles de millones de dólares<sup>115</sup>.

La preocupación sobre el gobierno corporativo y responsabilidad y la gestión de riesgos fueron factores significativos en la promulgación en el año 2010 de la Ley Dodd-Frank de reforma financiera y de protección de los consumidores. En la ceremonia de firma de la misma, el Presidente Obama declaró:

*Aunque numerosos factores han conducido a una fuerte recesión, la principal causa ha sido un fallo en nuestro sistema financiero. Ha sido la crisis nacida del fracaso en la responsabilidad desde ciertas esquinas de Wall Street hasta los pasillos de poder en Washington. Durante años, nuestro sector financiero ha estado gobernado por anticuadas y deficientes normas de obligado cumplimiento que permitieron a algunos jugar con el sistema y asumir riesgos que amenazaron la economía en su totalidad.*<sup>116</sup>

Además de los cambios profundos causados en el panorama de la regulación financiera, la Ley Dodd-Frank incluyó varias disposiciones específicas relacionadas con el gobierno corporativo y *compliance*. En el área del gobierno corporativo, la Ley Dodd-Frank contenía disposiciones relacionadas

---

<sup>115</sup>KOTZ, H. D., *Financial Regulation and Compliance. How to manage Competing and Overlapping Regulatory Oversight*, Edit. John Wiley & Sons, Inc, New York, 2015, pp. 24 y ss.

<sup>116</sup>Ver *Remarks by the President at Signing of Dodd-Frank Wall Street Reform and Consumer Protection Act*, 21 de julio de 2010 en <http://www.whitehouse.gov/the-press-office/remarks-president-signing-dodd-frank-wall-street-reform-and-consumer-protection-act>.

con: (a) el voto consultivo de los accionistas en la remuneración ejecutiva y contratos blindados; (b) limitaciones en el voto discrecional por los agentes; (c) retroacción en los incentivos de compensación; (d) independencia de los comités de compensación; (e) aumento del poder de revelación; (f) incentivos y protección del *whistleblower*; y (g) poder de acceso.

En el mismo año el Congreso de Estados Unidos también aprobó la *Foreign Account Tax Compliance Act* que entró en vigor en 2013 (más conocida por su acrónimo "FACTA") con el objetivo de luchar contra la evasión fiscal de nacionales o residentes norteamericanos en las operaciones que realizan fuera de las fronteras de EE.UU.<sup>117</sup>

En virtud de esta Ley el Internal Revenue Service (IRS. Servicio Interno de Beneficios), la autoridad fiscal en Estados Unidos, solicita a las instituciones financieras de todo el mundo que le reporten información sobre los activos y operaciones que sean titularidad de nacionales que residan fuera de Estados Unidos<sup>118</sup>. Si las entidades obligadas a reportar la anterior información no cumpliesen con su deber esto acarrearía importantes consecuencias y multas, el IRS puede incluso instar a la prohibición de cualquier tipo de operación a la entidad en cuestión<sup>119</sup>.

No obstante, para evitar problemas legales y costes de transacción a efectos de lograr el cumplimiento de tal normativa interna extraterritorial por parte de las entidades financieras extranjeras, EE.UU. ha articulado mecanismos alternativos tales como Acuerdos Intergubernamentales para implementar la FATCA. De hecho, EE.UU. ha elaborado varios modelos de acuerdo

---

<sup>117</sup>CALDERÓN MARTÍN, J., "Compliance en la normativa sectorial", ob. cit., p. 483.

<sup>118</sup>Ya que de acuerdo con ley norteamericana los impuestos de sus ciudadanos quedan gravados aunque residan fuera del país, incluso por las ganancias obtenidas en operaciones en el extranjero. Es fundamental tener en cuenta lo anterior desde el prisma del cumplimiento normativo, ya que aproximadamente 6 millones de ciudadanos estadounidenses viven fuera del país.

<sup>119</sup>Para las entidades financieras que no acepten firmar acuerdos con el IRS, la ley prevé que las transferencias de rendimientos y otros conceptos provenientes de esos activos en el exterior, estén sujetos a una retención del 30%. Esta sanción por no reportar la información supone en la práctica una prohibición para hacer negocios en Estados Unidos.

intergubernamental (IGAs), considerando las distintas circunstancias en las que se negocia cada acuerdo con cada país. El FATCA acordado con España responde al denominado Modelo 1A IGA Reciprocal, Preexisting TIEA or DTC, pudiendo mencionarse otros acuerdos IGA firmados con otros países como Reino Unido, Dinamarca, México, Irlanda, Suiza, Noruega, Alemania y Japón (IGA Modelo 2)<sup>120</sup>.

### **2.8.2 En Europa**

En Europa, en particular en los 28 Estados que conforman la Unión Europea, así como en otros pertenecientes al Área Económica Europea, se ha establecido un marco común que regula el mercado de instrumentos financieros cuyo objetivo es fijar un régimen homogéneo en el sector de los servicios financieros protegiendo sobre todo a los inversores y consumidores.

La Directiva 2004/39/EC sobre Mercados de Instrumentos Financieros, conocida por sus siglas en inglés como MiFID<sup>121</sup> (*Markets in Financial Instruments Directive*) entró en vigor en noviembre de 2007 y es la piedra angular de la regulación de los mercados financieros de la Unión Europea. La MiFID nace con la mencionada vocación de proteger a los inversores y fomentar la transparencia de las operaciones que realizan las entidades financieras frente a las mismas.

Al haberse articulado dicha regulación en forma de Directiva de la Unión Europea, los distintos Estados Miembros tuvieron cierto margen para transponer dichas obligaciones a su ordenamiento interno a través de su normativa nacional. Sin embargo debe resaltarse que las normas MiFID regularon cada uno de los aspectos que trataban con un alto grado de detalle,

---

<sup>120</sup><http://www.gomezacebo-pombo.com/media/k2/attachments/el-acuerdo-fatca-estados-unidos-espana-sobre-control-fiscal-de-cuentas-financieras-extranjeras.pdf>

<sup>121</sup>La Directiva 2004/39/CE y la Directiva 2006/73/CE componen, junto con el Reglamento (CE) 1287/2006, de directa aplicación desde su entrada en vigor el 1 de noviembre de 2007, la normativa comunitaria conocida coloquialmente como MiFID 6, que pretende crear un marco jurídico único armonizado en toda la Unión Europea para los mercados de instrumentos financieros y la prestación de servicios de inversión.



y además restringieron y condicionaron la capacidad de los Estados miembros de establecer, e incluso conservar, requisitos adicionales al margen de lo establecido por las referidas normas<sup>122</sup>.

Quedan sujetas a la MIFID aquellas entidades que participen en el mercado de instrumentos financieros, estableciendo importantes obligaciones de transparencia e información. Desde un punto de vista del cumplimiento normativo, los aspectos más relevantes de la MiFID están en relación con el establecimiento de controles internos que se refieran a los siguientes aspectos<sup>123</sup>:

- Las entidades obligadas por la MiFID deben obtener una autorización y haber sido reguladas en el Estado donde se encuentre la entidad matriz.
- Se establece la obligación de diferenciar a los clientes en categorías como contrapartes elegibles, clientes profesionales y clientes minoristas. A cada categoría se le debe ofrecer una protección diferente, que será mayor para los clientes minoristas, dado su menor conocimiento del mercado.
- Los operadores de mercados deben disponer de información clara y suficiente sobre las operaciones que realizan; deben hacer pública la información de pre-venta y cumplir con ciertos requisitos de cara a los inversores, así como información posterior a las ventas realizadas.
- Las entidades deben asegurar que tomarán todas las medidas necesarias para obtener el mejor resultado posible para atender a las órdenes de sus clientes.

---

<sup>122</sup>El Artículo 4 de la Directiva 2006/73/CE sólo permite a los Estados Miembros mantener o imponer requisitos adicionales al margen de la MiFID en supuestos excepcionales y siempre que se cumplan ciertas condiciones. Además les obliga a su comunicación a la Comisión Europea incluyendo su necesaria justificación. Es evidente que el espíritu del precepto es limitar hasta casi prohibir la libertad de los Estados miembros de apartarse de lo contenido en la MiFID en su transposición a la legislación nacional. DÍAZ RUIZ, E./ RUIZ BACHS, S., "Transposición de MiFID en España", en *Actualidad Jurídica Uría Menéndez*, nº 19, 2008, extraído de <http://www.uria.com/documentos/publicaciones/1924/documento/articuloUM.pdf?id=3171>.

<sup>123</sup>CALDERÓN MARTÍN, J., "Compliance en la normativa sectorial", ob. cit., pp. 485-486.

- Se establece una regulación exhaustiva para los denominados Intercambiadores Sistemáticos.

El 20 de octubre de 2011, la Comisión Europea adoptó una propuesta legislativa para la revisión de la MiFID en forma de una Directiva revisada y un nuevo Reglamento. Tras más de dos años de intensos debates, se adoptó la Directiva sobre mercados de instrumentos financieros por la que se deroga la Directiva 2004/39/CE y el Reglamento sobre mercados de instrumentos financieros, comúnmente denominados como MiFID II y MiFIR, fueron adoptadas por el Parlamento Europeo el 15 de abril 2014, por el Consejo de la Unión Europea el 13 de mayo de 2014 y publicada en el Diario Oficial de la Unión Europea el 12 de junio de 2014.

El comisario Michel Barnier ha llegado a resumir el espíritu de la MiFID II así: *“Hará que la negociación organizada de los instrumentos financieros se desarrolle en plataformas de negociación multilaterales y bien reguladas. Se establecen también reglas de transparencia estrictas que prohibirán la negociación anónima de las acciones y de otros instrumentos que puedan ser obstáculo para la formación de precios. Asimismo, las empresas de inversión deberán respetar normas más estrictas a fin de que los inversores puedan estar seguros de que los productos en los que invierten están adaptados a su perfil y que sus activos están bien protegidos. Se establece un sistema que limitará las posiciones que los traders tienen en derivados de materias primas y respecto a las operaciones de trading de alta frecuencia, las entidades que lo realicen deberán poner en marcha sistemas de corto circuito para evitar la fuga masiva de los activos”*<sup>124</sup>.

La Directiva MiFID II, entrará en vigor el próximo 3 de enero de 2018, está inspirada en las premisas de la seguridad, la eficacia y la transparencia de los

---

<sup>124</sup>[http://europa.eu/rapid/press-release\\_MEMO-14-15\\_en.htm?locale=en](http://europa.eu/rapid/press-release_MEMO-14-15_en.htm?locale=en)

mercados en aras de la mayor protección de los inversores y el fortalecimiento de las facultades de supervisión<sup>125</sup>.

Basándose en las normas ya establecidas, estas nuevas normas están diseñadas para tener en cuenta la evolución del entorno comercial desde la aplicación de la MiFID en 2007 y, a la luz de la crisis financiera, para mejorar el funcionamiento de los mercados financieros haciéndolos más eficientes, y transparente.

De manera paralela, tal y como sucedió en Estados Unidos, en la última década la necesidad de supervisión y control sobre las entidades cotizadas también ha sido prioridad en Europa dadas las deficiencias encontradas en la transparencia de las operaciones y estados financieros de las empresascotizadas. Así, en mayo del año 2006 entró en vigor en la Directiva 2006/43/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006<sup>126</sup>, que requiere a los departamentos de auditoría de las entidades cotizadas que supervisen la manera en que presentan la información financiera, la eficacia de sus controles internos y sus sistemas de gestión de riesgos. En esta misma línea, se aprobó la Directiva 2006/46, que requiere a las citadas entidades para que faciliten a los mercados donde operan una descripción de las características de sus sistemas de control interno y gestión de riesgos.

En España, con el objetivo de adaptar a las entidades españolas al citado marco regulatorio, la Comisión Nacional del Mercado de Valores (CNMV) constituyó un Grupo de Trabajo para elaborar una propuesta normativa en materia de Sistemas de Controles Internos de la Información Financiera (SCIIF). De esta manera se fijaron unos principios generales y buenas

---

<sup>125</sup>TROIANO, V. / MOTRONI, R., *La MiFID II: Rapporti con la clientela - regole di governance – mercati*, Milano, 2016.

<sup>126</sup>Directiva 2006/43/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a la auditoría legal de las cuentas anuales y de las cuentas consolidadas, por la que se modifican las Directivas 78/660/CEE y 83/349/CEE del Consejo y se deroga la Directiva 84/253/CEE del Consejo

prácticas en relación con el control interno en las que se basaron las entidades a la hora de implantar sus SCIIF<sup>127</sup>.

Desde un punto de vista del cumplimiento de las obligaciones normativas, el seguimiento de las recomendación de la CNMV asegura que las obligaciones de gestión de riesgos y presentación de la información financiera (íntimamente ligadas con otras obligaciones de reporte, como la necesidad de elaborar un Informe Anual de Gobierno Corporativo) se cumplirán de acuerdo a unos estándares predefinidos que garantizarán un mínimo de eficacia. Dichas obligaciones no están dirigidas exclusivamente a los comités de auditoría interna, sino que dependerá de los propios Consejos de Administración de las empresas cotizadas acordar e implantar unos SCIIF que conformen la cultura corporativa a todos los niveles y departamentos de sus sociedades.

La CNMV propone una serie de medidas que afectan directamente al nivel de concienciación del personal de la organización:

- Elaborar una declaración de valores éticos (códigos de conducta), en relación con la veracidad y fiabilidad de la información financiera y con el cumplimiento de la normativa aplicable.
- Establecer unos procedimientos para la supervisión y corrección de cualquier incumplimiento de los principios que conforman la ética profesional de la compañía.
- Seguir un criterio coherente para la designación de los comités de auditoría, basado en todo caso en sus conocimientos y experiencia en contabilidad, auditoría o gestión de riesgos<sup>128</sup>.

---

<sup>127</sup>El texto íntegro del Informe de la CNMC se puede consultar en [https://www.cnmv.es/DocPortal/Publicaciones/Grupo/Control\\_interno\\_sciifc.pdf](https://www.cnmv.es/DocPortal/Publicaciones/Grupo/Control_interno_sciifc.pdf)

<sup>128</sup>CALDERÓN MARTÍN, J., "Compliance en la normativa sectorial", ob. cit., pp. 487-488.

- Establecer unas líneas apropiadas de autoridad y responsabilidad en los procesos de elaboración de la información financiera.

Es importante para establecer un SCIIF eficiente tener en cuenta que no es suficiente establecer un código de buenas prácticas, sino que será necesario implantar un correcto sistema de supervisión de dicho SCIIF.

Por último, es imprescindible hacer una mención brevísima a los denominados Acuerdos de Basilea, que son una serie de convenios emitidos por el Comité de Basilea de Regulación Bancaria que establecen recomendaciones relativas a regulación bancaria<sup>129</sup>. Dicho Comité estaba, en su origen, compuesto por representantes de los bancos centrales y otras autoridades de regulación bancaria de los por entonces conocidos como Grupo de los Diez, España y Luxemburgo. En la actualidad, el resto de países significativos del G-20, así como otras grandes potencias bancarias como Hong Kong y Singapur están igualmente representados en este Comité. Aunque sus directrices son de naturaleza puramente facultativa, la gran mayoría de los integrantes tienden a implantar las políticas dotándolas de un carácter normativo<sup>130</sup>.

---

<sup>129</sup>La definición que hace el Comité de Basilea de cumplimiento es: "una función independiente que identifica, asesora, alerta, monitorea y reporta los riesgos de cumplimiento en las organizaciones, es decir, el riesgo de recibir sanciones por incumplimientos legales o regulatorios, sufrir pérdidas financieras o pérdidas de reputación por faltas de cumplimiento con las leyes aplicables, las regulaciones, los códigos de conducta y los estándares de buenas prácticas (juntos "leyes, reglas y estándares")".

<sup>130</sup>CALDERÓN MARTÍN, J., "Compliance en la normativa sectorial", ob. cit., pp. 488-489.

### III. PROGRAMAS DE CUMPLIMIENTO

#### 1. Definición y Objetivo

El propósito principal de los denominados programas de cumplimiento es asegurar que las actividades de la empresa no incumplan la legislación vigente y aplicable, e incluso más, no vulneren los propios estándares éticos autoimpuestos por la empresa.<sup>131</sup> Se trata de procedimientos y reglas que, aunque en principio no están dotados de fuerza jurídicamente vinculante, despliegan, sin embargo, una importante fuerza de obligatoriedad y coercibilidad, en virtud de su capacidad de persuasión y de represión<sup>132</sup>. Este código de conducta se puede definir como *“el conjunto de medidas adoptadas por la empresa para controlar dentro de lo exigible los peligros de infracción al ordenamiento jurídico que pueden derivar de su misma actividad”*<sup>133</sup>.

Tal y como ha sucedido en España, una vez que las personas jurídicas pueden ser penalmente punibles, debe estudiarse qué posibilidades de defensa tienen. Tal y como sostiene O. ARTAZA *“esta posibilidad de defensa surge en todo caso, lo prevean o no en forma expresa las diversas disposiciones legales que autorizan tal forma de imposición de responsabilidad penal”*<sup>134</sup>. De las opciones de defensa que pueden tener las personas jurídicas ante una imputación es especialmente relevante la existencia y la implementación de un código de conducta por parte de la empresa de manera anterior a la comisión del delito. La empresa necesita dotarse de un programa de cumplimiento corporativo que resulte efectivo para que pueda ser considerado como atenuante de la responsabilidad penal de la

---

<sup>131</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 367-368.

<sup>132</sup>A semejanza de otras expresiones del soft law; PASTORE, B., "Soft law, gradi di normatività, teoría delle fonti", *Lavoro e Diritto*, nº 1, 2003, p. 5.

<sup>133</sup>ARTAZA VARELA, O., "Programas de cumplimiento. Breve descripción de las reglas técnicas de gestión del riesgo empresarial y su utilidad jurídico-penal", en AA.VV., *Responsabilidad de la empresa y compliance. Programas de prevención, detección y reacción penal*, dirs. S. Mir, M. Corcoy y V. Gómez, Madrid, 2014, p. 233.

<sup>134</sup>ARTAZA VARELA, O., "Programas de cumplimiento...", ob. cit., pp. 231-232.

persona jurídica<sup>135</sup>. Los programas de *compliance* son un fenómeno relativamente nuevo, que hace referencia a unos protocolos de actuación que las empresas adoptan con el fin de controlar sus propias acciones y tratar de garantizar el cumplimiento de su legalidad aplicable<sup>136</sup>.

En el ámbito penal, el origen de los planes corporativos de prevención de riesgos (*Criminal Risk Management*) tuvo lugar en las décadas de los 60 y 70, y muy particularmente a propósito del caso *Watergate*, con la *Foreign Corrupts Practices Act*. Ya en los años 80, los programas de cumplimiento penal experimentaron un extraordinario auge con motivo de los Informes del *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), elaborados por la *Treadway Commission (National Commission on Fraudulent Financial Reporting)*. No obstante, los programas de prevención de comisión de delitos en el ámbito empresarial conocen su actual dimensión desde 2002, como consecuencia de la entrada en vigor de la citada SOX, motivada por una serie de escándalos financieros y el final de la denominada burbuja tecnológica<sup>137</sup>.

Los programas de cumplimiento constituyen una herramienta del soft law a los que las empresas se acogen como barrera de defensa ante una potencial responsabilidad de la empresa por los actos ilícitos cometidos así como para demostrar su responsabilidad para con la sociedad. Se trata de un programa en el que se deberán "*identificar los riesgos de comisión de actos ilícitos y establecer las estrategias de prevención y control de los mismos*"<sup>138139</sup>.

---

<sup>135</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 375.

<sup>136</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 367.

<sup>137</sup>No en vano, algunas importantes sociedades, como *Enron* o *Arthur Andersen*, llegaron a desaparecer como consecuencia de su implicación en escándalos financieros y de corrupción privada.

<sup>138</sup>MORÓN LERMA, E., "El compliance officer: régimen y responsabilidad", en AA.VV., *Cumplimiento normativo. Compliance*, Cuadernos de Derecho para Ingenieros, nº 14, dirs. M.A. Agúndez, J. Martínez-Simancas, Madrid, 2012, p. 68.

<sup>139</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 375.

Inicialmente, la aparición de estos programas en nuestro país ha estado vinculada con la legislación del mercado de valores. Su implantación responde, fundamentalmente, a los requerimientos de la antigua Ley 24/1988, de 28 de julio, de Mercado de Valores, que obliga a las empresas de servicios de inversión e instituciones a establecer procedimientos de control interno del cumplimiento normativo. También tiene origen en la Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva, que estableció igualmente la necesidad de las sociedades gestoras de estas instituciones de contar con mecanismos de control que garanticen el cumplimiento de las obligaciones que la normativa aplicable les impone<sup>140</sup>, al objeto de asegurar los riesgos que las afectan y garantizar el correcto funcionamiento de las funciones de gestión de los riesgos<sup>141</sup>.

En España, la responsabilidad penal de las personas jurídicas fue introducida en el ordenamiento jurídico español mediante la reforma del Código Penal operada por Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, que entró en vigor el 23 de diciembre de 2010 (LO 5/2010)<sup>142</sup>.

El 1 de julio de 2015 entró en vigor la Ley Orgánica 1/2015 que modifica la Ley Orgánica 10/1995 (LO 1/2015), la cual profundiza en todas aquellas cuestiones que integran esta responsabilidad penal<sup>143</sup>y, en concreto, los elementos que deben concurrir para que la empresa pueda quedar exonerada de responsabilidad, ya que establece, que la adopción y la aplicación efectiva de un programa de cumplimiento normativo puede actuar y servir como un

---

<sup>140</sup>ALONSO ALONSO, E., "Los informes de cumplimiento normativo, Compliance", en AA.VV., *Cumplimiento normativo. Compliance*, Cuadernos de Derecho para Ingenieros, nº 14, dirs. M.A. Agúndez, J. Martínez-Simancas, Madrid, 2012, p. 24.

<sup>141</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 368-369.

<sup>142</sup>La introducción de esta figura en España suscitó abundantes críticas y dudas que la la Circular 1/2011 de la Fiscalía General del Estado intentó resolver sin mucho éxito, por todo ello su aplicación práctica resultó muy escasa.

<sup>143</sup>Esta modificación del Código Penal de 2015 acomete una aproximación estructural del Decreto Legislativo italiano 231/2001, e incluso sobrepasa los parámetros de éste en muchos casos, orientándose a la visión tradicional de los programas de cumplimiento corporativo en Estados Unidos.



factor eximente o atenuante cuando una empresa esté sujeta a la responsabilidad penal por los delitos cometidos por sus directivos, administradores o empleados.

Y es que la reforma del Código Penal de 2015 establece los elementos objetivos que cada programa de cumplimiento debe incorporar para servir como medio de defensa corporativa ante ciertos delitos cometidos por sus directivos o empleados. Como condición indispensable se exige que con anterioridad a la comisión del delito la persona jurídica haya adoptado y ejecutado eficazmente un modelo de cumplimiento que resulte adecuado para prevenir delitos de la naturaleza del que fue cometido o para reducir de forma significativa el riesgo de su comisión<sup>144</sup>.

En particular, el Código distingue según quien cometa el delito de la siguiente manera:

- (I) los delitos cometidos en beneficio de la empresa por sus representantes legales o por los que tienen autoridad para tomar decisiones autorizadas (normalmente la alta dirección); y
- (II) los delitos cometidos en beneficio de la empresa por las personas bajo la dirección de otros ("individuos subordinados"), si la comisión del delito fuese posible, debido a la falta de vigilancia y control por la dirección de la compañía.

En el primer caso, el nuevo Código permite eximir a las empresas de la responsabilidad penal de conformidad con los siguientes requisitos:

- Ha de tener un modelo de control vigente con anterioridad a la comisión del delito y adecuado para prevenir los delitos señalados.

---

<sup>144</sup>La nueva reforma manifiesta de manera clara y precisa, lo que se ha incorporado en la legislación española de muchas otras jurisdicciones de todo el mundo, y también se contiene en los tratados internacionales a los que España se ha adherido. En particular, existe un paralelismo significativo con lo dispuesto en el Decreto Legislativo italiano 231/2001 en el hecho de que el modelo que contempla podría servir como defensa afirmativa en caso de comisión de delitos de muy diversa índole, no centrándose exclusivamente en el soborno y/o fraude corporativo.

- La supervisión del modelo tiene que estar a cargo de un órgano de supervisión con poderes independientes, con iniciativa y control. Así, el Código reconoce que en las pequeñas y medianas empresas el Consejo de Administración podrá realizar esta función directamente.
- Se tienen que poder concretar los autores individuales del delito, aunque intencional y fraudulentamente se pueda eludir el modelo de prevención.
- Tiene que probarse que las autoridades de la compañía no han descuidado sus deberes de supervisión y control.

En caso de que el delito fuera cometido por una persona subordinada, la empresa tendrá que demostrar que había aplicado efectivamente un modelo de organización y gestión adecuado para prevenir los delitos del mismo tipo, que los cometidos con anterioridad a la comisión de los mismos.

Para que el modelo se considere adecuado debe incorporar los siguientes elementos:

- La evaluación de riesgos, para identificar las actividades dentro de la empresa que pueden representar un peligro.
- Las políticas, procedimientos y controles para prevenir, mitigar y/o sancionar cualquier riesgo penal detectable.
- Sistema de gestión financiera para prevenir la comisión de los delitos indicados.
- Obligación de informar sobre los riesgos potenciales y/o actividades irregulares. Es decir, la necesidad de implementar canales de denuncia de irregularidades.
- Régimen disciplinario para sancionar cualquier violación del modelo de gestión.

- Verificación periódica y cambios en el modelo si se descubren vulneraciones importantes, o si hay cambios significativos en la organización, la estructura de control, o las actividades de la corporación<sup>145</sup>.

Huelga decir que la formación y preparación es clave para la efectividad del modelo, aunque el Código no lo ha incluido explícitamente como uno de los elementos principales.

Las multinacionales que operan en España con programas de cumplimiento ya establecidos, deberán acometer o garantizar una evaluación local de los riesgos de sus operaciones, de manera que adapten sus programas globales corporativos a las necesidades establecidas por el legislador en España.

En las empresas multinacionales con programas de cumplimiento corporativo bien establecidos, la mera traducción al idioma local del programa, no será suficiente para cumplir con los requisitos establecidos por el nuevo Código Penal - aunque supondrá un claro beneficio tenerlo, sobre todo, sí es el reflejo de la existencia de una verdadera cultura de cumplimiento dentro de la organización.

Estos programas se podrían equiparar a los “sistemas de calidad” ya que incluyen aspectos relacionados con distintos ámbitos de la actividad empresarial tal y como son la estructura organizacional, la distribución de responsabilidades, procedimientos y recursos utilizados por la empresa para asegurar la calidad de la dirección de ésta<sup>146</sup>.

---

<sup>145</sup>MUÑOZ, P., “Reforma Código Penal de 2015: planes de cumplimiento corporativo”. Extraído de: <http://www.legaltoday.com/practica-juridica/penal/economico/reforma-codigo-penal-de-2015-planes-de-cumplimiento-corporativo>.

<sup>146</sup>GRUNER, R.S./ BROWN, L.M., “Organizational Justice: Recognizing and Rewarding the Good Citizen Corporation”, *The Journal of Corporation Law*, vol. 21, 1996, p. 737. Para más definiciones de estos instrumentos, WALSH, C.J. /PYRICH, A., “Corporate Compliance Programs as a Defense to Criminal Liability: Can a Corporation Save its Soul?”, *Rutgers Law Review*, vol. 47, 1994-1995, pp. 645 y ss; WELLNER, P.A., “Effective Compliance Programs and Corporate Criminal Prosecutions”, *Cardozo Law Review*, vol. 27, 2005, pp. 497 y ss.

Por ello, tal y como hemos dicho, la función principal de un programa de cumplimiento es sistematizar los procedimientos que se consideren necesarios para asegurar que la actividad de la empresa no vulnera ninguna normativa y es acorde a sus propios estándares y, por tanto, disminuir la probabilidad o frecuencia de las situaciones en las que la empresa podría ser penalmente punible<sup>147</sup>.

El Programa de Cumplimiento pretende recoger unos principios que produzcan efectos prácticos, toda vez que se prevén consecuencias jurídicas en caso de inobservancia de tales procedimientos. Para conseguir dicho resultado la empresa debe generar una suerte de incentivos para el cumplimiento de los programas establecidos. Asimismo, también deben crearse desincentivos o sanciones mediante medidas disciplinarias y, eventualmente, con el ejercicio de acciones penales y civiles<sup>148</sup>. En este sentido, es también fundamental una monitorización adecuada del funcionamiento y cumplimiento de los programas, pues para su total efectividad debe generarse la capacidad de detectar oportunamente conductas que en ese momento resulten irrelevantes pero que puedan llegar a desencadenar en un delito<sup>149</sup>.

Por último, debe volver a resaltarse que la implantación de estos programas de cumplimiento no responde exclusivamente a la idea de mitigar los riesgos de responsabilidades penales, sino que obedece también a la idea anteriormente expuesta de buen gobierno corporativo como una respuesta a la sociedad que rodea a la empresa<sup>150</sup>.

---

<sup>147</sup>GRUNER, R.S., *Corporate Criminal Liability and Prevention*, Law Journal Press, New York, 2010, pp. 14-4 y ss.

<sup>148</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 368.

<sup>149</sup>ARTAZA VARELA, O., "Programas de cumplimiento...", ob. cit., pp. 237-238.

<sup>150</sup>Al respecto, FERNÁNDEZ RODRÍGUEZ, J.J., *De la condicionalidad social y los Acuerdos marco internaciones, sobre la evolución de la responsabilidad social empresarial*, edit. Thomson Reuters Aranzadi, Pamplona, 2012.

## **2. Características y contenido esencial**

El contenido del programa de cumplimiento normativo o de prevención de riesgos penales en la empresa no está regulado y por tanto, no responde a un único modelo, a excepción de determinados ámbitos sectoriales<sup>151</sup>. Por tanto, se puede afirmar que cada empresa puede adoptar el programa de cumplimiento que considere que mejor se adapta al logro de sus objetivos ya que no existe un diseño de programa de cumplimiento de carácter general o universal aplicable a todas las entidades.

Dicho lo anterior, se ha intentado extraer algunos elementos comunes y esenciales de un programa de cumplimiento eficaz a la luz de determinados modelos de Derecho comparado<sup>152</sup> y a la vista de algunas prácticas empresariales se vislumbran algunos elementos esenciales que configuran el plan de cumplimiento normativo<sup>153</sup>.

### **2.1 El carácter abierto y dinámico de los programas de cumplimiento**

Un programa de cumplimiento no tiene un contenido determinado. Este carácter abierto es una ventaja ya que permite una gran flexibilidad para adaptarse al transcurso del tiempo y de la evolución de la empresa así como a los distintos sectores de la actividad empresarial. Sin embargo, esta falta de precisión en cuanto a cuál debe ser el contenido de los programas de cumplimiento también puede resultar inconveniente desde el punto de vista de no tener nunca un nivel de certeza absoluta sobre lo que debe o no

---

<sup>151</sup>Como son las sociedades cotizadas cuyo programa de cumplimiento sí está vinculado a determinadas obligaciones impuestas por la ley del Mercado de Valores y el Código Unificado de Buen Gobierno.

<sup>152</sup>Como es el United States Sentencing Commission Guidelines Manual (2002), el decreto legislativo italiano 231, de 8 de junio de 2001 que regula la responsabilidad administrativa de las personas jurídicas derivadas de la comisión en su seno de ilícitas penales, o la ley chilena 20.393, de 25 de noviembre de 2009.

<sup>153</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 376.

incluirse, lo cual podría llegar a implicar un cierto nivel de inseguridad jurídica.<sup>154</sup>

A continuación se hará un análisis breve, ya que no es el centro de este estudio, de una estructura típica de un programa de cumplimiento atendiendo a los distintos estándares internacionales.

Generalmente la estructura de un programa de cumplimiento está compuesta por una introducción, una parte general y una parte especial. La parte general sería tendente a crear una cultura organizacional en la cual se respetase el cumplimiento de la ley por medio de unos principios rectores claros, y la parte especial suele estar dirigida al control del cumplimiento de dichos principios, es decir, al establecimiento de procedimientos y mecanismos que permitan asegurar (en la medida de lo posible) la efectividad del programa.<sup>155</sup>

Un contenido similar se puede observar en la metodología utilizada por el *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), organismo especializado en el control interno de la empresa el cual presenta un contenido muy similar en su metodología ya que diferencia una parte relativa a la organización empresarial y otra puramente procedimental al gestionar los posibles riesgos de infracción del ordenamiento jurídico<sup>156</sup>. También resultan interesantes los estándares que propone esta organización bajo la denominación de *Enterprise risk management*<sup>157</sup>.

---

<sup>154</sup>ARTAZA VARELA, O., "Programas de cumplimiento...", ob. cit., pp. 239-240.

<sup>155</sup>ARTAZA VARELA, O., "Programas de cumplimiento...", ob. cit., p. 242.

<sup>156</sup>Para una descripción acabada de tales instrumentos, MOELLER, R., *COSO Enterprise Risk. Establishing Effective Governance, Risk, and Compliance Processes*, Wiley Corporate F&A, 2011 (2ªed.), Kindle Edition, pp. 420 y ss.; LOUGHMAN, B.P. /SIBERY, R.A., *Bribery and Corruption. Navigating the Global Risks*, Wiley Corporate F&A, Kindle Edition, 2012, pp. 1323 y ss.

<sup>157</sup><https://www.coso.org/Pages/ermupdate.aspx>

En este sentido, de acuerdo con la *U. S. Federal Sentencing Guidelines for Organizations* (FSGO)<sup>158</sup>, para que una empresa obtenga una reducción en la multa impuesta debe haber implementado un programa de cumplimiento que sea efectivo para detectar las infracciones correspondientes. Para que dicho programa de cumplimiento sea eficaz en cuanto a atenuante de multas y demás sanciones su diseño debe cumplir con los dos aspectos destacados anteriormente: el programa debe generar una cultura organizacional respetuosa con la legislación vigente y contar con los mecanismos de control adecuados.

### **2.1.1 El fomento de una cultura organizacional tendiente al cumplimiento de la ley**

Junto con los objetivos tradicionales de toda compañía, es decir la obtención de beneficios y el logro de los objetivos empresariales fijados, existe otro reto fundamental que es el cumplimiento del ordenamiento jurídico en su más amplia concepción. Dicho objetivo queda reflejado como meta fundamental en cualquier plan de cumplimiento.

Para ello deben establecerse una serie de medidas dirigidas a crear una cultura de empresa en la que se valore el cumplimiento de la ley, y que dichos valores morales que la empresa ha decidido abrazar se recojan en el llamado código ético o código de conducta.<sup>159</sup> En este sentido, en España,

---

<sup>158</sup>Las FSGO contienen una serie de circunstancias que agravan y que atenúan, en su caso, la responsabilidad de la empresa para cuando se den los requisitos que contiene el mismo instrumento. Escapa al ámbito de este artículo un estudio detallado de estas directrices, así como el análisis de aquellos factores que son tenidos en cuenta para agravar el monto de la multa a la empresa condenada. Más bien interesará aquí únicamente una de las circunstancias que atenúan la responsabilidad penal de las empresas, a saber, que la misma disponga de un "programa ético y de cumplimiento efectivo". En relación con los efectos prácticos de contar con un Programa de Cumplimiento, NIETO MARTIN, A., *La responsabilidad penal de las personas jurídicas: un modelo legislativo*, Valencia, 2008, p. 191; HUFF, K.B., "The Role of Corporate Compliance Programs in Determining Corporate Criminal Liability: A Suggested Approach", *Columbia Law Review*, vol. 96, 1996, pp. 1267 y ss.

<sup>159</sup>Para NIETO MARTIN, A., *La responsabilidad penal...*, ob. cit., pp. 240 y SS., un Código de conducta se podría identificar "con un conjunto de disposiciones que tienen como finalidad reforzar los mandatos que se contienen en un texto legal. Éstos "constituyen el tronco del sistema de organización interno, sobre él descansan el resto de contenidos".

se ha señalado que el objetivo fundamental del código ético debe ser “*promover una cultura dentro de la organización que, más allá de asegurar el cumplimiento de la ley, anime a que la actividad en general de la empresa se corresponda con determinados patrones éticos*”<sup>160</sup>.

Actualmente, en el mundo del *compliance* es un hecho que la mejor forma de prevenir conductas delictivas es fomentar una cultura ética y unos valores comunes entre todos los integrantes de la empresa<sup>161</sup>. Los valores de la empresa son los pilares más importantes de cualquier organización. Con ellos una compañía se define a sí misma, porque los valores de una

---

<sup>160</sup>NIETO MARTIN, A., *La responsabilidad penal...*, ob. cit., p. 241. En general se puede decir que sus principales funciones son: a) refuerzo del mandato normativo y la asignación de relevancia al cumplimiento de la ley como uno de los objetivos prioritarios de la organización; b) cumplir con una función de especificación o concreción de las normas jurídicas, "mostrando a sus destinatarios la forma en que debe actuar el empleado ante una oportunidad delictiva o una situación de riesgo para determinados bienes jurídicos". Esto implica que deben estar redactados en términos suficientemente flexibles como para ir adaptándose a nuevas situaciones que se vayan presentando en el ejercicio propio de la actividad de la empresa. Se suele decir, además, que este tipo de instrumentos sirven para "reducir la complejidad" vinculada al comportamiento de acuerdo con la norma penal en determinados ámbitos de regulación relativamente complejos. Esta concreción del contenido de la norma viene dada por la definición de cómo cumplir con la exigencia legal; c) cumplirían con una función externa (destinada a sujetos fuera de la estructura organizacional) vinculada a la regulación de la relación de la empresa con otros organismos y al respeto de su normativa interna en esta interacción. Ejemplos claros en donde esta finalidad es del todo relevante serían los de la lucha contra la corrupción, en donde se pretende evitar que las empresas "cierren los ojos" ante determinadas ilegalidades que se puedan cometer en la contratación con empresas ubicadas en el extranjero mediante la delegación de la tarea de contratar con éstas. O también el sector productivo en relación con la contratación con proveedores con el objeto de impedir, por ejemplo, que el suministro de determinados bienes se haya obtenido mediante trabajo infantil, etc.; d) en éste se fijarían las normas de comportamiento de la empresa en forma general, por ende, contendría no sólo el reforzamiento del mandato, ya sea penal o proveniente de otra área del ordenamiento jurídico, sino que puede ir más lejos en el sentido de establecer, por ejemplo, los procedimientos tendientes a regular la conducta esperada luego de la comisión de un ilícito o los procedimientos necesarios para poder advertir de la comisión de una conducta delictiva, etc. Ver al respecto, también, GORDON, S. D., "Implementation of Effective Compliance and Ethics Programs and the Federal Sentencing Guidelines", AA.VV., *Corporate Compliance Answer Book*, edit. Practising Law Institute, 2016, pp. 43 y ss. Ver también, en España, BACIGALUPO ZAPATER, E., *Compliance y Derecho penal*, Aranzadi, Pamplona, 2011, pp. 45-60. Otros ámbitos en los que esta finalidad de los Códigos de conducta es de gran relevancia serían el de prevención de riesgos laborales (art. 2 del RD 39/1997), el de Sanidad Alimentaria, por medio del Sistema de Análisis de Peligros y Puntos Críticos (RD 2207/1995), o, en materia medioambiental, por medio de los sistemas de gestión exigidos por el Reglamento CEE 1836/93.

<sup>161</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 380. Teniendo en cuenta que el programa de cumplimiento debe ser conocido y que se impone a todos los miembros de la entidad, resulta casi obligado cierto grado de participación de los propios destinatarios de los programas de cumplimiento. La participación en la elaboración de los programas facilita el conocimiento y contribuye a que las decisiones que se deben adoptar tengan una mayor repercusión preventiva.



organización son los valores de sus miembros, y especialmente los de sus dirigentes.

Por tanto, el código ético recoge los principios y valores de la empresa, así como los objetivos a alcanzar y la forma en la que deben ser alcanzados. Tal y como dice Adela Cortina "*Los marcos éticos sin herramientas para integrarlos en la vida cotidiana están vacíos, y las herramientas sin marcos están ciegas*"<sup>162</sup>.

De hecho, éste fue el propósito de las reformas introducidas en Estados Unidos (por ejemplo, la SOX de 2002) en la primera década de este siglo, principalmente con el objeto de reforzar la adopción de códigos de conducta que incluyan un estándar en el comportamiento ético mínimo esperado por la organización<sup>163</sup>. Y es que la adopción de un código de conducta en el que quede recogida la cultura empresarial de la compañía, se ha transformado en un pilar básico de un programa de cumplimiento efectivo.

Por ello es fundamental que esta "conciencia" de la organización sea especialmente aceptada y promocionada desde la alta dirección (lo que se conoce como "*tone at the top*"), para que a su vez genere en toda la empresa una cultura que considere fundamental el cumplimiento del ordenamiento jurídico y los estándares éticos de la empresa<sup>164</sup>.

---

<sup>162</sup>LOZANO AGUILAR, J. F., *Códigos éticos para el mundo empresarial*, Madrid, 2004.

<sup>163</sup>En relación con la génesis, objetivos y críticas a este instrumento, HEFENDEHL, R., "Enron, WorldCom, and the Consequences: Business Criminal Law Between Doctrinal Requirements and the Hopes of Crime Policy", *Buffalo Criminal Law Review*, vol. 8, 2005, pp. 51-54; SALVADOR CODERCH, P./GOMEZ LIGÜERRE, C.I., "Respondeat Superior II. De la responsabilidad por hecho de otro a la responsabilidad de la organización", *InDret*, nº 3, 2002, pp. 1 y 22, extraído de [http://www.indret.com/pdf/088\\_es.pdf](http://www.indret.com/pdf/088_es.pdf); FOFFANI, L., "Escándalos económicos y reformas penales: prevención y represión de las infracciones societarias en la era de la globalización", *Revista Penal*, nº 23, 2009, pp. 35 y ss.; GORDON, S.D., "Implementation...", ob. cit., pp. 35 y ss.; SCHÜNEMANN, B., "The Sarbanes-Oxley Act of 2002: A German Perspective", *Buffalo Criminal Law Review*, vol. 8, 2004, pp. 43 y ss., con un énfasis diverso en la descripción de este instrumento destacando la relevancia que se le asignaría a la responsabilidad individual.

<sup>164</sup>ARTAZA VARELA, O., "Programas de cumplimiento...", ob. cit., p. 246.

En este sentido, se ha definido la cultura organizacional como “*el conjunto de reglas y principios que guían el comportamiento individual y grupal que han sido determinados por la dirección de la empresa y que son expresados como valores compartidos por la organización o principios rectores, reforzados por una serie de procedimientos desarrollados en la misma*”<sup>165</sup>.

Tal y como se ha mencionado con anterioridad, desde un prisma de prevención de riesgos penales de la empresa destacan por su importancia las *U. S. Federal Sentencing Guidelines for Organizations* (FSGO). El informe del *Advisory Group* sostiene que uno de los principales objetivos de las FSGO es el de crear incentivos para el refuerzo del cumplimiento de la ley por parte de la empresa<sup>166</sup>, dichos incentivos consistirían en el establecimiento de determinadas consecuencias ligadas a un comportamiento meritorio o reprochable dentro de la actividad empresarial. Según las conclusiones del grupo, para que dichos mecanismos funcionen, los valores del código ético deben estar integrados dentro de la cultura organizacional<sup>167</sup>.

Debe insistirse en que la existencia de un código de conducta es irrelevante si la cultura ética o valores del mismo no están realmente interiorizados por todos los trabajadores de la compañía, y de manera muy especial por la alta dirección<sup>168</sup>. Así como tampoco resultaría suficiente la mera descripción de ciertos valores y conductas si el cumplimiento de las mismas no intenta

---

<sup>165</sup> *Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines*, del 7/10/03 p. 52, extraído de [http://www.usc.gov/sites/default/files/pdf/training/organizational-guidelines/advgprpt/AG\\_FINAL.pdf](http://www.usc.gov/sites/default/files/pdf/training/organizational-guidelines/advgprpt/AG_FINAL.pdf). En España se refiere a este aspecto de la actividad empresarial, entre otros, BACIGALUPO ZAPATER, E., *Compliance...*, ob. cit., pp. 17-19.

<sup>166</sup> En este sentido, el *Report of the Ad Hoc Advisory Group...*, ob. cit., p. 51; GÓMEZ JARA, C., “Responsabilidad penal de las personas jurídicas y contratación pública. A propósito de la nueva directiva Europea sobre contratación pública”, *La Ley* nº 8175, 2014, p. 125; GORDON, S.D., “Implementation...”, ob. cit., p. 41; SHARP PAINE, L., “Managing for Organizational Integrity”, *Harvard Business Review*, marzo-abril 1994, pp. 106 y ss.

<sup>167</sup> ARTAZA VARELA, O., “Programas de cumplimiento...”, ob. cit., p. 247.

<sup>168</sup> Al respecto, ver entrevista a Michael Toffel en 2007 para *Harvard Business School*, “Industry Self-Regulation: What's Working (and What's Not)?”, en donde se refuerza la idea de que la sola adopción de un código de conducta no es suficiente sin otros mecanismos complementarios. Disponible en Web: <http://hbswk.hbs.edu>.

asegurarse por medio de la implantación de una serie de procedimientos o medidas<sup>169</sup>.

### 2.1.2 El control y la administración del riesgo

Como apuntábamos en el último epígrafe, además del establecimiento de los valores éticos de la compañía y el fomento de esta cultura ética entre los trabajadores, el otro pilar fundamental de un programa de cumplimiento es la adopción de las medidas y procedimientos adecuados para asegurar el respeto a la legalidad dentro de la actividad empresarial.

Es imposible establecer un único tipo de procedimientos o medidas que funcionen para todo tipo de empresas, ya que la eficacia de los mismos dependerá de su adaptación al sector, tipo, tamaño de empresa que se trate y ésta es la tendencia actual que se ve corroborada por las modificaciones que se han desarrollado en las FSGO<sup>170</sup>. En este sentido, las FSGO no imponen un sistema de control determinado sino que señalan una serie de aspectos que la propia organización debe tener en cuenta para valorar si el sistema de control es el adecuado o no. En cierta manera las FSGO establecen unos criterios con los que debería cumplir cualquier sistema de control y que si llega el caso el juez deberá revisar<sup>171</sup>.

Por lo mismo, dentro de las medidas a establecer en cuanto al control interno se distinguen dos procesos fundamentales, el de *Risk Assessment* (evaluación de riesgos) como se denomina en la práctica angloamericana, y el *Risk Mitigation* (reducción o mitigación de riesgos). Tal y como señala

---

<sup>169</sup>Ver al respecto GORDON, S.D., "Implementation...", ob. cit., p. 50, con referencias directas al caso "Enron" y la falta de sustancia que presentaría el Código de conducta de la misma, la que sólo sería un "mero papel". Además, HECHLER BAER, M., "Governing Corporate Compliance", *Boston College Law Review*, vol. 50, 2009, pp. 4 y ss., especialmente en relación con la evolución en el ámbito angloamericano para evitar el problema del "*cosmetic compliance*" (o programas de cumplimiento de "mero papel" como se los suele denominar).

<sup>170</sup>En relación con la relevancia del "tamaño" y complejidad de la empresa, GORDON, S.D., "Implementation...", ob. cit., pp. 34-35.

<sup>171</sup>ARTAZA VARELA, O., "Programas de cumplimiento...", ob. cit., p. 249.

RAUSAND, el propio ejercicio de definición de un riesgo es altamente complejo<sup>172</sup>. En 1996 el reconocido investigador STAN KAPLA recibió el Premio al Reconocimiento de la Society of Risk Analysis<sup>173</sup> y en su discurso de agradecimiento señaló que la definición de análisis de riesgos era un continuo problema, y recordó que cuando la Society Risk Analysis se inauguró se creó una comisión para fijar la definición de “riesgo” y que cuatro años después dicha comisión desistió en su tarea llegando a la conclusión que lo mejor era no definir la palabra riesgo y que cada autor explicase a qué se estaba refiriendo al utilizar dicho concepto<sup>174</sup>.

En el ámbito del Risk Assesment se incluye la definición de los riesgos que deben ser controlados, es decir se deben identificar todos los potenciales riesgos a los que se expone la actividad de la empresa<sup>175</sup>. Una vez identificados los posibles riesgos, la compañía debería analizar cada área de actividad e identificar a los trabajadores de las mismas. A continuación debe iniciarse una segunda fase de evaluación cualitativa y cuantitativa de los riesgos que consiste en definir la probabilidad de que se presente el riesgo y el impacto que tendría.

El *Advisory Group* ha señalado a propósito del análisis de las FSGO que para evaluar la efectividad de un programa de cumplimiento deben analizarse los estándares de conducta que contiene y que el sistema de

---

<sup>172</sup>RAUSAND, M., *Risk Assessment: Theory, Methods, and Applications (Statistics in Practice)*, ed. Wiley, New Jersey, 2011. M. RAUSAND afirma que si preguntas a diez personas distintas su definición de riesgo te darán diez definiciones diferentes entre si. Lo mismo sucederá si dicho experimento lo realizas entre la comunidad científica o entre los propios expertos en riesgos.

<sup>173</sup><http://sra.org/>

<sup>174</sup>KAPLAN, S., “The words of Risk Analysis”, *Risk Analysis an International Journal*, vol. 17, Issue 4, ed. Wiley Online Library, 1997, pp 401- 523.

<sup>175</sup>HEALTH and SAFETY EXECUTIVE, “Risk assessment, A brief guide to controlling risks in the workplace”.Extraído de [www.hse.gov.uk/pubns/indg163.htm](http://www.hse.gov.uk/pubns/indg163.htm)

control interno sea capaz de reducir las infracciones de la ley más frecuentes o típicas del sector en que esté englobada la compañía<sup>176</sup>.

Por tanto, un programa de cumplimiento que no se centra de manera específica en gestionar los riesgos potenciales más frecuentes y de mayor magnitud vinculados a los peligros previamente identificados de su actividad, no podría considerarse efectivo. Es importante también destacar que es fundamental para la efectividad del programa que la evaluación de riesgos esté en continua actualización.

COSO recomienda que una vez superada la evaluación de los riesgos, se inicie la planificación de los procedimientos y mecanismos para controlar los riesgos identificados. Las FSGO contienen principios y características de los mecanismos de control que son útiles a la hora de diseñar esta fase del programa de cumplimiento.

## **2.2 Involucración de la alta dirección de la empresa en labores de supervisión y control, y delegación adecuada de funciones de vigilancia<sup>177</sup>**

Uno de los puntos fundamentales para que un programa de cumplimiento resulte efectivo e implique una atenuante en caso de que se cometiese un acto ilícito en el seno de la empresa, es el grado de relación que el mismo debe guardar con los administradores y la alta dirección de la compañía. Es fundamental que dicho personal esté involucrado de una manera activa en el diseño del programa así como en la supervisión del sistema de control que se establezca<sup>178</sup>.

---

<sup>176</sup>*Report of the Ad Hoc Advisory Group...*, cit., pp. 56 y 87, según los cuales las evaluaciones de riesgo deben realizarse en todas las etapas del desarrollo, prueba e implementación de un programa de cumplimiento para asegurar que el esfuerzo de cumplimiento sea efectivo y esté bien coordinado.

<sup>177</sup>ARTAZA VARELA, O., "Programas de cumplimiento...", ob. cit., p. 253.

<sup>178</sup>*Report of the Ad Hoc Advisory Group...*, ob. cit., p. 59-60. Así, por ejemplo, una de las modificaciones propuestas por el *Advisory Group* es la inclusión de una referencia directa al

No sólo debe la alta dirección estar involucrada sino que además tienen cierta cuota de responsabilidad en el diseño e implementación del programa, ya que es su responsabilidad que la compañía cuente con el mismo<sup>179</sup>. Y es que la implantación de un programa de cumplimiento es una decisión que le corresponde al titular de la entidad. En su regulación no interviene, normalmente, nadie más que la propia cúpula de la organización. Desde un punto de vista de derecho laboral las compañías crean un ámbito de regulación autónomo, partiendo de su propio poder de autoorganización<sup>180</sup>.

Tal y como hemos mencionado antes, un sistema de cumplimiento no está sujeto a obligaciones específicas, sino que su contenido es de carácter abierto al igual que lo es su proceso de elaboración, asumiendo la compañía el total protagonismo en cuanto al diseño de principios preventivos y definición de procedimientos de control para verificar el respeto de la legalidad y de la normativa que le es de aplicación, así como de los principios y políticas internas de la empresa.<sup>181</sup>

No obstante lo anterior, para que la acción preventiva pueda tener efectos reales sobre la prevención de un delito en la empresa, en la práctica es

---

involucramiento de los altos ejecutivos en esta labor. Lo que se desprende de su propuesta de redacción de la Sección 8B2.1 (b) (2) de las FSGO.

<sup>179</sup>En forma expresa, el art. 4 de la ley 20.393 chilena: "Modelo de prevención de los delitos. Para los efectos previstos en el inciso tercero del artículo anterior, las personas jurídicas podrán adoptar el modelo de prevención a que allí se hace referencia, el que deberá contener a lo menos los siguientes elementos: 1) Designación de un encargado de prevención. a) La máxima autoridad administrativa de la persona jurídica, sea ésta su directorio, un socio administrador, un gerente, un ejecutivo principal, un administrador, un liquidador, sus representantes, sus dueños o socios, según corresponda a la forma de administración de la respectiva entidad, en adelante la 'Administración de la Persona Jurídica', deberá designar un encargado de prevención, quien durará en su cargo hasta tres años, el que podrá prorrogarse por períodos de igual duración".

<sup>180</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 379-380.

<sup>181</sup>LIÑAN LAFUENTE, A., "El control preventivo de la responsabilidad penal de las personas jurídicas", en AA.VV., *Cumplimiento normativo. Compliance*, Cuadernos de Derecho para Ingenieros, nº 14, dirs. M.A. Agúndez, J. Martínez-Simancas, Madrid, 2012, p. 48. Por otra parte, ante la posibilidad de que la entidad pueda ser considerada responsable penalmente (art. 31 bis 1CP) por delitos cometidos por personas sin vinculación laboral con cierto régimen de independencia de la entidad, aunque sometidos a su autoridad (agentes financieros, agentes de seguros), resulta también hasta cierto punto entendible que en la configuración del sistema la entidad actúe bajo su exclusiva autoridad

necesaria la consulta y participación de los agentes implicados, y de manera especial de los representantes de los trabajadores<sup>182</sup>.

De manera similar a los procesos de redacción de los planes de prevención de riesgos laborales en la empresa<sup>183</sup>, es muy recomendable que en los procesos de redacción de los planes de cumplimiento también se escuchen y valoren las opiniones de los empleados de la empresa (al ser también ellos posibles autores de los delitos susceptibles de provocar la responsabilidad penal de la empresa, y no sólo la alta dirección) porque *“la asunción del mismo adquirirá un mayor convencimiento y será más sencilla que si durante el proceso de elaboración del plan no se ha producido la participación activa de las unidades del sistema general de gestión en la definición del papel preventivo que tendrá que desempeñar”*<sup>184</sup>. Lo anterior no sólo encuentra su razón en que un programa de cumplimiento diseñado estrictamente por la alta dirección y sin ninguna participación del resto de los empleados es muy difícil que sea acogido e implantado efectivamente en toda la empresa, sino porque el grado de participación de los empleados en su redacción puede ser tenido en cuenta por los órganos de enjuiciamiento como causa de exoneración de responsabilidad penal de las entidades, a la hora de valorar el cumplimiento eficiente del control que debe ejercer el administrador sobre las actividades sociales de los empleados o personas que se encuentren bajo su autorización<sup>185</sup>.

Tal y como señalan M. BALLBÉ y R. MARTÍNEZ respecto a la intervención y participación de los colectivos en un procedimiento no se trata tanto de una representación mecánica de diferentes intereses, sino para asegurar con esta

---

<sup>182</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 380.

<sup>183</sup>Aunque la medida no es enteramente trasladable a nuestro ámbito porque se exige expresamente en el art. 33 LPRL.

<sup>184</sup>Módulo IV. "Obligaciones empresariales en materia preventiva (I)", en AA.VV., *Prevención de riesgos laborales. Instrumentos de aplicación*, coord. C. Alfonso Mellado, C. Salcedo Beltrán, e I. Rosat Aced, Tirant lo Blanch, Valencia, 2010, pp. 274 y ss.

<sup>185</sup>Art. 31 bis 1 CP

participación una deliberación pública donde se busque una nueva solución fruto de esta deliberación colectiva<sup>186</sup>.

Además de por esta razón, la participación de los empleados en la redacción de un programa de cumplimiento también puede encontrarse en el principio legal de intervención de los representantes de los trabajadores en las decisiones de la empresa que comporten incidencia relevante en las condiciones de trabajo<sup>187</sup>. Admitido que el Plan de *compliance* trata de implementar un sistema de prevención y de control de riesgos penales en la empresa, que incide en los derechos o intereses de los trabajadores, existe, en consecuencia, la obligación de la empresa de consultar a las representaciones legales sobre dicha cuestión. El empresario viene, así, obligado a abrir un trámite formal de consulta con los representantes de los trabajadores, entendiéndose por tal, según lo dispuesto en el párrafo 2º del art. 64.1 del TRLET, “*el intercambio de opiniones y la apertura de un diálogo*”.<sup>188</sup>

Sin embargo, una vez fijado lo anterior debe también destacarse que la ausencia de tal deber de consulta no origina la ineficacia de la decisión empresarial adoptada irregularmente, toda vez que no lleva aparejada sanción jurídica alguna, salvo la responsabilidad administrativa. La falta de sanción jurídica específica convierte la previsión estatutaria en una “norma

---

<sup>186</sup>BALLBÉ, M./ MARTÍNEZ, R., “Law and Globalization: Between the United States and Europe”, ob. cit pp. 160.

<sup>187</sup>Es preciso observar que, de conformidad con lo dispuesto en el párrafo f) del art. 64.5 TRLET, el órgano representativo de los trabajadores (comité de empresa y, en su caso, los delegados de personal) tiene “*derecho a emitir informe, con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por éste “, sobre “implantación y revisión de sistemas de organización y control de trabajo*”.

<sup>188</sup>De acuerdo del art. 64.6 TRLET, no es una simple obligación de información sin incidencia en la decisión empresarial, sino que es un requisito de negociación informal que debe incidir en las decisiones de la empresa. Esta característica de obligación-condición de carácter negocial se hace patente al establecerse que la consulta deberá realizarse “*de tal manera que permita a los representantes de los trabajadores, sobre la base de la información recibida, reunirse con el empresario, obtener una respuesta justificada a su eventual informe y poder contrastar sus puntos de vista u opiniones con objeto, en su caso, de poder llegar a un acuerdo sobre las cuestiones indicadas*”. Siendo, además obligado que “*la consulta deberá permitir que el criterio del comité pueda ser conocido por el empresario a la hora de adoptar o de ejecutar las decisiones*”.



imperfecta”<sup>189</sup>, cuyo incumplimiento no entraña más que, en su caso, una sanción administrativa. En conclusión, dada la débil fuerza coercitiva del deber de consulta establecido en el TRLET, la participación de los representantes de los trabajadores adquiere el carácter de verdadero deber o carga para la entidad, más por su importancia como estándar de diligencia en la valoración por los órganos judiciales del control en la evitación de actos ilícitos en la empresa, que por lo que representa como reconocimiento de los derechos de representación de los trabajadores en las decisiones de la empresa<sup>190</sup>.

La alta dirección no sólo debe estar involucrada sino que además, tiene cierta cuota de responsabilidad en el diseño e implementación del programa, ya que es su responsabilidad que la compañía cuente con dicho programa así como definir aquellos integrantes de la alta dirección que quedarán encargados de supervisar el cumplimiento general de éste.

Debe tenerse en cuenta que la delegación de la responsabilidad de vigilancia del mismo queda limitada por la exigencia de una comunicación continua a la alta dirección, en cuanto al efectivo funcionamiento del modelo organizativo. El organismo de vigilancia requiere un alto grado de autonomía e independencia que puede ser satisfecho si se sitúa de manera elevada en la estructura jerárquica de la compañía de manera que tenga una comunicación directa e inmediata con el Consejo de Administración de la misma.

### **2.3 Comunicación y formación continua de los integrantes de la empresa**

Es fundamental aclarar que la obligación del conocimiento adecuado de los procedimientos existentes en la empresa respecto al cumplimiento de la Ley

---

<sup>189</sup>MONEREO PÉREZ, J.L., *Los derechos de información de los representantes de los trabajadores*, Civitas, Madrid, 1992, p. 260.

<sup>190</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 383.

no queda cumplida por una mera publicación de los mismos, sino que debe existir un conocimiento real y actualizado junto con una motivación apropiada por parte de los empleados para cumplir dichos procedimientos<sup>191</sup>.

Debe tenerse en cuenta que la forma en que la empresa cumpla con los requisitos de conocimiento efectivo y constante actualización será de su exclusiva responsabilidad<sup>192</sup>.

En cuanto a la comunicación y la formación de los empleados respecto al programa de cumplimiento, las FSGO disponen de ciertos principios que Osvaldo Artaza resume de la siguiente manera<sup>193</sup>:

*“A. La organización deberá adoptar medidas razonables para comunicar periódicamente, y de manera práctica, sus estándares y procedimientos, además de otros aspectos de su programa ético y de cumplimiento, a los individuos que están referidos en el subapartado (B), llevando a cabo programas efectivos de entrenamiento y distribuyendo de otras maneras la información que resulte apropiada para los roles y responsabilidades que corresponden a dichos individuos.*

*B. Los individuos referidos en el subapartado (A) son los miembros de la directiva, el personal de la alta dirección, el personal con autoridad significativa, los empleados de la organización y, en su caso, los representantes de la organización”.*

---

<sup>191</sup> *Report of the Ad Hoc Advisory Group...*, ob. cit., pp. 70 y 71. En términos muy diversos la ley 20.393 (Chile), que al parecer exige únicamente una comunicación formal a los integrantes de la empresa por medio de la incorporación de las diversas obligaciones que derivan del sistema de prevención de delitos en los respectivos reglamentos y contratos de trabajo (art. 4. 3 d).

<sup>192</sup> *Report of the Ad Hoc Advisory Group...*, ob. cit., p. 69, señala que la empresa debe tener la flexibilidad para determinar el tipo de programa de entrenamiento que quiera adoptar y cómo hará circular debidamente la información de acuerdo al tamaño de la organización y el tipo de conductas delictivas que podrían ser cometidas en el marco del desarrollo de su actividad.

<sup>193</sup> ARTAZA VARELA, O., "Programas de cumplimiento...", ob. cit., p. 256.

## 2.4 Adopción de mecanismos de monitorización y evaluación del programa

Constituye un elemento fundamental para la configuración de Programa de Cumplimiento eficaz la previsión de mecanismos de auditoría, supervisión y seguimiento de la actuación preventiva con el fin de evaluar el programa periódicamente y detectar debilidades.

Este papel preventivo de supervisión y control es desempeñado por órganos colegiados o unipersonales designados por la empresa (*compliance officer*) dependiendo de su naturaleza, estructura, y complejidad de las actividades que desempeñe. Para que el *compliance officer* realice eficazmente las funciones de control y supervisión es necesario que se le dote de los recursos humanos, técnicos, materiales y económicos necesarios<sup>194</sup>. Tal y como veremos, entre las funciones de dicho responsable de cumplimiento normativo se encuentra la implementación del programa de prevención de ilícitos, la recepción de comunicaciones y denuncias, así como de investigación de concretas actividades irregulares y de informe a los titulares del negocio de los resultados de la investigación. Asimismo el *compliance officer* deberá elevar periódicamente al Consejo de Administración o al comité ejecutivo informes sobre del grado de cumplimiento del plan y formular propuestas de mejora, especialmente si se detectan nuevos riesgos o que cree que las medidas adoptadas no están siendo eficaces.<sup>195</sup>.

También las FSGO establecen ciertos principios en cuanto a los procedimientos diseñados para evitar incumplimientos de la Ley mediante la incorporación de la exigencia de monitorización, auditorías y evaluación. Las FSGO señalan que la compañía debe establecer medidas razonables para

---

<sup>194</sup>Esto último es un requisito del propio Código Penal, cuando en su artículo 31 5.3º establece que "Los modelos de organización y gestión a que se refieren la condición 1.ª del apartado 2 y el apartado anterior deberán cumplir los siguientes requisitos: (...) Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos"

<sup>195</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 378.

asegurarse el cumplimiento efectivo del programa ético y de cumplimiento, incluyendo controles y auditorías para detectar la conducta delictiva y la evaluación periódica de la efectividad del mismo.

El *Advisory Group* destaca lo importante que resulta para el éxito del programa de cumplimiento que el mismo cuente con un sistema de evaluación continuo<sup>196</sup>.

La doctrina y jurisprudencia norteamericanas en su análisis de las FSGO ha destacado que la práctica de la auditoría interna debe centrarse en la detección y prevención de los potenciales riesgos identificados como los más típicos dentro del sector donde opera la compañía<sup>197</sup>. Asimismo, se ha destacado la relevancia de contar con una auditoría externa para prevenir dichos riesgos.

Otro requisito que las FSGO señalan respecto al sistema de evaluación y monitorización de un programa de cumplimiento es que contenga métodos eficaces y rápidos de comunicación la alta dirección y administración de la empresa acerca de sus resultados, de forma que estos queden suficientemente informados en tiempo para que puedan considerar efectivo el programa de cumplimiento con el que cuenta la compañía<sup>198</sup>.

---

<sup>196</sup> *Report of the Ad Hoc Advisory Group...*, ob. cit., p. 75. Este grupo da algunos ejemplos de directrices vinculadas a este aspecto en determinados sectores de gran relevancia, y que pueden servir para facilitar la comprensión de los fines que se pretenden con esta exigencia. Así, por ejemplo, aquellos estándares diseñados por el *International Standar Organization for an Environmental Management System* (EMS), cuyo propósito está dado, en parte, para asegurar el cumplimiento de la regulación medioambiental y que requiere que tal sistema incluya medidas de monitoreo, auditoría y de evaluación. Otro ejemplo útil es el dado en el marco de la *Health Care Association*, que ha propuesto algunos criterios para evaluar la calidad de los PC en organizaciones hospitalarias o clínicas (pp. 74 y ss.).

<sup>197</sup> En este sentido se manifiesta NIETO MARTIN, A., "Responsabilidad social, gobierno corporativo y autorregulación: sus influencias en el Derecho penal de la empresa", *Política Criminal*, nº 5, 2008, p. 10, para el cual la "metodología esencial" en la confección de un sistema de autoorganización es el conocido como *risk assessment*.

<sup>198</sup> *Report of the Ad Hoc Advisory Group...*, ob. cit., p. 77.

## 2.5 Sistemas de reporte o denuncia interna

Dentro de los programas de cumplimiento es un elemento esencial la implantación de unos sistemas de denuncia interna de irregularidades (whistleblowing), objeto del presente trabajo.

Debe adelantarse que dicho mecanismo no deja de suscitar recelos, especialmente por cierta predisposición contraria a la delación en el contexto cultural europeo. Asimismo, también plantea interesantes debates de encaje con determinados derechos fundamentales de raigambre constitucional. Se hará referencia más adelante a este tipo de previsiones.

Las FSGO señalan como una obligación para que el programa de cumplimiento pueda considerarse efectivo que cuente con un sistema de denuncias internas que contenga mecanismos que aseguren el anonimato y la confidencialidad, de tal manera que los empleados de la organización puedan presentar denuncias al conocer de conductas delictivas realizadas en el seno de la empresa sin miedo a represalias.

El informe del *Advisory Group* señala que la organización empresarial depende, en gran medida, de la información que pueda ser proporcionada por sus empleados y miembros para la corrección de potenciales o actuales conductas ilícitas ocurridas dentro de la empresa<sup>199</sup>. Por ello los mecanismos que se adopten para permitir el acceso de información deben cumplir con ciertos elementos mínimos<sup>200</sup>. Dicho informe deja claro que las investigaciones realizadas al respecto destacan que los empleados de una compañía no estarán predispuestos a dar información sobre prácticas

---

<sup>199</sup>Report of the Ad Hoc Advisory Group..., ob. cit., p. 77.

<sup>200</sup>ARTAZA VARELA, O., "Programas de cumplimiento...", ob. cit., pp. 260-261.

delictivas que puedan conocer si la compañía no asegura de alguna forma un alto grado de confidencialidad.<sup>201</sup>

En este sentido, se puede observar el desarrollo que ha tenido en la práctica empresarial y legislativa de Norteamérica, el tratamiento y la protección de los *whistleblower*, especialmente tras los escándalos empresariales de casos como *Enron*<sup>202</sup> o *Worldcom*<sup>203</sup> y lo determinantes que fueron los testimonios de los empleados de las respectivas compañías para el esclarecimiento de estos casos<sup>204</sup>.

Tal y como hemos apuntado, la implantación de un canal de denuncias es un requisito obligatorio establecido por el Código Penal Español para que el programa de cumplimiento pueda calificar como una atenuante o eximente en cuanto a la responsabilidad penal de la persona jurídica<sup>205</sup>.

## 2.6 Adopción de mecanismos disciplinarios y de incentivos internos

Como también hemos señalado, otro requisito exigible a un programa efectivo de cumplimiento, es el establecimiento de "mecanismos

---

<sup>201</sup> *Report of the Ad Hoc Advisory Group...*, ob. cit., p. 77. Al respecto, sostienen que tanto la experiencia como la investigación han demostrado que los integrantes de la empresa se muestran reacios a efectuar tales reportes (de denuncia) a menos que se asegure un alto nivel de confidencialidad, así como que no exista posibilidad alguna de que se tomen medidas en su contra si el reporte se efectúa de buena fe. Ver también GORDON, "Implementation...", ob. cit., p. 55, en relación al concepto de *non-retaliation*.

<sup>202</sup> Se demostró además que contar con documentos, códigos o manuales escritos no era suficiente – Enron tenía un código de conducta de 64 páginas –, redoblándose los esfuerzos por integrar el cumplimiento normativo en la cultura de la empresa y por monitorizar el desempeño.

<sup>203</sup> Para una descripción general de esta serie de casos, FRIEDRICH, D., "Enron et al.: Paradigmatic White Collar Crime Cases for the New Century", *Critical Criminology*, vol. 12, 2004, pp. 114 y ss.

<sup>204</sup> *Report of the Ad Hoc Advisory Group...*, ob. cit., p. 80. Para más detalles ver, entre otros, NIETO MARTIN, A., *La responsabilidad penal...*, ob. cit., pp. 255 y ss.; RODRÍGUEZ YAGÜE, C., "La protección de los *Whistleblowers* por el ordenamiento español: aspectos sustantivos y procesales", en AA.VV., *Fraude y Corrupción en el Derecho penal económico europeo. Eurodelitos de corrupción*, coords. L. Arroyo y A. Nieto Martín, edit. Universidad de Castilla-La Mancha, Cuenca, 2006, pp. 447 y ss.; RAGUÉS I VALLES, R., "¿Héroes o traidores?. La protección de los informantes internos (*whistleblowers*) como estrategia político criminal", *Indret* nº 3, 2006, pp. 7 y ss.; GORDON, S.D., "Implementation...", ob. cit., pp. 54 y ss.

<sup>205</sup> Artículo 31 del CP

disciplinarios o de incentivos internos”<sup>206</sup>. El principal objetivo de este requisito es reforzar la cultura organizacional mediante la presencia de consecuencias reales (tanto incentivos como medidas sancionadoras) que demuestren que el modelo no es sólo un documento sin transcendencia real en la práctica<sup>207</sup>.

Por ello, dentro del Programa de Cumplimiento también debe incluirse un protocolo disciplinario (sistema de infracciones y sanciones), sobre la base de que los principios éticos no tendrían la más mínima eficacia, si no se establecieran tales mecanismos coercitivos. Así se atribuye, al empresario la posibilidad de sancionar directamente los incumplimientos de políticas internas a los empleados que incumplan el Programa de Cumplimiento<sup>208</sup>.

## **2.7 Reacción adecuada y actualización permanente del modelo**

Una vez recibida la denuncia interna, la compañía debe establecer en el programa de cumplimiento la respuesta que dará a dicha denuncia y las medidas que se establecerán con el fin de prever dichas conductas detectadas. Las FSGO también establecen algunos criterios para definir qué medidas específicas deben tomar las empresas atendiendo a tres criterios<sup>209</sup>.

El primero de ellos es la incorporación al programa de los principios generalmente aceptados por la práctica empresarial, que además pueden estar determinados por la legislación aplicable. Las FSGO subrayan que la no incorporación de las costumbres empresariales típicas del sector al que pertenezca la organización empresarial así como estándares requeridos se

---

<sup>206</sup> *Report of the Ad Hoc Advisory Group...*, ob. cit., p. 86. En un sentido similar, GORDON, S.D., "Implementation...", ob. cit., p. 56.

<sup>207</sup> GRUNER, R.S./ BROWN, L.M., "Organizational Justice...", ob. cit., p. 751.

<sup>208</sup> GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 379.

<sup>209</sup> GÓMEZ-JARA DIEZ, *La responsabilidad penal*, cit., pp. 127 y ss.

tendrá en cuenta de manera muy negativa en el momento de valorar si el programa ético y de cumplimiento resulta verdaderamente efectivo.

El segundo es el tamaño de la organización. Para todo tipo de tamaños se exige la misma eficacia y el mismo nivel de calidad de los mecanismos implementados pero a organizaciones empresariales pequeñas no se les exige ni el mismo nivel de gasto en la implementación de estas medidas, ni el mismo nivel de formalidades que les son exigibles a empresas de mayor tamaño<sup>210</sup>.

En tercer lugar, debe tenerse en cuenta si la conducta delictiva ya se había producido con anterioridad en la empresa. Lo anterior significaría que los procedimientos internos no han sido actualizados para hacerlos efectivos, incumpliendo uno de los criterios básicos de efectividad descritos con anterioridad.

### **3. Naturaleza y eficacia jurídico-laboral de los programas de cumplimiento**

Al estudiar la naturaleza que tiene un plan de cumplimiento se llega a la conclusión de que reviste fundamentalmente de una naturaleza privada, ya que contiene una serie de pautas y normas que despliegan sus efectos entre la empresa como persona jurídica y sus directivos y empleados. No obstante, no es menos cierto que un plan de cumplimiento sí tiene también cierto carácter público, en la medida en que también tiene como objetivo fundamental el respeto de la legalidad y la neutralización de los riesgos penales<sup>211</sup>.

Podría decirse que los planes de cumplimiento funcionan sobre dos planos distintos de la ética: una ética interna y una externa. La ética interna trata de ejemplificar los comportamientos aceptables para la empresa y establecer las

---

<sup>210</sup>ARTAZA VARELA, O., "Programas de cumplimiento...", ob. cit., p. 265.

<sup>211</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 383-384.



pautas de conducta acordes a sus valores, tratando de hacer una compañía íntegra y respetuosa, que vela internamente por el cumplimiento de la legalidad y de las normas propias de actuación, mientras un plan de cumplimiento también tiene que implantar una ética externa, en el sentido de que intenta preservar el orden público mediante el diseño y la ejecución de un buen sistema de prevención de delitos.

Estos programas de *compliance*, en contraste con otras guías o códigos de conducta, con los que comparte un fin ético corporativo similar, tienen un objeto más preciso y – en cierta manera, instrumental- en la medida en que se conciben para la función de cumplimiento efectivo de los compromisos en evitación de posibles responsabilidades especialmente en el ámbito penal<sup>212</sup>.

La cuestión que debe analizarse aquí es la inclusión de este catálogo de conductas de cumplimiento obligatorio dentro del sistema normativo o de fuentes de la relación laboral. No se puede decir que carezcan de efectividad o se hallen desprovistas de toda trascendencia jurídica, porque se trata de formulaciones éticas de carácter preceptivo que comportan un grado de compromiso aun mayor que las propias normas jurídicas, en la medida en que expresan verdaderas y propias obligaciones exigibles a los directivos y trabajadores, y cuya contravención depara efectos en el ámbito disciplinario. Pero, ¿de dónde le viene al empresario la facultad de dictar pautas de comportamiento que devienen referencias inexcusables para los empleados?

Es de sobra conocido que el empresario, tras la derogación en el Estatuto de los Trabajadores de 1980 (ET) de las normas que habilitaban para dictar reglamentos de régimen interior de la empresa, carece de potestad normativa para regular condiciones de trabajo y de comportamiento en la empresa.<sup>213</sup> Por tanto, está descartado que el plan de *compliance* constituya una

---

<sup>212</sup>MORATO GARCÍA, R.M., "Incumplimiento de los códigos...", ob. cit., pp. 422 y ss.

<sup>213</sup>GOÑI SEIN, J. L., "Valor Jurídico de los códigos de conducta empresariales", AA.VV., *Ética empresarial y códigos de conducta*, dir. J.L. Goñi, Madrid, 2011, pp. 584 y ss.

manifestación del poder normativo del empresario, como, se ha encargado de puntualizar nuestro Tribunal Supremo en la sentencia de 11 de junio de 2008, al señalar que el empresario no ostenta “*ninguna facultad normativa sobre la ordenación de la relación laboral*”<sup>214</sup>.

Con todo, el TS no ha negado que el empresario posea cierto deber unilateral de facto y discrecional para establecer obligaciones laborales, sino que lo ha situado dentro del ámbito del poder de dirección del art. 20 del ET, esto es, en la potestad del empresario para dictar instrucciones en el ejercicio de las facultades directivas<sup>215</sup>.

Sin embargo, dicha afirmación debe ser matizada, ya que el poder de dirección no puede suponer un poder ilimitado de regulación de las condiciones de trabajo, ni puede constituir un derecho que permita eludir los mecanismos que nuestro derecho (y el de muchos de los ordenamientos jurídicos comparados) tiene para la fijación de las condiciones de trabajo, tal y como es la negociación colectiva y la participación de los representantes de los trabajadores (art. 82.2 TRLET).

Por ello, parece razonable entender que no serán admisibles las obligaciones de cumplimiento normativo que puedan exceder lo que pueda ser integrado de forma natural en el contenido del contrato, según los principios de la buena fe contractual, ni tampoco aquellas otras que puedan sobrepasar los límites impuestos por el ejercicio regular del poder de dirección, dispuesto a través del cumplimiento de los trabajadores de las órdenes e infracciones del empresario (arts. 5, c y 20.2 TRLET).

---

<sup>214</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 385-386.

<sup>215</sup>En la sentencia de 7 de marzo de 2007, el Tribunal Supremo ha declarado la idoneidad jurídica de la circular interna del código de conducta del personal del Banco de España para regular materias de carácter estrictamente laboral, afirmando que “*no existe obstáculo alguno de orden lógico o jurídico para que tal normativa de autodeterminación no se extienda también a materias de innegable naturaleza laboral, pues ello no significaría más que el simple ejercicio del poder de dirección que al empresario corresponde art. 20 ET*”.

#### **4. El cumplimiento normativo en ordenamientos de sociedades especiales**

A lo largo de los últimos años en diversos sectores se han desarrollado normas y recomendaciones relativas al denominado buen gobierno corporativo, incorporando frecuentemente programas de cumplimiento normativo, en alguno de los cuales se ha contemplado el establecimiento de canales de denuncia. Se analizará este fenómeno en el ámbito de las sociedades cotizadas y en el de las sociedades que actúan en los mercados financieros (entidades de crédito, entidades aseguradoras y empresas de servicios de inversión).

##### **4.1 El gobierno corporativo, el cumplimiento normativo y el canal de denuncia en la regulación de las sociedades cotizadas**

A partir de la crisis financiera internacional, han surgido numerosas iniciativas relacionadas con las buenas prácticas en materia de gobierno corporativo, pues entre las diversas causas que la propiciaron se encuentran importantes deficiencias en esta materia. Diversos organismos internacionales y, en particular, la OCDE y la Unión Europea han mostrado especial preocupación por el establecimiento de un adecuado control y una eficiente y prudente gestión de los riesgos en las empresas. Se ha alcanzado el convencimiento de la trascendencia que tiene para las sociedades cotizadas ser gestionadas de manera transparente<sup>216</sup>. Esa perseguida transparencia abarca diversos ámbitos, entre los que se encuentran la estructura organizativa y la situación financiera patrimonial.

---

<sup>216</sup>La transparencia que se requiere para el eficiente funcionamiento de los mercados de valores, se extiende a las sociedades que cotizan en ellos. Las sociedades cotizadas han de ser gestionadas de manera transparente como factor esencial para la generación de valor en las empresas, la mejora de la eficiencia económica y el refuerzo de la confianza de los inversores. La transparencia mejora el control interno, la responsabilidad corporativa y favorece la confianza de accionistas e inversores potenciales. La transparencia se proyecta sobre diversos ámbitos: la estructura organizativa, la situación financiero-patrimonial, las decisiones básicas de gestión con trascendencia en la negociación de los valores y la estructura accionarial. Vid. Código del buen gobierno de las sociedades cotizadas, CNMV, 18 de febrero de 2015, p. 7.

En España ha habido avances muy apreciables en materia de buen gobierno corporativo, con la finalidad de mejorar la eficacia y responsabilidad en la gestión de las sociedades y de colocar a un alto nivel los estándares nacionales de cumplimiento de los principios de buen gobierno. El Consejo de Ministros de 10 de mayo de 2013, acordó la creación de una Comisión de Expertos en materia de gobierno corporativo<sup>217</sup>, para proponer las iniciativas y las reformas normativas que se considerasen adecuadas para garantizar el buen gobierno de las empresas y para prestar apoyo y asesoramiento a la CNMV en la modificación del Código Unificado de Buen Gobierno de las Sociedades Cotizadas de mayo de 2006<sup>218</sup>.

La Comisión de Expertos, en atención al mandato recibido, desarrolló su trabajo distinguiendo entre las mejoras de gobierno corporativo que debían ser incorporadas a normas legales, y aquellas otras que debían mantenerse como recomendaciones de buen gobierno de carácter voluntario, sujetas al principio conocido internacionalmente como "cumplir o explicar".

La Comisión de Expertos en materia de Gobierno Corporativo elaboró el "Estudio sobre propuestas de modificaciones normativas" de fecha 14 de octubre de 2013<sup>219</sup>. La Ley 31/2014, de 3 de diciembre, por la que se modificó

---

<sup>217</sup>Orden ECC/895/2013, de 21 de mayo, por la que se publica el Acuerdo del Consejo de Ministros de 10 de mayo de 2013, por el que se crea una Comisión de expertos en materia de gobierno corporativo.

<sup>218</sup>Los objetivos que debían guiar a esta Comisión eran velar por el adecuado funcionamiento de los órganos de gobierno y administración de las empresas españolas para conducir las a las máximas cotas de competitividad; generar confianza y transparencia para los accionistas e inversores nacionales y extranjeros; mejorar el control interno y la responsabilidad corporativa de las empresas españolas, y asegurar la adecuada segregación de funciones, deberes y responsabilidades en las empresas, desde una perspectiva de máxima profesionalidad y rigor (Vid. Código del buen gobierno de las sociedades cotizadas, CNMV, 18 de febrero de 2015, pp. 7-8).

<sup>219</sup>*Estudio sobre propuestas de modificaciones normativas. Comisión de Expertos en materia de Gobierno Corporativo (creada por Acuerdo del Consejo de Ministros, de 10 de mayo de 2013, publicado por Orden ECC/895/2013, de 21 de mayo), Madrid, 14 de octubre de 2013, en [http://www.cnmv.es/docportal/publicaciones/codigogov/cegc\\_estmodif\\_20131014.pdf](http://www.cnmv.es/docportal/publicaciones/codigogov/cegc_estmodif_20131014.pdf), p. 4.*

Este estudio se apoyó en la Propuesta de Código Mercantil, elaborada por la Sección de Derecho Mercantil de la Comisión General de Codificación de 17 de junio de 2013.

En este Estudio, entre otros aspectos, se consideraba que el conjunto de facultades indelegables del Consejo de Administración debía completarse con asuntos que habían sido objeto de especial consideración a raíz de la crisis financiera, como son: la determinación de la política de control y

la Ley de Sociedades de Capital para la mejora del gobierno corporativo, reconoció expresamente que su articulado se basaba en este "Estudio de la Comisión de Expertos", respetando la práctica totalidad de sus recomendaciones (Preámbulo III). Por esta Ley se establecen entre las facultades indelegables del Consejo de Administración de las sociedades cotizadas: la determinación de la política de control y gestión de riesgos, la supervisión de los sistemas internos de información y control, y la determinación de la política de gobierno corporativo de la sociedad (arts. 529 ter y 249 bis TRLSC). Asimismo, se dispone que el Consejo de Administración de una sociedad anónima cotizada debe constituir una comisión de auditoría (art. 529 terdecies.2 TRLSC). El número de miembros de la comisión de auditoría y su funcionamiento deben establecerse en los estatutos o en el reglamento del Consejo de Administración, debiendo favorecerse la independencia en el ejercicio de sus funciones<sup>220</sup> (art. 529 quaterdecies.3 TRLSC). Entre sus funciones está la de supervisar la eficacia del control interno de la sociedad y los sistemas de gestión de riesgos, así

---

gestión de riesgos, y la supervisión de los sistemas internos de información y control (*Estudio sobre propuestas de modificaciones normativas. Comisión de Expertos en materia de Gobierno Corporativo...*, ob. cit., p. 45). Se proponía que el Consejo de Administración de las sociedades cotizadas no pudiera delegar las facultades de decisión en determinadas materias, entre las que se encontraban específicamente la determinación de la política de control y gestión de riesgos y la supervisión de los sistemas internos de información y control (*Estudio sobre propuestas de modificaciones normativas. Comisión de Expertos en materia de Gobierno Corporativo...*, ob. cit., p. 46). Así mismo se sugería que el Consejo de Administración de una sociedad cotizada debía constituir obligatoriamente, una comisión de auditoría.

La Comisión de Expertos considera que la Comisión de Auditoría debe estar (i) formada íntegramente por consejeros no ejecutivos; (ii) al menos dos de sus miembros deben ser independientes, y al menos uno debe ser designado teniendo en cuenta sus conocimientos y experiencia en materia de contabilidad, auditoría o en ambas; (iii) el presidente debe ser un consejero independiente (*Estudio sobre propuestas de modificaciones normativas. Comisión de Expertos en materia de Gobierno Corporativo...*, ob. cit., p. 64). En el reglamento del Consejo de Administración debería disponerse que la Comisión de Auditoría tendría, entre otras funciones la de supervisar la eficacia del control interno de la sociedad y los sistemas de gestión de riesgos (*Estudio sobre propuestas de modificaciones normativas. Comisión de Expertos en materia de Gobierno Corporativo...*, ob. cit., p. 65).

<sup>220</sup>Esta Comisión ha de estar compuesta exclusivamente por consejeros no ejecutivos, dos al menos, deben ser consejeros independientes y uno de ellos ha de ser designado teniendo en cuenta sus conocimientos y experiencia en materia de contabilidad, auditoría o en ambas (art. 529 quaterdecies.1 LSC). El presidente debe ser designado de entre los consejeros independientes que formen parte de ella y debe ser sustituido cada cuatro años, si bien puede ser reelegido una vez transcurrido un plazo de un año desde su cese (art. 529 quaterdecies.2 TRLSC).

como gestionar con el auditor de cuentas las debilidades significativas del sistema de control interno detectadas en el desarrollo de la auditoría, sin quebrantar su independencia (art. 529 quaterdecies.3 y 4 TRLSC).

Las sociedades anónimas cotizadas deben hacer público un informe anual de gobierno corporativo (arts. 540.1 y 538 TRLSC). Dicho informe debe enviarse a la CNMV y publicarse como hecho relevante (art. 540.2 y 3 TRLSC). El informe debe ofrecer una explicación detallada de la estructura del sistema de gobierno de la sociedad y de su funcionamiento. El informe de gobierno corporativo debe incluir un apartado dedicado a sistemas de control del riesgo (art. 540.4.e TRLSC); así mismo, debe consignarse el grado de seguimiento de las recomendaciones de gobierno corporativo o, en su caso, la explicación de la falta de seguimiento de dichas recomendaciones (art. 540.4.g TRLSC), atendiendo al principio de "cumplir o explicar"<sup>221</sup>.

La Comisión de Expertos elaboró y la CNMV aprobó el "Código de buen gobierno de las sociedades cotizadas", de 18 de febrero de 2015<sup>222</sup>, el cual está dirigido a las sociedades cotizadas<sup>223</sup> y se caracteriza por la voluntariedad, con sujeción al principio de "cumplir o explicar"<sup>224</sup>.

---

<sup>221</sup>Cada sociedad es libre de seguir estas recomendaciones de gobierno corporativo, pero se exige que, cuando no se cumplan, se expliquen los motivos de no hacerlo, al objeto de que los accionistas, los inversores y los mercados lo valoren.

<sup>222</sup>Código del buen gobierno de las sociedades cotizadas, CNMV, 18 de febrero de 2015, disponible en [https://www.cnmv.es/docportal/publicaciones/codigogov/codigo\\_buen\\_gobierno.pdf](https://www.cnmv.es/docportal/publicaciones/codigogov/codigo_buen_gobierno.pdf).

<sup>223</sup>Se entiende por tales aquellas cuyas acciones están admitidas a negociación en un mercado secundario oficial de valores (art. 495.1 TRLSC).

<sup>224</sup>La utilización de códigos de buen gobierno de carácter voluntario junto con el principio de "cumplir o explicar" es el sistema seguido de forma consistente en los principales países de la Unión Europea y en otros países desarrollados, resaltando su flexibilidad en el modo de ser aplicado y la posibilidad de constituirse en una referencia de buenas prácticas de gobierno corporativo. La Unión Europea ha recogido expresamente en su normativa la validez de este principio de actuación, confirmado en el Libro Verde de la Unión Europea sobre gobierno corporativo de las sociedades cotizadas. (Bruselas, 5.4.2011 COM(2011) 164 final).

El Código recomienda reforzar las normas legales en relación con la función de la auditoría interna, ampliar las funciones de la comisión de auditoría y establecer determinados criterios adicionales sobre su composición que refuercen su especialización e independencia. Así, se recomienda: a) que los miembros de la comisión de auditoría, y de forma especial su presidente, se designen teniendo en cuenta sus conocimientos y experiencia en materia de contabilidad, auditoría o gestión de riesgos, y que la mayoría de dichos miembros sean consejeros independientes (Recomendación 39); b) que bajo la supervisión de la comisión de auditoría, se disponga de una unidad que asuma la función de auditoría interna que vele por el buen funcionamiento de los sistemas de información y control interno y que funcionalmente dependa del presidente no ejecutivo del consejo o del de la comisión de auditoría (Recomendación 40); c) que el responsable de la unidad que asuma la función de auditoría interna presente a la comisión de auditoría su plan anual de trabajo, informe directamente de las incidencias que se presenten en su desarrollo y someta al final de cada ejercicio un informe de actividades (Recomendación 41); d) que a la comisión de auditoría en relación con los sistemas de información y control interno además de las funciones previstas en la Ley, le corresponda la función de *"establecer y supervisar un mecanismo que permita a los empleados comunicar, de forma confidencial y, si resulta posible y se considera apropiado, anónima, las irregularidades de potencial trascendencia, especialmente financieras y contables, que adviertan en el seno de la empresa"* (Recomendación 42.1.c).

Asimismo se señala que la sociedad debe disponer de una función de control y gestión de riesgos ejercida por una unidad o departamento interno, bajo la supervisión directa de la comisión de auditoría o, en su caso, de otra comisión especializada del Consejo de Administración<sup>225</sup>. La legislación mercantil incluye entre las facultades indelegables del Consejo de Administración la

---

<sup>225</sup>Código del buen gobierno de las sociedades cotizadas, CNMV, 18 de febrero de 2015, II. Principios, II.3. Consejo de administración, punto 21, p. 15.

aprobación de una política de control y gestión de riesgos (art. 529 ter TRLSC). El Código avanza un paso más, pues recomienda que la política de control y gestión de riesgos identifique al menos: a) los distintos tipos de riesgo, financieros y no financieros (entre otros los operativos, tecnológicos, legales, sociales, medio ambientales, políticos y reputacionales); b) la fijación del nivel de riesgo que la sociedad considere aceptable; c) las medidas previstas para mitigar el impacto de los riesgos identificados, en caso de que llegaran a materializarse; d) los sistemas de información y control interno que se vayan a utilizar para controlar y gestionar los riesgos, incluidos los pasivos contingentes o riesgos fuera de balance (Recomendación 45). Así mismo el Código recomienda que bajo la supervisión directa de la comisión de auditoría o, en su caso, de una comisión especializada del Consejo de Administración, exista una función interna de control y gestión de riesgos ejercida por una unidad o departamento interno de la sociedad, que tenga atribuidas expresamente las siguientes funciones: a) asegurar el buen funcionamiento de los sistemas de control y gestión de riesgos y, en particular, que se identifiquen, gestionen, y cuantifiquen adecuadamente todos los riesgos importantes que afecten a la sociedad; b) participar activamente en la elaboración de la estrategia de riesgos y en las decisiones importantes sobre su gestión; c) velar por que los sistemas de control y gestión de riesgos mitiguen los riesgos adecuadamente en el marco de la política definida por el Consejo de Administración (Recomendación 46).

El Código recomienda que la supervisión del cumplimiento de las reglas de gobierno corporativo, de los códigos internos de conducta y de la política de responsabilidad social corporativa se atribuya a una o se reparta entre varias comisiones del Consejo de Administración, que pueden ser la comisión de auditoría, la de nombramientos, la de responsabilidad social corporativa, en caso de existir, o una comisión especializada, que el Consejo de Administración decida crear al efecto, a las que específicamente se les atribuyan entre otras, la "*supervisión del cumplimiento de los códigos internos*



*de conducta y de las reglas de gobierno corporativo de la sociedad"* y la "evaluación de todo lo relativo a los riesgos no financieros de la empresa incluyendo los operativos, tecnológicos, legales, sociales, medio ambientales, políticos y reputacionales" (Recomendación 53.a y g).

El Código recomienda que la política de responsabilidad social corporativa<sup>226</sup> incluya los principios o compromisos que la empresa asuma voluntariamente en su relación con los distintos grupos de interés e identifique al menos, entre otros: los mecanismos de supervisión del riesgo no financiero, la ética y la conducta empresarial; los *canales de comunicación*, participación y diálogo con los grupos de interés (Recomendación 54 letras e y f).

#### **4.2 El cumplimiento normativo en el ordenamiento de las entidades de crédito**

El Comité de Basilea de Supervisión Bancaria acordó en diciembre de 2010 el "Marco regulador global para reforzar los bancos y sistemas bancarios" (Basilea III), que tenía como finalidad evitar futuras crisis y mejorar la cooperación internacional. La Unión Europea trasladó a su ordenamiento jurídico esos acuerdos mediante el Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de servicios de inversión, y por el que se modifica el Reglamento (UE) n.º 648/2012 y la Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de servicios de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE<sup>227</sup>.

---

<sup>226</sup>Sobre el marco normativo de la responsabilidad social corporativa y en el derecho de sociedades vid. EMBID IRUJO, J. M./ DEL VAL TALENS, P., *La responsabilidad social corporativa y el Derecho de sociedades de capital: entre la regulación legislativa y el soft law*, Madrid, 2016, pp. 74 y ss.

<sup>227</sup>Vid. SPINDLER, G., "Reformas en el gobierno corporativo al nivel de los órganos de Risk Management Recent reforms in corporate governance of banks according to the CRD IV-Directive",

Dentro del ordenamiento español y encuadrada en este marco de reformas, la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito, y su desarrollo reglamentario<sup>228</sup>, han supuesto para estas entidades un avance muy sustantivo en materia de gobierno corporativo. Las reformas introducidas pretenden el establecimiento de sistemas de gobierno corporativo eficientes<sup>229</sup>, ante la evidencia de que la regulación prudencial de las entidades de crédito debe promover las prácticas de gestión más eficientes y óptimas para el desarrollo de una actividad compleja y arriesgada como es la financiera (Preámbulo II).

Las entidades de crédito deben ejercer su actividad sometidas a las normas de gobierno corporativo establecidas en la LOSSEC y a las demás que resulten aplicables<sup>230</sup> (art. 28 LOSSEC). Estas entidades deben establecer procedimientos sólidos de gobierno corporativo<sup>231</sup>, que han de incluir procedimientos eficaces de identificación, gestión, control y comunicación de los riesgos a los que estén expuestas o puedan estarlo y mecanismos

---

en AA.VV., *Crisis y reforma del sistema financiero*, coords. A.J. Recalde Castells, I. Tirado Martí y A.B. Perdices Huetos, Pamplona, 2014, p. 235.

<sup>228</sup>Real Decreto 84/2015, de 13 de febrero, por el que se desarrolla la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

<sup>229</sup>Vid. FERNANDEZ-SORDO LLANEZA, E., "El gobierno corporativo de las entidades financieras ante la crisis económica", en AA.VV., *Crisis y reforma del sistema financiero*, coords. A.J. Recalde Castells, I. Tirado Martí y A. B. Perdices Huetos, Pamplona, 2014, p. 293.

<sup>230</sup>TAPIA HERMIDA, A.J., señala que estas normas legales de gobierno corporativo tienen una naturaleza mixta, abarcan normas de gobierno corporativo en sentido estricto y normas de gestión y control de los riesgos típicos de la actividad bancaria. Por ello, este conjunto de normas no concuerda exactamente con lo que se entiende como reglas de buen gobierno en las sociedades cotizadas. La LOSSEC llama "sistema de gobierno corporativo" de las entidades de crédito (art. 29) a disposiciones relativas a las condiciones de acceso y de ejercicio de su actividad bancaria, que se extiende a un conjunto de normas que van más allá de las reglas tradicionales de buen gobierno del Derecho de Sociedades, pues no sólo se refieren a las relaciones internas de los órganos de la entidad de crédito en beneficio de sus socios; sino que alcanzan a la gestión eficiente de los riesgos típicos de la actividad bancaria, en beneficio de sus clientes. Esta misma amplitud de las denominadas "normas de gobierno corporativo" se contemplaba en la regulación de los otros intermediarios financieros típicos: las empresas de servicios de inversión y las entidades aseguradoras (*Manual de Derecho del Mercado Financiero*, Madrid, 2015, p. 100).

<sup>231</sup>Vid. ALCALÁ DÍAZ, M.A., "Las normas de gobierno corporativo de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de las entidades de crédito", *Revista La Ley mercantil*, nº 10, 2015, pp. 4-11.

adecuados de control interno<sup>232</sup>. Estos procedimientos y mecanismos deben ser exhaustivos y proporcionados a la naturaleza, escala y complejidad de los riesgos inherentes al modelo empresarial y a las actividades de la entidad y deben respetar los criterios técnicos relativos a la organización y al tratamiento de los riesgos que se determinan reglamentariamente (art. 29.1 LOSSEC).

El Consejo de Administración de las entidades de crédito debe definir un sistema de gobierno corporativo que garantice una gestión sana y prudente, y que incluya el adecuado reparto de funciones en la organización y la prevención de conflictos de intereses, así mismo debe controlar y evaluar periódicamente su eficacia y adoptar las medidas adecuadas para solventar sus deficiencias. El Consejo de Administración tiene como funciones indelegables la vigilancia, control y evaluación periódica de la eficacia del sistema de gobierno corporativo, así como la adopción de las medidas adecuadas para solventar sus deficiencias; y asumir la aprobación y vigilancia de la aplicación de su estrategia de riesgo y su gobierno interno (art. 29.2 y 3 LOSSEC).

Las entidades de crédito deben contar en base consolidada o subconsolidada, y en su caso individual, con sistemas, estrategias, procedimientos y mecanismos para dar cumplimiento a la normativa de ordenación y disciplina. A tal efecto, deben: disponer de una función de auditoría interna que vele por el buen funcionamiento de los sistemas de información y control interno; y contar con una unidad que desempeñe "*la función de cumplimiento normativo*", esta función debe tener carácter integral, comprendiendo, entre otras, las obligaciones que al respecto resulten de la prestación de servicios de inversión y de la normativa de prevención del blanqueo de capitales (art. 43.1.b y c ROSSEC).

---

<sup>232</sup>Igualmente, como parte de los procedimientos de gobierno y estructura organizativa, las entidades de crédito y grupos consolidables de entidades de crédito que presten servicios de inversión deben respetar los requisitos de organización interna recogidos en la legislación de los mercados de valores (art. 29.6 LOSSEC).

Estas funciones de auditoría interna y "*de cumplimiento normativo*" deben ser desempeñadas bajo el principio de independencia respecto a las áreas, unidades o funciones sobre las que gire su verificación. El Consejo de Administración de la entidad de crédito debe ser informado periódicamente, de los resultados de las labores verificativas llevadas a cabo por las funciones de auditoría interna y "*de cumplimiento normativo*" (art. 43.2 ROSSEC).

El Consejo de Administración es el responsable de los riesgos que asuma una entidad de crédito. El Consejo de Administración debe en el ejercicio de su responsabilidad sobre gestión de riesgos: a) dedicar tiempo suficiente a la consideración de las cuestiones relacionadas con los riesgos; b) aprobar y revisar periódicamente las estrategias y políticas de asunción, gestión, supervisión y reducción de los riesgos a los que esté o pueda estar expuesta. A estos efectos, se deben establecer canales eficaces de información hacia el Consejo de Administración que abarquen todos los riesgos importantes y las políticas de gestión de riesgos y sus modificaciones; así mismo deben garantizar que el Consejo de Administración pueda acceder sin dificultades a la información sobre la situación de riesgo de la entidad y, si fuese necesario, a la función de gestión de riesgos y a asesoramiento externo especializado (art. 37 LOSSEC y art. 44 ROSSEC).

Las entidades de crédito deben disponer de una unidad u órgano que asuma la función de gestión de riesgos proporcional a la naturaleza, escala y complejidad de sus actividades, independiente de las funciones operativas, que tenga autoridad, rango y recursos suficientes, así como el oportuno acceso al Consejo de Administración (art. 38.1 LOSSEC)<sup>233</sup>.

---

<sup>233</sup>Las entidades de crédito que determina el Banco de España (en razón a su tamaño, su organización interna y por la naturaleza, la escala y la complejidad de sus actividades), deben establecer un comité de riesgos. Este comité ha de estar integrado por miembros del consejo de administración que no desempeñen funciones ejecutivas y que posean los oportunos conocimientos, capacidad y experiencia para entender plenamente y controlar la estrategia de riesgo y la propensión al riesgo de la entidad, y en todo caso el presidente y al menos un tercio de los miembros han de ser consejeros independientes. Las entidades que a juicio del Banco de España no tengan que

Al Banco de España le corresponde supervisar los sistemas, estrategias, procedimientos o mecanismos de cualquier tipo, aplicados por las entidades de crédito para dar "*cumplimiento a la normativa de ordenación y disciplina*" (art. 51 LOSSEC). Al Banco de España le corresponde supervisar los riesgos a los cuales están o pueden estar expuestas las entidades, y determinar si los mecanismos "*de cumplimiento normativo*"<sup>234</sup> mantenidos por las entidades de crédito garantizan una gestión y cobertura sólida de sus riesgos (art. 52 LOSSEC)<sup>235</sup>. También le corresponde al Banco de España supervisar el cumplimiento por parte de las entidades de crédito de las normas sobre responsabilidad en la gestión de riesgos, así como de las demás normas sobre gobierno corporativo (art. 53 LOSSEC).

#### **4.3 El cumplimiento normativo en la regulación de las entidades aseguradoras<sup>236</sup>**

El cumplimiento normativo en el sector asegurador ha tenido un importante desarrollo en el ordenamiento comunitario. La Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su

---

establecer un comité de riesgos han de constituir comisiones mixtas de auditoría que asumirán las funciones correspondientes del comité de riesgos (art. 38 LOSSEC).

<sup>234</sup>El Banco de España puede elaborar guías técnicas, dirigidas a las entidades y grupos supervisados, indicando los criterios, prácticas, metodologías o procedimientos que considera adecuados para el cumplimiento de la normativa de supervisión. Las guías elaboradas por el Banco de España se han de referir, entre otros, a la evaluación de los riesgos y al adecuado cumplimiento de normas de ordenación y disciplina (art. 54.a LOSSEC). El Banco de España puede requerir a las entidades y grupos supervisados una explicación de los motivos por los que se hubieran separado de dichos criterios, prácticas, metodologías o procedimientos.

<sup>235</sup>Vid. TAPIA HERMIDA, A.J., *Manual...*, ob. cit., p. 114.

<sup>236</sup>En relación con esta materia, hay que destacar el FORO ASEGURADOR DE CUMPLIMIENTO ha publicado en la *Revista Española de Seguros* el cuaderno monográfico nº 7, 2016, dedicado a *La función de verificación de cumplimiento*. Así mismo vid. TAPIA HERMIDA, A.J., "Los puntos críticos del proceso de implementación del sistema de gobierno en las entidades aseguradoras españolas", Blog de Alberto J. Tapia Hermida, 28 marzo, 2016, disponible en <http://ajtapia.com/2016/03/los-puntos-criticos-del-proceso-de-implementacion-del-sistema-de-gobierno-en-las-entidades-aseguradoras-espanolas/>

ejercicio (Solvencia II)<sup>237</sup>, completada por el Reglamento Delegado UE 2015/35<sup>238</sup>, dispone que las empresas de seguros y de reaseguros deben establecer un sistema eficaz de control interno (formando parte del segundo pilar de Solvencia II)<sup>239</sup>, que ha de constar, como mínimo, de procedimientos administrativos y contables, de un marco de control interno, de mecanismos adecuados de información a todos los niveles de la empresa y de una "*función de verificación del cumplimiento*"<sup>240</sup>. Esta "*función de verificación del cumplimiento*" ha de comprender el asesoramiento al órgano de administración, dirección o supervisión acerca del cumplimiento de las disposiciones legales, reglamentarias y administrativas<sup>241</sup>; asimismo, le corresponde la evaluación de las posibles repercusiones de cualquier modificación del entorno legal en las operaciones de la empresa y la determinación y evaluación del riesgo de cumplimiento (art. 46 Directiva 2009/138/CE y art. 266 Reglamento Delegado (UE) 2015/35). La "*función de*

---

<sup>237</sup>Vid. CASTILLO PLAZA, C. A., "Transposición e implementación de la directiva 2009/138/CE (SOLVENCIA II)", en AA.VV., *La reforma del derecho del seguro*, dirs. J. Bataller Grau, M.R. Quintans Eiras y A.B. Veiga Copo, Pamplona, 2015, pp. 305 y ss.

<sup>238</sup>Esta Directiva 2009/138/CE está completada por el Reglamento Delegado UE 2015/35, de la Comisión de 10 de octubre de 2014 por el que se completa la Directiva 2009/138/CE del Parlamento Europeo y del Consejo sobre el acceso a la actividad de seguro y reaseguro y su ejercicio.

<sup>239</sup>La Directiva Solvencia II basa en tres pilares que se refuerzan mutuamente su concepción de la solvencia de las entidades aseguradoras y reaseguradoras. El primero está constituido por reglas uniformes sobre requerimientos de capital determinados en función de los riesgos asumidos por las entidades. El segundo de los pilares está integrado por un nuevo sistema de supervisión con el objetivo de fomentar la mejora de la gestión interna de los riesgos por las entidades. El tercero se refiere a las exigencias de información y transparencia hacia el mercado sobre los aspectos clave de los riesgos asumidos por las entidades y su forma de gestión (Preámbulo II, 2º párr. LOSSEAR).

Una de las novedades que incorporó la Directiva 2009/138/CE (Directiva Solvencia II) es el reconocer que algunos riesgos sólo pueden tenerse debidamente en cuenta a través de exigencias en materia de gobierno de las entidades y no a través de los requisitos cuantitativos.

<sup>240</sup>El Reglamento Delegado (UE) 2015/35 establece que el sistema de control interno ha de garantizar el cumplimiento de las disposiciones legales, reglamentarias y administrativas vigentes por parte de la empresa de seguros o reaseguros, así como la eficiencia y la eficacia de las operaciones de la empresa a la luz de sus objetivos, y garantizará también la disponibilidad de información financiera y de otro tipo y su fiabilidad (art. 266 Reglamento Delegado (UE) 2015/35).

<sup>241</sup>Las empresas de seguros y reaseguros deben establecer políticas documentadas y procedimientos adecuados para garantizar que todas las personas que dirijan de manera efectiva la empresa o desempeñen otras funciones fundamentales cumplan en todo momento las exigencias de aptitud (cualificación profesional, competencia y experiencia adecuadas para hacer posible una gestión sana y prudente) y honorabilidad (personas de buena reputación e integridad) vid. art. 42 de la Directiva 2009/138/CE y art. 273 Reglamento Delegado (UE) 2015/35).

*verificación del cumplimiento*" de las empresas de seguros y reaseguros ha de establecer una política y un plan de verificación del cumplimiento. La "*política de verificación del cumplimiento*" debe definir las responsabilidades, competencias y deberes de información de la función de verificación del cumplimiento. El "*plan de verificación del cumplimiento*" ha de establecer las actividades previstas de la función de verificación del cumplimiento, que tendrán en cuenta todas las áreas de actividad pertinentes de las empresas de seguros y reaseguros y su exposición al riesgo de incumplimiento. Las obligaciones de la *función de verificación del cumplimiento* deben incluir la evaluación de la idoneidad de las medidas adoptadas por la empresa de seguros o reaseguros para evitar cualquier incumplimiento (art. 270 Reglamento Delegado UE 2015/35).

El Reglamento Delegado contiene diversos mecanismos para desarrollar las actividades de la "*función de cumplimiento*". Así, se establece que el informe sobre la situación financiera y de solvencia debe contener información, en relación con el sistema de control interno, "*una descripción de cómo se implementa la función de verificación del cumplimiento*" (art. 294.5.b). El informe periódico de supervisión debe incluir "información sobre las actividades realizadas con arreglo a la función de verificación durante el período de referencia" (art. 308.5.b). Así mismo, respecto de la supervisión de la solvencia de grupo en relación con los grupos con gestión centralizada de riesgo se dispone que las empresas matrices deben de incluir entre las actividades de su función de cumplimiento las que afecten a sus filiales<sup>242</sup> (art. 351.1.b).

En la normativa nacional acorde con lo dispuesto en la Directiva 2009/138/CE y asumiendo lo establecido en el Reglamento Delegado UE 2015/35, se

---

<sup>242</sup>Al evaluar si los procesos de gestión de riesgos y los mecanismos de control interno de la empresa matriz engloban a la filial, el supervisor de grupo y las demás autoridades de supervisión afectadas deben analizar si se cumple, entre otros, el requisito de que la empresa matriz lleve a cabo en gran medida la función de verificación del cumplimiento con respecto a la filial, de forma que dicha empresa matriz lleve a cabo la mayoría de las tareas de la función de verificación del cumplimiento (art. 351.1.b Reglamento Delegado UE 2015/35)

establece como una de las condiciones de ejercicio de la actividad aseguradora el sistema de buen gobierno financiero<sup>243</sup>. La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras y su desarrollo reglamentario<sup>244</sup>, regulan las exigencias de un eficaz sistema de gobierno<sup>245</sup>.

Las entidades aseguradoras y reaseguradoras deben disponer de un sistema eficaz de gobierno que garantice la gestión sana y prudente de la actividad y que sea proporcionado a su naturaleza, el volumen y la complejidad de sus operaciones (art. 65.1 LOSSEAR). El sistema de gobierno debe estar sujeto a una revisión interna periódica (art. 44.1 ROSSEAR).

Las entidades aseguradoras y reaseguradoras contarán con políticas escritas referidas a la gestión de riesgos, el control y la auditoría internos, y, en su caso, la externalización de funciones o actividades<sup>246</sup>, y se asegurarán de su aplicación. Las políticas escritas deben ser aprobadas por el órgano de administración de la entidad, se revisarán, al menos, anualmente y se

---

<sup>243</sup>Vid. TAPIA HERMIDA, A.J., "Los puntos críticos del proceso de implantación del sistema de gobierno en las entidades aseguradoras", *Revista Española de Seguros*, nº 167, 2016, p. 333. TAPIA HERMIDA, A.J., "El sistema de gobierno de las entidades aseguradoras", en AA.VV., *Estudios Jurídicos en memoria del profesor Emilio Beltrán. Liber Amicorum*, T. I, Valencia, 2015, pp. 990 y ss. y "Sistema de Gobierno de las Entidades Aseguradoras y Reaseguradoras", en AA.VV., *Supervisión en Seguros Privados. Hacia Solvencia II. Actas del Congreso de Ordenación y Supervisión en Seguros Privados*, dirs. V. Cuñat Edo, J. Bataller Grau, Colección Homenajes y Congresos, Valencia, 2013, pp. 283 y ss.

<sup>244</sup>Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

<sup>245</sup>En concreto, Capítulo I del Título III (arts. 65 a 67) de la LOSSEAR y Capítulo I del Título III (arts. 44 a 47) del ROSSEAR.

<sup>246</sup>Las entidades aseguradoras o reaseguradoras que externalicen parte de sus funciones seguirán respondiendo del cumplimiento de sus obligaciones. Las entidades pueden externalizar sus funciones o actividades operativas críticas o importantes salvo cuando se perjudique sensiblemente la calidad de su sistema de gobierno y se aumente indebidamente el riesgo operacional, menoscabe la capacidad de la DGS y FP para supervisar el cumplimiento de las obligaciones de la entidad o afecte al servicio continuo y satisfactorio para los tomadores de seguros. Con la finalidad de evitar estos efectos negativos, debe designarse dentro de la entidad a una persona responsable de la función o actividad externalizada, que cuente con la experiencia y conocimientos suficientes para comprobar la actuación de los proveedores de servicios. Previamente ha de comunicarse a la DGS y FP la externalización de funciones o actividades críticas o importantes, y cualquier cambio posterior significativo, que puede oponerse a las mismas, en el plazo de un mes desde la recepción de la comunicación (art. 67.1, 2, 3 y 4 LOSSEAR).



adaptarán a los cambios significativos en el sistema o área correspondiente (arts. 65.2 LOSSEAR y 44.2 ROSSEAR). Las cuatro funciones fundamentales del sistema de gobierno de las entidades aseguradoras son: la de gestión de riesgos, la de "*verificación del cumplimiento*", la de auditoría interna y la actuarial. El sistema de gobierno ha de establecer mecanismos eficaces que garanticen el cumplimiento de la normativa en relación con la gestión de riesgos, el control interno y de cumplimiento y la auditoría interna. El responsable último del sistema de gobierno es el órgano de administración de las entidades aseguradoras y reaseguradoras. La DGS y FP ha de verificar el sistema de gobierno de las entidades aseguradoras y reaseguradoras (art. 65 LOSSEAR).

Las entidades aseguradoras y reaseguradoras deben establecer, documentar y mantener un sistema de control interno apropiado a su organización, que debe constar de procedimientos administrativos y contables, de una estructura adecuada, de mecanismos apropiados de información a todos los niveles y de una *función de verificación del cumplimiento*. La *función de verificación del cumplimiento* ha de comprender el asesoramiento al órgano de administración acerca del cumplimiento de las disposiciones legales, reglamentarias y administrativas que afecten a la entidad y acerca del cumplimiento de su normativa interna; asimismo, comportará la evaluación del impacto de cualquier modificación del entorno legal en las operaciones de la entidad y la determinación y evaluación del riesgo de cumplimiento (art. 66.3 LOSSEAR).

Una de las obligaciones fundamentales de la función de cumplimiento, conlleva la realización de planes de verificación tendentes a conocer el grado de cumplimiento o incumplimiento de las disposiciones legales y normativas. Las conclusiones de esos trabajos deben ser trasladados a la dirección efectiva de la entidad para que, en todo caso, ésta sea plenamente conocedora de los riesgos legales que la entidad pudiera estar asumiendo. Uno de los pilares básicos es la información y el *reporting* a la dirección

efectiva, otro pilar es la prevención y la mitigación de los riesgos legales que pudieran existir.

Esta función vela por el cumplimiento de las disposiciones legales, reglamentarias y administrativas, así como por el cumplimiento de la normativa interna aplicable y por el mantenimiento de los más altos valores corporativos y éticos en toda la organización. Esta finalidad de la función de cumplimiento debe ponerse en consonancia con la necesaria articulación de una política y un plan de verificación del cumplimiento que incluya la evaluación de las medidas adoptadas para evitar cualquier incumplimiento de acuerdo con el artículo 270 del Reglamento Delegado<sup>247</sup>.

Es de destacar a efectos del cumplimiento normativo que la LOSSEAR recoge la figura de la "denuncia pública" por la cual se pone en conocimiento de la Administración hechos o situaciones que puedan ser constitutivos de infracciones de normas de supervisión de los seguros privados. Una vez que se reciba una denuncia, se ha de remitir al órgano competente para que realice las actuaciones que procedan, que pueden ser: a) acordar el archivo de la denuncia cuando se considere infundada, no se concreten o identifiquen suficientemente los hechos o las personas denunciadas; b) iniciar las actuaciones que procedan si existen indicios suficientes de veracidad en los hechos imputados y éstos son desconocidos para la Administración, en cuyo caso, la denuncia no formará parte del expediente administrativo. Al denunciante no se le ha de considerar interesado en las actuaciones administrativas que se inicien como consecuencia de la denuncia, ni se le ha de informar del resultado de las mismas, ni tampoco está legitimado para la interposición de recursos o reclamaciones en relación con los resultados de las correspondientes actuaciones (art. 211 LOSSEAR).

---

<sup>247</sup>FORO ASEGURADOR DEL CUMPLIMIENTO, *La Función de verificación del cumplimiento...*, ob. cit., p. 20.

#### **4.4 El cumplimiento normativo en la regulación de las empresas de servicios de inversión**

El texto refundido de la Ley del Mercado de Valores, aprobado por el Real Decreto Legislativo 4/2015, de 23 de octubre y demás normativa aplicable<sup>248</sup> disponen que las empresas de servicios de inversión y las restantes entidades que presten servicios de inversión deben ejercer su actividad con respecto a las normas de gobierno corporativo y los requisitos de organización interna.

Las empresas de servicios de inversión deben contar con sólidos procedimientos de gobierno corporativo, incluida una estructura organizativa clara, adecuada y proporcionada al carácter, escala y complejidad de sus actividades y con líneas de responsabilidad bien definidas, transparentes y coherentes, asimismo las restantes entidades que presten servicios de inversión, deben contar con una estructura organizativa clara, adecuada y proporcionada al carácter, escala y complejidad de los servicios de inversión que presten. El Consejo de Administración de las empresas de servicios de inversión debe definir un sistema de gobierno corporativo que garantice una gestión eficaz y prudente de la entidad, y que incluya el adecuado reparto de funciones en la organización y la prevención de conflictos de intereses (art. 185.1 y 5 TRLMV).

Entre los principios por los que se ha de regir el sistema de gobierno corporativo se encuentra el que el consejo de administración ha de garantizar el cumplimiento de la legislación aplicable<sup>249</sup> y la supervisión efectiva de la

---

<sup>248</sup>RD 217/2008, de 15 de febrero, sobre el régimen jurídico de las empresas de servicios de inversión y de las demás entidades que prestan servicios de inversión y por el que se modifica parcialmente el Reglamento de la Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva, aprobado por el Real Decreto 1309/2005, de 4 de noviembre, modificado por el RD 358/2015 de 8 de mayo.

<sup>249</sup>Vid. SERRANO SORDO, T., "Las normas de conducta en la prestación de servicios de inversión. El reglamento interno de conducta como instrumento para asegurar el cumplimiento normativo: especial referencia a las obligaciones en materia de abuso de mercado", en AA.VV., *Gobierno corporativo: La estructura del órgano de gobierno y la responsabilidad de los administradores*

alta dirección. El Consejo de Administración ha de vigilar la aplicación del sistema de gobierno corporativo y responderá de ella, para lo que debe controlar y evaluar periódicamente la eficacia del sistema y adoptar las medidas adecuadas para solventar sus deficiencias (art. 185.2.a, b y d y 3 TRLMV).

Las empresas de servicios de inversión y las restantes entidades que prestan servicios de inversión deben disponer de una unidad que garantice el desarrollo de la *función de cumplimiento normativo* bajo el principio de independencia con respecto a aquellas áreas o unidades que desarrollen las actividades de prestación de servicios de inversión sobre las que gire el ejercicio de aquella función. En este sentido, deben existir procedimientos y controles para garantizar que el personal cumple las decisiones adoptadas y las funciones encomendadas. La *función de cumplimiento normativo* debe controlar y evaluar regularmente la adecuación y eficacia de los procedimientos establecidos para la detección de riesgos, y las medidas adoptadas para hacer frente a posibles deficiencias, así como asistir y asesorar a las personas competentes responsables de la realización de los servicios de inversión para el cumplimiento de las funciones (art. 193.2.a TRLMV).

El Consejo de Administración es el responsable de los riesgos que asuma una empresa de servicios de inversión; por ello, a estos efectos, deben establecerse canales eficaces de información al Consejo de Administración sobre las políticas de gestión de riesgos de la empresa y todos los riesgos importantes a los que esta se enfrenta. El Consejo de Administración debe aprobar y revisar periódicamente las estrategias y políticas de asunción, gestión, supervisión y reducción de los riesgos a los que la empresa de servicios de inversión esté o pueda estar expuesta. Las empresas de servicios de inversión deben disponer de una unidad u órgano que asuma la

---

(Adaptado a la Ley 31/2014, de 3 de diciembre), dirs. Alfonso Martínez- Echevarria y García de Dueñas, Pamplona, 2015, pp. 687 y ss.

función de gestión de riesgos proporcional a la naturaleza, escala y complejidad de sus actividades, independientemente de las funciones operativas, que tenga autoridad, rango y recursos suficientes, así como el oportuno acceso al Consejo de Administración" (art. 194.1, 2.b y 3 TRLMV).

## IV. EL WHISTLEBLOWING

### 1. Antecedentes y desarrollo histórico del whistleblowing

La globalización, la internacionalización de las empresas, la cultura y conciencia en lo que respecta a la ética y a la integridad de las empresas, junto con el Gobierno Corporativo, la RSC y las políticas de prevención contra el fraude, la corrupción y el acoso, han llevado a desarrollar el principio de *whistleblowing*, regulando la figura y el estatuto del whistleblower<sup>250</sup>.

#### 1.1 Antecedentes

Los antecedentes más lejanos de la figura del delator pueden remontarse hasta la aparición de las primeras grandes civilizaciones. En la Antigua Roma, la figura estaba incluso institucionalizada y su estatuto jurídico definido. Existían delatores profesionales cuya tarea consistía en proporcionar información a los funcionarios del Erario público para facilitar los cobros de los tributos debidos. Su labor consistía en dar a conocer la *notitia criminis*, y probar la acusación para no ser castigado como calumniador y así recibir el *praemia delatorum*. Generalmente, les acompañaba mala fama, pero algunos autores los han descrito como guardianes de la aplicación de las leyes y actores del interés público.

Los fundamentos actuales de la configuración de estos mecanismos de denuncia se encuentran en EEUU a mediados del siglo XIX, dónde aparecen las claves para perfilar a los actuales whistleblowers<sup>251</sup>.

---

<sup>250</sup>HARTMAN, L./ ELM, D. /RADIN, T./ POPE, K.R., "Translating Corporate Culture around the World: A cross-cultural analysis of whistleblowing as an example of how to say and do the right thing" *Politeia: Corporate and Stakeholder Responsibility Theory and Practice*, Vol. Anno XXV Iss. Nº 93, 2009, pp. 255-260; CALLAHAN, E.S./ DWORKIN, T.M./ FORT, T.L. /SCHIPANI, C.A., "Integrating Trends in Whistleblowing and Corporate Governance: Promoting Organizational Effectiveness, Societal Responsibility, and Employee Empowerment", *American Business Law Journal*, vol. 40, 2002, pp. 177-215.

<sup>251</sup>GARCIA MORENO, B., Whistleblowing y canales institucionales de denuncia", en AA.VV., *Manual de cumplimiento penal en la empresa*, dir. A. Nieto Martín, Valencia, Tirant lo Blanch, 2015, p. 208.

## 1.2 Evolución de la concepción del whistleblower en EEUU

En Estados Unidos se pueden distinguir tres etapas en la concepción del whistleblower, caracterizadas por diferentes concepciones: como caza recompensas, como resistente y como herramienta del *compliance* en el sector privado. Tal y como se ha señalado es fundamental conocer la obra de M. BALLBÉ en la que se analizan las distintas transformaciones del sistema administrativo norteamericano, las grandes diferencias con el sistema europeo y el porqué de su evolución, donde ya entonces M. BALLBÉ apuntaba el efecto que dicha evolución ha tenido en el fenómeno del *compliance* en general y por ello en la figura del whistleblower en particular<sup>252</sup>.

### 1.2.1 El whistleblower como caza - recompensas

Los whistleblowers aparecen con fuerza en la escena norteamericana durante la Guerra de Secesión. Su configuración no surge de una ética empresarial o de la prevención de la criminalidad sino como una concepción propia de la privatización de las funciones de seguridad y policía en un país con escaso peso de las Administraciones Públicas. Hasta el siglo XX, el modelo estatal estadounidense giró en torno al individuo y la comunidad, rechazando la organización del Estado administrativo, que sí se desarrolló en Europa.

Las labores de policía fueron asumidas por los ciudadanos (*posse comitatus*, *sheriff*) y por investigadores privados y empresas de seguridad<sup>253</sup>. En este contexto, en el que era habitual recurrir a la colaboración ciudadana en la investigación y persecución de los delitos, el papel de los informantes resultó fundamental.

---

<sup>252</sup>BALLBÉ, M./ MARTÍNEZ, R., "Law and Globalization: Between the United States and Europe", ob. Cit pp. 145 y ss.

<sup>253</sup>Para un análisis en profundidad sobre las labores de policía asumidas por los ciudadanos en EEUU y las perversiones de dicho sistema resulta fundamental la obra de BALLBÉ, M. "El futuro del derecho administrativo en la globalización: entre la americanización y la europeización", ob. cit. pp 222.

La False Claims Act de 1863 (FCA) supuso el impulso más significativo de la figura del whistleblower. La Guerra Civil norteamericana estuvo marcada por el fraude: los contratistas suministradores del ejército proporcionaban caballos enfermos, munición y armas defectuosas y provisiones en mal estado. La FCA preveía la posibilidad de que el ciudadano que tuviera conocimiento de la violación de esta ley interpusiera la denuncia en nombre del Gobierno, lo que podría reportarle una recompensa de entre el 15 y el 25% de la cantidad recuperada al final del litigio. Los whistleblowers, que podrían ser calificados de caza-recompensas, se convirtieron así en colaboradores retribuidos del Gobierno Federal, que hicieron posible la recuperación de grandes cantidades de dinero gracias a las informaciones que revelaron.

### **1.2.2 El whistleblower como *ethical resister***

En la década de los 60, como consecuencia de determinados factores sociales y políticos, se produjo un cambio en la concepción de los whistleblowers, hasta entonces movidos por el interés propio, que comienzan a intervenir desinteresadamente, impulsados por convicciones morales y de conciencia social. Y lo hacen sabiendo que no sólo no obtendrán recompensa por ello, sino que su actuación podrá incluso reportarles importantes consecuencias negativas.

Uno de los principales motores de cambio fue la oposición de las grandes compañías a las nuevas regulaciones que incrementaban considerablemente la intervención pública en el desarrollo de la actividad empresarial. El crecimiento -en tamaño, riqueza e influencia- de las grandes compañías tras la II Guerra Mundial dio lugar a un importante movimiento social que impulsó, como contrapartida, la intervención federal para la protección de trabajadores,



consumidores y medio ambiente frente a los posibles abusos de las empresas<sup>254</sup>.

La materialización de estas reivindicaciones, mediante la aprobación de extensas regulaciones para el sector privado y la creación de numerosas agencias administrativas, marcó las relaciones entre el Gobierno y las empresas. Muchas de las prácticas empresariales tradicionales eran ilegales de acuerdo con la nueva normativa y algunas entidades se mostraron incapaces de asumir los costes necesarios para cumplir con las nuevas obligaciones impuestas en materia de seguridad y medio ambiente. En este contexto, muchas corporaciones prefirieron continuar con su actividad tal y como la habían desarrollado hasta entonces, tratando de mantener ocultas las irregularidades y asumiendo las posibles sanciones que derivaran de ello. A pesar de la inobservancia generalizada de estas normas administrativas, muy pocas fueron las empresas efectivamente sancionadas. A ello ayudó significativamente la relajada supervisión que se ejerció por los cuerpos administrativos, muchas veces integrados por funcionarios fuertemente vinculados a alguna entidad privada.

La incapacidad demostrada por el Gobierno y las empresas para controlar los riesgos derivados de los avances tecnológicos, y la generalizada desconfianza en la integridad de los funcionarios, que creció debido a la Guerra de Vietnam y al escándalo del Watergate, contribuyeron también de forma decisiva a este cambio de tendencia.

En un contexto como éste, marcado por la corrupción y la falta de compromiso con el interés público tanto de la Administración como de las grandes empresas, los whistleblowers constituyeron una nueva forma de “resistencia ética”. En este periodo, los principales avances legislativos en materia de *whistleblowing* se desarrollaron, a partir de la reforma de la Civil

---

<sup>254</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., pp. 209-213

Service Act en 1978, en torno a la protección de los funcionarios que denunciaran comportamientos indebidos en la Administración.

### **1.2.3 La era compliance: el whistleblower en el sector privado**

En las últimas décadas, el rol de los whistleblowers se ha extendido del ámbito público al privado, como instrumentos al servicio de los intereses de las empresas.

Entre las medidas de prevención y control de los “*compliance programs*”, ha resultado especialmente importante la implementación de canales de denuncia o diálogo con los miembros de la organización, tanto para realizar consultas como para denunciar los posibles comportamientos indebidos. Así se desprende de las *guidelines*, recomendaciones y modelos de gestión establecidos tanto por los legisladores como por instituciones y organizaciones internacionales<sup>255</sup>.

Para la expansión de estos instrumentos en el sector privado ha resultado fundamental la adopción de la citada SOX de 2002, que nació como respuesta a los grandes escándalos financieros de la década anterior (Enron, Worldcom...) y que como hemos visto introdujo importantes cambios en las prácticas financieras y en la gobernanza corporativa, aspirando a dotar a las entidades de mayor transparencia y a los inversores de una protección más eficaz.

En lo que a los canales de denuncia se refiere, además de prever un completo sistema de protección del whistleblower, la SOX de 2002 exigía a las sociedades estadounidenses que cotizaran en bolsa, a sus filiales y también a las sociedades no estadounidenses que cotizaran en alguno de los mercados de valores de EEUU, que establecieran en su comité de auditoría procedimientos (i) para la recepción, custodia y tratamiento de quejas recibidas de los auditores en relación con la contabilidad, controles contables

---

<sup>255</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 210.

internos o cuestiones de auditoría; y (ii) para las denuncias confidenciales y anónimas que los empleados pudieran plantear en relación a prácticas contables o de auditoría cuestionables (Sección 301-4). En la práctica, estos preceptos supusieron la rápida expansión de los canales de denuncia: la mayoría de las grandes empresas, al cotizar en los mercados de valores estadounidenses, debían dotarse de uno para cumplir con las disposiciones de la ley<sup>256</sup>.

En la actualidad, además de la legislación federal, todos los Estados norteamericanos han aprobado ya leyes de protección de los whistleblowers y muchos de ellos también de fomento de la delación. Y es que ante el éxito de la FCA —especialmente en cuanto a recaudación de fondos—, la mayoría de los Estados americanos iniciaron la elaboración de sucedáneos de la ley federal. Más de un tercio de los Estados y el Distrito de Columbia han incorporado ya a su ordenamiento una False Claim Act.

Desde mediados del siglo XIX los ordenamientos jurídicos estadounidenses incentivan los actos de delación por diferentes medios, como el ofrecimiento de protección ante represalias o las recompensas económicas para el informante<sup>257</sup>. Estos incentivos se añaden a las amplias posibilidades con las que los jueces y fiscales cuentan para llegar a acuerdos con aquellos que, habiendo intervenido en hechos delictivos, están dispuestos a delatar a otros responsables.

---

<sup>256</sup>SOX. Section 301 (4): "COMPLAINTS. *Each audit committee shall establish procedures for (A) the receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters; and (B) the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters*".

LOMAS, P. / KRAMER, J. D., *Corporate Internal Investigations. An International Guide*, 2ª ed., 2013, pp. 7, 47-181, 323-326.

HARTMAN, L./ ELM, D. /RADIN, T./ POPE, K.R., "Translating Corporate Culture...", ob. cit., pp. 255-266.

<sup>257</sup>Como hemos señalado anteriormente, el primer antecedente de la protección jurídica de los whistleblowers, suele situarse en la False Claims Act de 1863 que preveía recompensas económicas para los informantes. Más referencias en QUIGLEY, S. K., "Whistleblower Tug-Of-War: Corporate attempts to secure internal reporting procedures in the: face of external monetary incentives provided by the Dodd-Frank act", *Santa Clara Law Review*, nº 52, 2012, p. 260.

Como ya hemos visto, particularmente significativas han sido las estadounidenses *Sentencing Guidelines* que propone a los jueces federales criterios para lograr una doctrina judicial uniforme, y que incluye los canales de denuncia entre los contenidos que debe tener un *effective compliance program* para que pueda operar como atenuante de la responsabilidad de la entidad o, en determinadas circunstancias, suspender la ejecución de la pena<sup>258</sup>. Las Guidelines establecen, entre otras exigencias, para considerar que el programa sea efectivo en la prevención y detección del delito el que la empresa<sup>259</sup> “*haya dado pasos razonables para establecer y dar a conocer un sistema, que puede incluir mecanismos que permitan el anonimato y la confidencialidad, por medio del cual los empleados y agentes de la compañía puedan denunciar o solicitar orientación acerca de conductas delictivas posibles o efectivas sin temor de represalias*”<sup>260</sup>.

El *United States Attorney's Manual*<sup>261</sup> confiere una clara trascendencia jurídico-penal al hecho de contar con estos procedimientos. Este texto recoge los criterios que el Departamento de Justicia elabora como pauta para los fiscales en el momento de formular acusaciones o alcanzar acuerdos con las defensas<sup>262</sup>. Entre los requisitos que los fiscales han de tener en cuenta en caso de posibles infracciones de la *Foreign Corrupt Practices Act* se incluye el que la empresa cuente con un “*sistema de denuncia que incluya una “línea de ayuda” para directivos, ejecutivos, empleados, agentes y terceras partes*”

---

<sup>258</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 210.

<sup>259</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 163-165.

<sup>260</sup>Para las concretas referencias, cfr. POLLACK, B. J., "Time to stop living vicariously: a better approach to corporate criminal liability", *American Criminal Law Review*, nº 46, pp. 1396-198. Ver también ALONSO GALLO, J., "Los programas de cumplimiento", AA.VV., *Estudios sobre las reformas del Código Penal, operadas por las LO 5/2010 de 22 de junio, y 3/2011, de 28 de enero*, dir. J. Díaz-Maroto y Villarejo, Madrid, 2011, pp. 159 y ss.

<sup>261</sup><https://www.justice.gov/usam/united-states-attorneys-manual>

<sup>262</sup>POLLACK, B. J., "Time to stop...", ob. cit., pp. 1398 y ss.

para informar de sospechas de violaciones del código de conducta o de infracciones penales"<sup>263</sup>.

### **1.3 La importancia del whistleblowing en los escándalos financieros más importantes del último siglo**

Los delitos en la empresa y la corrupción entre agentes privados y el Estado y entre particulares han sido frecuentes desde finales del siglo XX hasta el momento actual que vienen siendo una tónica habitual.

A principios del siglo XXI han ocurrido numerosos escándalos financieros que han conmocionado el mundo y han hecho reflexionar a los políticos de ambos lados del Atlántico. Especialmente importantes por su gravedad han sido los casos Enron y WorldCom y años más tarde los casos Lehman Brothers, Siemens, UBS y AIG<sup>264</sup>. Estos escándalos demostraron la necesidad de revisar la efectividad de los estándares de contabilidad, la regulación de la auditoría, y los principios de ética y buen gobierno de las compañías y demostraron la importancia de los whistleblowers.<sup>265</sup>

Y es que en la mayoría de ellos, los whistleblowers han jugado un papel fundamental en su resolución<sup>266</sup>. A continuación haremos un breve repaso de los casos más flagrantes de corrupción del último siglo los cuales fueron descubiertos por un denunciante o whistleblower.

---

<sup>263</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. p. 165.

<sup>264</sup>TARANTINO, A., *Governance, Risk, and Compliance Handbook*. Wiley. 2008, pp. 113-116.

AGRAWAL, A./ CHADHA, S., "Corporate Governance and accounting scandals", *Journal of Law and Economics*, vol. XLVIII, 2005, pp. 371 y ss; COFFEE, J. F., *Gatekeepers. The professions and corporate governance*. Oxford, 2006, pp. 4, 11, 15, 16, 18, 24; SCHWARTZ, M. / WATKINS, S. *Power Failure: The Inside Story of the Collapse of Enron*, New York, 2003; COFFEE, J. C., Jr, "What Caused Enron - A Capsule Social and Economic History of the 1990s", *Cornell Law Review*, vol. 89, Issue, 2004, pp. 268 y ss. SOLOMON, J./ SOLOMON, A., *Corporate Governance and accountability*, Londres, 2004, pp. 31-35.

<sup>265</sup>AYALA, A. /IBARGUEN, G. S. "A Market Proposal for Auditing the Financial Statements of Public Companies" extraído de <http://www.webcitation.org/5tZ0THjI8>

<sup>266</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1223. Los norteamericanos han celebrado el 150 aniversario de la citada FCA, y nadie duda de que la ley mencionada ha sido el instrumento más eficaz en la lucha contra el fraude, y que los whistleblowers han contribuido muy positivamente a la sociedad norteamericana

## A) Enron

Uno de los mayores escándalos financieros, revelado en octubre de 2001, fue el caso de Enron que condujo a la quiebra de una de las empresas gasistas más importantes, y a la disolución de Arthur Andersen, una de las cinco sociedades de auditoría y contabilidad más grandes del mundo.<sup>267</sup>

Sherron Watkins, empleada en el departamento financiero de Enron, reportó al presidente y al director financiero, sobre la existencia de irregularidades en la contabilidad y finanzas de la empresa. La dirección de la empresa decidió cambiarla de puesto de trabajo, en lugar de llevar a cabo las necesarias investigaciones que mitigaran el riesgo, así como depurar responsabilidades<sup>268</sup>. A su vez, en el descubrimiento del fraude de Enron tuvo un importante papel la periodista de la revista Fortune Bethany McLean, publicando el famoso artículo “¿Exactamente cómo gana dinero Enron?”<sup>269</sup>.

Unos activos ascendentes a \$63,4 mil millones convirtieron la quiebra de Enron en la mayor bancarrota corporativa en la historia de Estados Unidos hasta la quiebra de WorldCom el año siguiente<sup>270</sup>.

## B) WorldCom

Cynthia Cooper, junto con parte de su equipo, vicepresidenta en el departamento de auditoría de WorldCom, llevó a cabo investigaciones internas, por las que descubrieron que la empresa estaba llevando a cabo prácticas ilegales. Ante la pasividad de la dirección, Cooper decidió trasladar

---

<sup>267</sup>BRATTON, W.W., "Enron and the Dark Side of Shareholder Value", *Tulane Law Review*, May 2002, Forthcoming. Extraído de <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1508&context=facpub>

<sup>268</sup>CLARK, C., "Los cambios en el Gobierno Corporativo tras la Sarbanes-Oxley Act: una historia con moraleja también para el legislador", en *Gobierno Corporativo y crisis empresariales*. II seminario Harvard-Complutense de Derecho mercantil, edit. Marcial Pons, Madrid, 2006, pp. 16-18.

<sup>269</sup>MCLEAN, B. / ELKIND, P., *The smartest guys in the room. The amazing rise and scandals fall of Enron*, New York, 2004.

<sup>270</sup>BENSTON, G.J., "The Quality of Corporate Financial Statements and Their Auditors before and after Enron", *Policiy analysis*, Noviembre 2003. Extraído de <http://www.webcitation.org/5tZ00qlbE>

sus sospechas al consejo de administración, sin que éste reaccionara, lo que finalmente concluiría con el colapso y la desaparición de la empresa. Este hecho provocó que se empezara a cuestionar, entre otros muchos aspectos del Buen Gobierno en la empresa, lo que respecta a la independencia de los miembros de los comités de la empresa, especialmente el comité de auditoría<sup>271</sup>.

Lo que en algunos países podría haber sido considerado como un acto traidor, y a las denunciantes como traidoras o chivatas, en Estados Unidos Coopers y el agente del FBI Coleen Rowley fueron considerados por la revista TIME personajes del año 2002<sup>272</sup>.

La caída de Enron provocó que el Congreso y el Senado de los EE.UU., a través del senador demócrata Paul Sarbanes y del congresista republicano Michael G. Oxley, aprobaran la citada ley SOX. La SOX se caracteriza por tener un carácter eminentemente imperativo<sup>273</sup>. Como hemos visto, esta ley introdujo importantes cambios en el sistema financiero de los EEUU; un endurecimiento de las auditorías de las empresas y las empresas auditoras, obligándolas a que los auditores fueran independientes del management; una rotación de los auditores después de un cierto tiempo; y endureció el régimen de responsabilidad del Consejero Delegado (CEO) y del director financiero (CFO), teniendo ambos que certificar las cuentas de la sociedad, castigando el incumplimiento de esta certificación hasta con 20 años de prisión<sup>274</sup>. Con

---

<sup>271</sup>DEVINE, T. / MAASSARANI, T.F., *The Corporate Whistleblower's Survival Guide*, Berret-Koehler, 2011, pp. 1-4.

<sup>272</sup>MICELI, M./ NEAR, J./ POLLEX, J./ MOREHEAD, T., *Whistle-blowing in organization*; Routledge/Psychpress. New York-London, 2008, pp. 1-4, 6; KELLY, J., "The Year of the Whistle-Blowers", *Time*, nº 30, 2002.

<sup>273</sup>MOBERLY, R., "Sarbanes-Oxley's Structural Model to Encourage Corporate Whistleblowers", *Byu Law Review*, 2006, pp. 1107-1180.

<sup>274</sup>CHAMBERS, A., *Corporate Governance Handbook*, IDDAS, 5ª ed., 2012, pp. 547-559.

esta ley se pretendió erradicar fraudes como los ocurridos<sup>275</sup>, intentando evitar crisis financieras y recobrar la confianza de los inversores<sup>276</sup>.

La historia nos ha demostrado que la SOX no asustó a algunos empresarios, y especialmente a banqueros que han seguido cometiendo hechos ilícitos y provocando la mayor crisis financiera de los últimos 80 años, trasladada al cine con películas y reportajes como Insider e Inside Job<sup>277</sup>.

### C) Lehman Brothers

La caída de Lehman Brothers no fue sólo un escándalo financiero, sino que provocó el mayor desastre económico y financiero a nivel mundial desde la gran depresión.

Mientras la entidad recibía de las agencias de rating casi la máxima calificación crediticia, el vicepresidente del banco, Matthew Lee, envió una carta en el mes de mayo del año 2008 al management, en la que comunicaba y describía las distintas irregularidades contables que estaban ocurriendo en el banco. El banco ordenó a su auditora externa Ernst & Young que investigara los hechos. Matthew Lee se puso en contacto con la auditora explicándole las deficiencias e irregularidades existentes en el sistema contable del banco, manifestando la auditora que las denuncias de Matthew Lee no habían sido suficientemente probadas. En el mes de junio, Matthew Lee fue despedido del banco<sup>278</sup>.

---

<sup>275</sup>Enron, WorldCom, Tyco, Dysney, Parmalat, BCCI, etc.

<sup>276</sup>Véase resolución judicial de los tribunales de Delaware al respecto: Caso Oracle Corp. Derivative Litigation, 824 A 2d 917. Caso Walt Disney Company Derivative Litigation, 825 A d 275. Del Ch. 2003, respecto a la indemnización por el despido de Michael Ovita, máximo ejecutivo de la compañía. La agencia más influyente e importante es la Institucional Shareholders Services (ISS, junto con la Governance Metrics Internacional (GMI), The Corporate Library, Moody's y Standard & Poor's.

<sup>277</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1220.

<sup>278</sup>DEVINE, T. / MAASSARANI, T.F., *The Corporate Whistleblower's...*, ob. cit., CLARK, A., "Lehman whistleblower lost his job weeks after raising alarm". *The Guardian*. March 16, 2010, Extraído de <https://www.theguardian.com/business/2010/mar/16/lehman-whistleblower-auditors-matthew-lee> y MCDONALD, L. / ROBINSON, P., *A Colossal Failure of Common Sense: The Inside Story of the Collapse of Lehman Brothers*. Ebury press. 2009.



Efectivamente, Lehman Brothers sucumbió, y con su colapso convirtió el 14 de septiembre de 2008 en el día en el que el sistema bancario de EE.UU cambió su forma de funcionar. Su bancarrota, con un pasivo de 613.000 millones de dólares (unos 430.000 millones de euros) y unos activos teóricamente valorados en 639.000 millones de dólares (pero cuyo valor de liquidación resultaba mucho menor) se convirtió en la mayor de la historia, seis veces superior a la de Worldcom en 2002 y 10 veces mayor que la de Enron en 2001<sup>279</sup>.

#### D) Madoff

En el año 2008, entró en escena Bernie Madoff, persona con excelente reputación en el mundo de las finanzas. La bola de nieve creada por él fue tan grande que ni la promulgación de la SOX pudo evitar que continuara con sus prácticas dando lugar a un fraude multimillonario.

A diferencia del caso Enron, en donde fueron una periodista financiera, Bethany McLean, y una empleada del departamento financiero de la empresa, Sharon Watkins, las que descubrieron el fraude, en el caso Madoff lo descubrió una persona sencilla y estudiosa, matemático de profesión, llamado Harry Markopoulus, quien trabajaba para la competencia de Madoff en el año 1999<sup>280</sup>.

Harry Markopoulus fue ignorado por la SEC de Boston y Nueva York, por el diario Wall Street Journal y, por la Fiscalía General de los EE.UU. Ante esta circunstancia, la prensa y muchos autores se han cuestionado el porqué la SEC, la fiscalía y el periódico económico más importante de los EE.UU. no

---

<sup>279</sup>[http://elpais.com/diario/2008/09/16/economia/1221516004\\_850215.html](http://elpais.com/diario/2008/09/16/economia/1221516004_850215.html)

<sup>280</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1221.

descubrieron algo tan evidente y fácil de entender como la comisión de una estafa piramidal al estilo Ponzi<sup>281</sup>.

Muchos autores y periodistas han apuntado tres datos significativos: la familia del ex Fiscal General del Estado Eliot Splitter, a través del holding Splitter trust, tenía invertida gran cantidad de dinero en la empresa de Madoff, y la pareja sentimental de la hija de Madoff trabajaba en la SEC cuando se estaba produciendo el fraude. La SEC permitía que empresas como la de Madoff fueran auditadas por una auditora compuesta por tres miembros, en este caso uno de sus tres miembros tenía 79 años de edad y pasaba la mayor parte de su tiempo pescando en Florida<sup>282</sup>.

En el caso Madoff, España fue el tercer país más afectado por la actuación fraudulenta del señor Madoff, llevando a la quiebra a numerosas gestoras de fondos y haciendo perder mucho dinero a personas que confiaban en el sistema financiero mundial.

## E) UBS

Con posterioridad al caso Madoff, y en plena crisis económica, surgió la denuncia de un ex banquero del mayor banco suizo UBS instalado en Estados Unidos, Bradley Birkenfeld que provocó que el país con más cuentas bancarias no regularizadas en el mundo cambiara su normativa.

Bradley Birkenfeld en octubre de 2005 renunció a su puesto en UBS y apenas un par de meses después acudió al Departamento de Justicia Americano informando sobre las prácticas ilegales del banco suizo. El 7 de mayo de 2008 Birkenfeld fue detenido y acusado de conspiración cuando se preparaba para volar a Suiza. Debe recordarse que para disfrutar de los derechos de un informador, Birkenfeld tenía que proporcionar “revelaciones completas y

---

<sup>281</sup>ZUCKOFF, M., *Ponzi's Scheme: The True Story of a Financial Legend*, Random House: New York, 2005.

<sup>282</sup>MARKOPOLOS, H., *No one would listen: A True Financial Thriller*, Wiley, 2010.

veraces”, y en su caso Birkenfeld ocultó ciertas información de algunos clientes, por tanto no tenía derecho a dicho estatus. En el juicio, el banquero expatriado reconoció sólo el cargo de conspiración y el fiscal admitió que la trama corrupta de UBS no habría podido salir a la luz sin Birkenfeld.<sup>283</sup> Una paradoja que terminó cuando salió de la cárcel después de una fuerte presión por parte de organizaciones como el National Whistleblowers Center, que alegaban que su encarcelamiento creaba un precedente que podía provocar que otros informadores no se atreviesen a revelar lo que saben.

La recompensa que Birkenfeld recibió es la más cuantiosa de la historia de EE.UU: 104 millones de los más de 400 recuperados de UBS por Hacienda, que le felicitó por su “colaboración excepcional”. Gracias a él, consiguieron firmar con UBS un acuerdo de 780 millones y el nombre de 5.000 clientes estadounidenses sospechosos de evasión fiscal para evitar el juicio

La denuncia de Birkenfeld provocó que los Presidentes y Jefes de Estado Obama, Brown, Merkel y Sarkozy se reunieran para tratar un tema tan delicado como el de la banca suiza y las cuentas no declaradas, firmándose, después de un año de negociaciones, dos acuerdos –Acuerdo Rubik– entre los gobiernos de Alemania e Inglaterra con las autoridades suizas por el que Suiza dejaría de ser un lugar en donde personas de gran parte del mundo depositaran su dinero o parte de él en sus bancos sin pagar los correspondientes impuestos en sus países de residencia fiscal. En España se aprobó una amnistía fiscal, que junto a otras medidas legislativas daba opción a las personas que tenían dinero en el extranjero no declarado a regularizar su situación tributaria irregular<sup>284</sup>. Dicha medida ha sido declarada inconstitucional por el TC en Sentencia de fecha 8 de junio de 2017.

---

<sup>283</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., pp. 1222-1223.

<sup>284</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1223.

## F) Olympus

Michael Woodford, ejecutivo de Olympus, al descubrir los distintos fraudes contables que se estaban cometiendo en la empresa, decidió denunciar los hechos a las autoridades competentes. En el año 2011 los accionistas de la empresa exigieron la renuncia de todo el Consejo en bloque. Los accionistas al conocer el estado financiero de la sociedad, obligaron al consejo a que presentara su dimisión.

El expresidente de Olympus, Tsuyoshi Kikukawa, fue demandado por la propia compañía en el mes de enero de 2012 junto con 18 altos cargos, por ser considerados los responsables de un fraude contable de al menos 117.700 millones de yenes (unos 1.150 millones de euros) provocando que las acciones perdieran en torno a la mitad de su valor. La compañía Olympus reconoció haber falsificado sus cuentas para encubrir grandes pérdidas en inversiones financieras.

El fraude fue descubierto poco después de que el fabricante de cámaras y productos de óptica despidiese al director ejecutivo Michael Woodford cuando éste cuestionó una serie de pagos dudosos entre sus ejecutivos, en concreto, los 687 millones de dólares que Olympus pagó en concepto de comisiones a los consejeros financieros en el proceso de adquisición de la compañía británica de equipos médicos Gyrus. Se descubrió que la firma había desviado cantidades millonarias a través de adquisiciones artificiales para ocultar pérdidas a los inversores y reguladores.

## G) Amgen

El caso de las empresas Amgen fue destapado por el whistleblower Kassie Westmoreland contra la empresa de biotecnología más grande de los EE.UU., Amgen Inc.

La compañía había faltado a la verdad entre abril de 2004 y mayo de 2007, efectuando públicamente falsas declaraciones y omitiendo información relevante respecto a las previsiones sobre la eficacia y comercialización de dos de sus fármacos contra la anemia, “Aranesp” y “Epogen”, habiendo modificado artificialmente al alza el precio de las acciones, lo que posteriormente, una vez que se hizo público, conllevó grandes pérdidas a los inversores.

A fin de incrementar las ventas, Amgen vendió ilegalmente los medicamentos con la intención de que se usaran con dosis que la Administración de Medicamentos y Alimentos de EE.UU (FDA) había rechazado y se destinaran para tratamientos que no habían sido aprobados.

Finalmente, en diciembre de 2012 la compañía se declaró culpable y aceptó pagar ante un tribunal federal de Brooklyn una multa de 762 millones de dólares por los cargos criminales y civiles derivados de la introducción en el mercado, la promoción y la venta ilegal de los medicamentos.

El acuerdo supuso una de las mayores sanciones por fraude a una compañía de biotecnología en la historia de EE.UU. El fiscal federal Marshall Miller señaló que *“en lugar de trabajar para alargar y mejorar la vida humana, Amgen buscó ilegalmente los beneficios empresariales mientras ponía en peligro la seguridad de consumidores vulnerables que sufrían enfermedades”*.

#### H) Well Care

Gracias a la denuncia de un whistleblower, la empresa Well Care llegó en el mes de abril del año 2012 a un acuerdo con el gobierno estadounidense abonando la cantidad de 137,50 millones de dólares.

En octubre de 2007, el FBI intervino sus instalaciones en Florida y se inició una investigación federal de seis años. Se acusó a la compañía de estafar

dinero a programas del Medicaid, lo que permitió a la empresa mantener millones de dólares en fondos subsidiarios.

Well Care estaba obligada por ley a gastar un 80% del dinero que recibía del Estado para la prestación de los servicios de salud mental y destinarlos directamente en los pacientes. El 20% restante podía ir destinado a gastos administrativos. La compañía canalizó millones de dólares a través de una filial encubriendo los gastos con el objetivo de evitar devolver el dinero no utilizado por importe de 40 millones de dólares.

#### l) Volkswagen

En septiembre de 2015 salió a la luz que la compañía Volkswagen había trucado sus coches para evitar los límites a las emisiones. El mayor fabricante de automóviles del mundo llegó a reconocer que había instalado un software con el fin de eludir los controles medioambientales en 11 millones de vehículos diésel de todo el mundo.

El fraude se destapó después de que la Agencia Medioambiental Estadounidense (EPA) acusará a Volkswagen de haber hecho trampa al instalar en 482.000 vehículos de EE.UU de manera deliberada un programa informático especialmente diseñado para evitar los límites a las emisiones. El escándalo le reportó a Volkswagen unas pérdidas diarias de 23,8% en la Bolsa. En EE.UU se le condenó a pagar una multa al Departamento de Justicia de 4.300 millones de dólares.

En el año 2015 la compañía registró las mayores pérdidas de su historia en 1.600 millones de euros (1.800 millones de dólares).

## 2. El whistleblowing en el Derecho comparado

### 2.1 El whistleblowing en el Derecho Internacional

El fenómeno whistleblowing en general, y los canales de denuncia corporativos en particular, no han recibido especial atención por parte de los legisladores nacionales. En general, el desarrollo funcional de los canales de denuncia no ha ido acompañado, en la mayoría de los casos, del correspondiente desarrollo legislativo. Con excepción del ámbito anglosajón, la regulación del whistleblowing ha sido parcial y sectorial y casi nunca abordada de manera específica sino de forma tangencial<sup>285</sup>.

La normativa internacional, las recomendaciones y demás instrumentos de soft law elaborados por organizaciones internacionales y agencias de protección de datos y también, aunque en menor medida, las regulaciones nacionales sobre whistleblowing han ofrecido las pautas para diseñar los canales de denuncia corporativos. Las directrices contenidas en estos documentos son, en la mayoría de los casos, coincidentes y complementarias, lo que ha facilitado en gran medida la labor de las empresas. Este grado de estandarización, que aparece en materia de whistleblowing y en general en todos los aspectos del *compliance*, constituye la base de las propuestas para la implantación de los canales de denuncia que se contienen en este trabajo<sup>286</sup>.

En este sistema internacional ocupa un lugar central, la citada Convención de Naciones Unidas contra la corrupción, de 31 de octubre de 2003, por haber avanzado significativamente en el desarrollo y protección de la figura del whistleblower, y por la amplia implantación que ha logrado al tratarse de un instrumento de *hard law* y de carácter universal que cuenta con un elevado número de ratificaciones.

---

<sup>285</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 212.

<sup>286</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 212.

A nivel regional, pueden destacarse las disposiciones de la Convención interamericana contra la corrupción de 1996<sup>287</sup> (art. III, 8), la Convención de la Unión Africana para prevenir y combatir la corrupción de 2003<sup>288</sup> (arts. 5.5-7) y el Protocolo contra la corrupción de la Southern African Development Community de 2001 (art. 4.1).

En Europa los instrumentos más importantes en esta materia son la Convención penal sobre la corrupción, de 27 de enero de 1999 (art. 21) y la Convención civil sobre la corrupción, de 4 de noviembre de 1999 (art. 9)<sup>289</sup>.

Los legisladores nacionales se han mostrado menos receptivos a regular específicamente esta institución. Así alrededor de una decena de países, casi todos del ámbito anglosajón, han aprobado normas sobre whistleblowing abordando su regulación sólo de forma parcial<sup>290</sup>.

La implantación de procedimientos internos de denuncia progresivamente se ha extendido a otros países. Este efecto expansivo se ha producido por dos razones: en primer lugar, por la presión ejercida desde los Estados Unidos sobre las empresas multinacionales, que han extendido sus programas de

---

<sup>287</sup>[http://www.oas.org/juridico/spanish/faq\\_ac\\_sp.htm](http://www.oas.org/juridico/spanish/faq_ac_sp.htm). Esta Convención, que fue el primer instrumento jurídico internacional en este campo, menciona expresamente entre sus fundamentos el reconocimiento de la trascendencia internacional de la corrupción y la necesidad de contar con un instrumento de tal carácter que promueva y facilite la cooperación entre los países para combatirla, y consecuentemente con esta motivación, se fijó dos propósitos: El primero, promover y fortalecer el desarrollo, por cada uno de los Estados Parte, de los mecanismos necesarios para prevenir, detectar, sancionar y erradicar la corrupción. Y, el segundo, promover, facilitar y regular la cooperación entre los Estados Parte a fin de asegurar la eficacia de las medidas y acciones para prevenir, detectar, sancionar y erradicar los actos de corrupción en el ejercicio de las funciones públicas y los actos de corrupción específicamente vinculados con tal ejercicio.

La CICC establece obligaciones vinculantes dentro del marco del derecho internacional e identifica los actos de corrupción a los que se aplicará, así como principios para combatir eficazmente la corrupción. Subraya la importancia de las medidas para prevenirla; aborda el desarrollo institucional y la aplicación efectiva de las medidas que se adopten para enfrentarla; exige la tipificación de ciertas conductas corruptas específicas; y contiene disposiciones sobre extradición, incautación de activos, asistencia jurídica recíproca y asistencia técnica en casos de corrupción que ocurran en otros Estados Parte o que los afecten.

<sup>288</sup><http://www.opengovguide.com/standards-and-guidance/african-unions-convention-on-preventing-and-combating-corruption/?lang=es>

<sup>289</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 212.

<sup>290</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 213.



prevención del delito a todas las filiales situadas en otros países; y, en segundo lugar, por la elaboración de convenios y otros instrumentos normativos a escala internacional. La expansión de los procedimientos internos de denuncia, se ha visto favorecida por la OCDE que en sus Principios del Gobierno Corporativo de 2004 incluyó entre sus recomendaciones un apartado 11 dedicado a los procedimientos de denuncia en el que se manifestaba que *“las partes interesadas, incluidos los empleados individuales y sus órganos representativos, deberán poder manifestar libremente sus preocupaciones en relación con posibles prácticas ilegales o no éticas al Consejo, y sus derechos no deberán quedar comprometidos por realizar este tipo de manifestaciones”*. A tal efecto este texto aconsejaba *“el establecimiento de procedimientos y puertos seguros”* para recoger las denuncias relativas a comportamientos ilegales o poco éticos presentadas por los empleados ya sea personalmente o a través de sus órganos representativos, y por terceros que no pertenezcan a la sociedad, añadiendo que tal previsión *“redunda en beneficio de la propia empresa y de sus partes interesadas”*<sup>291</sup>.

## **2.2 El whistleblowing en Estados Unidos**

### **2.2.1 Breve repaso a la legislación Estadounidense**

Cabe recordar que la primera Enmienda de la Constitución de los Estados Unidos de América ya estableció la protección de aquellos empleados que denunciaran conductas contrarias a la primera enmienda de los derechos de los trabajadores federales. La primera Enmienda, así como la Ley de derechos civiles de 1871, permitía a los trabajadores del gobierno federal reclamar por orden judicial una compensación económica si eran discriminados al llevar a cabo una denuncia.

---

<sup>291</sup>Principios de Gobierno Corporativo de la OCDE, 2004 (extraído de <http://www.oecd.org/dataoecd/47/25/37191543.pdf>, pp. 17-48). Otro texto relevante de la OCDE es la Good Practice Guidance on Internal Controls, Ethics, and Compliance, de 2010 (extraído de <http://www.oecd.org/investment/briberyininternationalbusiness/anti-briberyconvention/44884389.pdf>), que en su apartado 11 alude a los procedimientos de denuncia.

En Estados Unidos existen numerosas leyes estatales y federales que regulan la figura del whistleblower, su protección y las recompensas que éstos perciben por denunciar hechos ilícitos en perjuicio del Estado<sup>292</sup>. Tal y como hemos visto a lo largo de la revisión del concepto de whistleblower en EE.UU, no se puede hablar de una fecha concreta en la que la figura del whistleblower irrumpe en la normativa estadounidense, sino que lo ha hecho de manera gradual y desde diferentes prismas. No obstante, los acontecimientos que marcaron la década de los 60 tales como la guerra de Vietnam y los nuevos riesgos derivados del desarrollo de la industria y de la tecnología propiciaron un contexto adecuado para impulsar nuevas normas regulatorias de esta figura.<sup>293</sup>

Ahora bien, la regulación de la protección del denunciante se ha visto muy influenciada por la evolución de la doctrina del Atwill employment (libre despido) que permitía a finales del s. XIX despedir libremente a los trabajadores sin ningún tipo de justificación o motivo. Esto provocó una serie de críticas a principios del s.XX que hizo que la teoría del despido fuera evolucionando hasta exigir una justificación por parte del empresario que quisiera despedir al trabajador<sup>294</sup>. Todo ello dio lugar a una multiplicidad de leyes estatales y federales relativas a la figura del whistleblower lo que implicó un conjunto de leyes contradictorias entre sí generando numerosas críticas al respecto<sup>295</sup>.

A continuación se hace un breve apunte de las leyes que regulan la entrega de incentivos económicos a los whistleblowers:

---

<sup>292</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1233.

<sup>293</sup>BOWDEN, P., "A Comparative Analysis of Whistleblower Protection. Australian Association for Professional and Applied Ethics", 12th *Annual Conference, Adelaida*, Australia, 2005 pp. 10-11.

<sup>294</sup>KOHN, S. M., *Concepts and Procedures in Whistleblowers Law*. Quorum Books, London, 2001, pp. 21-25.

<sup>295</sup>KOHN, S. M., *Concepts and Procedures...*, ob. cit., pp. 21-25.

1) La FCA es la más antigua de las leyes Qui Tam. Regula la posibilidad de entregar incentivos a los whistleblowers por la comisión de fraudes al Estado. La Ley tiene por objeto promover a los denunciantes prometiéndoles un porcentaje del dinero obtenido o recaudado. Aquellos que tuvieran conocimiento de cualquier fraude cometido al Estado percibirían entre el 10% y el 30% del dinero recaudado por el Estado<sup>296</sup>. Fue una de las primeras leyes que protegía a los denunciantes en Estados Unidos hasta el punto de garantizar una protección contra el despido injustificado.

2) La Sección 406 del Internal Revenue Services (IRS). La Qui Tam IRS incentiva a los ciudadanos a que denuncien fraudes fiscales cometidos al Estado.

3) La Sección 21F de la Securities Exchange Act. La SEC Qui Tam incentiva a los ciudadanos a que denuncien fraudes relacionados con el sector financiero y con la normativa del mercado de valores.

4) La Sección 23 de la Commodity Exchange Act.

5) La Dodd Frank Act. El 22 de julio del año 2010, el Presidente de los EE.UU., Barack Obama, firmó una ley que proveía de elevadas recompensas a personas individuales que informaran acerca de las violaciones de las leyes federales del mercado de valores, incluida la FCPA, a las autoridades (SEC,). Esta ley se denominó Dodd Frank Wall Street and Consumer Protection Act, y establece la posibilidad de obtener cuantiosas cantidades de dinero (entre el 10% y el 30% de la sanción impuesta), siempre que la cantidad recaudada por el gobierno supere el millón de dólares, por reportar conductas fraudulentas, como información privilegiada, blanqueo de capitales, infracciones fiscales, y otras violaciones de la FCPA, por empleados y competidores<sup>297</sup>.

---

<sup>296</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1233.

<sup>297</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., pp. 1233-1234.

6) La sección 922 de la SOX establece procedimientos que permiten a los empleados de las grandes empresas denunciar hechos ilícitos, estableciendo mecanismos de protección del whistleblower, siendo las denuncias recibidas por el *Compliance Officer* (CO) o el *Ombudsman*, remitiendo el informe del CO al comité de auditoría. Como hemos visto, como consecuencia del escándalo de Enron que se produjo, a través de la SOX, se obligó a toda compañía que cotizara en el mercado norteamericano a implementar internamente un canal de denuncia interna y/o externa que detectara fraudes en la empresa<sup>298</sup>.

### **2.2.1.1 False Claim Act**

Es necesario hacer especial hincapié en la FCA ya que en los Estados Unidos ha resultado fundamental en la lucha contra el fraude. Desde 1987 el gobierno federal ha abonado en indemnizaciones la cantidad de 2,877 billones de dólares.

Su origen tiene lugar en el año 1777, año en el que se firmó la Declaración de Independencia. Durante la Guerra de la Independencia diez marines decidieron denunciar ("*blow the whistle*") ante los Tribunales las torturas y trato inhumano sufridos por parte de los soldados ingleses arrestados a manos del comandante norteamericano Esek Hopkins, al mando de la nave Warren, oficial de reconocido prestigio, con importantes contactos con los políticos de Rhode Island.

El Capitán John Grannis informó al Congreso sobre los hechos y solicitó ante éste, el 26 de marzo de 1777, la suspensión del cargo y que se juzgara al comandante por esos hechos. El comandante fue suspendido y expulsado del ejército. Interpuso una denuncia en Rhode Island contra los diez denunciadores, siendo dos de ellos detenidos y enviados a prisión. El 23 de julio del año 1778, el Congreso se pronunció, manifestando que "*los señores*

---

<sup>298</sup>MOBERLY, R., "Sarbanes-Oxley's Structural Model to Encourage Corporate Whistleblower's", *BYU Law Review*. 2006.

*Marven y Shaw fueron arrestados por hacer lo que debían y por lo que creían que era justo, cumpliendo con su deber*". A los pocos días, el Congreso firmó y redactó la primera ley de protección de los delatores (whistleblowers), estableciendo que *"esa es la obligación y el deber de toda persona –militar o civil– en el servicio de los Estados Unidos de América, de informar lo antes posible al Congreso o cualquier otra autoridad gubernamental de cualquier conducta dolosa, fraudulenta, o relacionada con delitos menores, que tengan conocimiento"*. El Congreso dispuso que todo ciudadano que denunciara unos actos delictivos estaría legalmente protegido y defendido de ataques y represalias provenientes del denunciado, así como de toda mentira difamatoria que se produjera en su contra. El Congreso sería el encargado de abonar los gastos de defensa del denunciante<sup>299</sup>. Los denunciantes/delatores, finalmente ganaron la causa, abonando el Estado los gastos de su defensa, 1.418 de dólares<sup>300</sup>.

Como consecuencia de lo anterior y de otros diversos fraudes cometidos contra el Estado durante la guerra de secesión civil norteamericana el Presidente Lincoln convenció al Congreso y al Senado acerca de la necesidad de implantar una ley que protegiera al Estado de estos fraudes cuyo resultado fue la FCA en el año 1868. La FCA otorgaba al denunciante el 50% de lo que se recaudara producto de la denuncia, posteriormente fue modificada en numerosas ocasiones (1943, 1986, converging taxes 2006, securities fraud 2010) afectando al procedimiento y al porcentaje de compensación percibido por el whistleblower<sup>301</sup> proporcionándole entre un 15% o un 30 % sobre el total de lo recuperado incluyendo daños, costos, honorarios y sanciones. Tenía por objeto otorgar protección a los

---

<sup>299</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., pp. 1214-1215.

<sup>300</sup>KOHN, S. M., *The Whistleblower's handbook. A step by step to Doing What's Right and Protecting Your Self*. Lyons Press, 2011, pp. 195-200.

<sup>301</sup>LAHMAN LARRY, D., "Bad Mules, a primer of the Federal False Claim Act", *Oklahoma Bar Journal*, vol. 76, nº 12, 2005, p. 901; PAGE WEST, R., *Advising the Qui Tam Whistleblower: From Identifying a Case to Filing Under the False Claims Act*, edit. American Bar Association, 2009, pp 1-9.

denunciantes hasta el punto de que se ha considerado como la ley de denuncia que más éxito ha tenido en Estados Unidos.

En virtud de la citada ley, cualquier ciudadano que tenga conocimiento de un acto de falsedad o fraude puede presentar una demanda como delator mediante el ejercicio de la acción Qui Tam<sup>302</sup>. Además, la ley contempla no sólo poder percibir un porcentaje de lo recaudado sino también la posibilidad de reincorporar al empleado con el mismo estatus y antigüedad, la obtención del duplo de los pagos atrasados junto con intereses, así como una indemnización por los daños y perjuicios sufridos<sup>303</sup>.

Como su nombre indica, la finalidad de esta ley es la de eliminar las reclamaciones falsas ante el gobierno de Estados Unidos relacionadas con asuntos como la prestación de servicios médicos, el uso de medicamentos, el pago de tasas o los subsidios federales. La reclamación puede referirse a cualquier cantidad de dinero o de bienes que estén destinados a los intereses del gobierno. Ahora bien, es necesario que esas reclamaciones falsas se hayan realizado con conocimiento de su falsedad. Es decir, el infractor debe haber actuado con temeraria inobservancia de la veracidad o falsedad de la información.<sup>304</sup> Se trata de determinar si la reclamación responde a la finalidad de la ley de evitar el riesgo de inducir al gobierno a realizar pagos indebidos<sup>305</sup>.

La importancia de esta ley radica, en parte, en las cantidades de dinero que ha permitido recaudar. A título de ejemplo, en 1986 se recuperaron más de 30 mil millones de dólares, desde el año 2009 se han recaudado 14.2 mil millones y tan sólo en 2012 se recuperaron más de 5 mil millones de dólares.

---

<sup>302</sup>KOHN, S.M., *Concepts and Procedures...*, ob. cit., p. 204.

<sup>303</sup>Federal false claims acts <http://www.cftc.gov/ConsumerProtection/WhistleblowerProgram/index.htm>

<sup>304</sup>31 U.S.C & 3729 (b) (1) (a) U.S. Government Publishing office. Extraído de <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title31/pdf/USCODE-2011-title31-subtitleIII-chap37-subchapIII-sec3729.pdf>.

<sup>305</sup>KOHN, S.M., *Concepts and Procedures...*, ob. cit., pp. 209-210.

Por último, respecto al procedimiento que regula, una vez que el ciudadano presenta la demanda, ésta es archivada durante el tiempo que el gobierno investiga la situación y decide si intervenir o no. En el supuesto de que el gobierno opte por no continuar con el procedimiento, corresponde al delator decidir si seguir o no con el pleito.

### **2.2.1.2 La Foreign Corrupt Practices Act (FCPA)**

En la aclaración del escándalo Watergate en Estados Unidos<sup>306</sup> el whistleblower "Deep Throat" denunció las prácticas ilegales llevadas a cabo por el gabinete del presidente Nixon, poniéndose en contacto con los periodistas del Washington Post, Bob Woodward y Carl Bernstein. La identidad de Deep Throat se mantuvo en secreto durante 30 años; conociéndose finalmente su identidad, Mark Fet. De estos hechos se deriva la FCPA, que castiga con severas penas de cárcel e importantes sanciones económicas a las empresas o personas jurídicas que sobornaran a funcionarios públicos en el extranjero, y cuya característica especial es su alcance extraterritorial<sup>307</sup>.

La FCPA<sup>308</sup> sanciona a las personas físicas que violen la ley con una pena de prisión superior a cinco años y una multa superior a 250.000 dólares y, para las empresas, establece una pena de multa por encima de los 2 millones de dólares, y una pena de prisión superior a cinco años.

La FCPA prohíbe la toma de represalias en contra de los delatores. Los empleadores en ningún caso pueden despedir, amenazar o discriminar a los que aporten información a las autoridades. La ley permite a los denunciantes

---

<sup>306</sup>Las compañías de los EE.UU., además de las corporaciones en Francia, el Reino Unido y Alemania, pagaron algo más de mil millones de dólares en multas o acuerdos por violaciones a la FCPA, tal y como recoge [www.Fcpa-worldcompliance.com](http://www.Fcpa-worldcompliance.com).

<sup>307</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1216.

<sup>308</sup><http://www.justice.gov/criminal/fraud/fcpa/statutes/regulations.html> y <http://www.transparency-usa.org/documents/FCPAvsBriberyAct.pdf>.

que las informaciones que aporten a las autoridades sean anónimas<sup>309</sup>. Desde la entrada en vigor de la FCPA, el Gobierno de los EE.UU. ha observado un incremento notable de denunciantes, obligando a las empresas a llegar a acuerdos con el Estado por valor de muchos millones de euros<sup>310</sup>.

### 2.2.1.3 Whistleblowers Protection Act (WPA)

Esta ley se basa en la libertad de expresión y tiene como finalidad la protección de aquella persona que realiza la revelación de una mala práctica del gobierno (como puede ser una incorrecta administración o el abuso por parte de la autoridad) que pueda suponer un peligro para la salud o la seguridad<sup>311</sup>.

A través de la *Office of Special Counsel* (OSC) o del denominado *Meryt Systems Protections Board* (MSPB), la ley respalda el llamado “sistema de méritos” al proteger a los empleados federales de prácticas prohibidas, especialmente represalias por denuncias. El MSPB es configurado como un tribunal de naturaleza administrativa responsable de la aplicación y revisión de las decisiones de la propia OSC<sup>312</sup>.

No obstante, de esta ley no siempre se hizo un uso correcto, abusando en ocasiones el denominado “Consejero Especial” (*Special Counsel*) de su posición y autoridad para actuar en perjuicio de los denunciantes. Tanto es

---

<sup>309</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1234.

<sup>310</sup>Como ejemplos, en el mes de junio del año 2010 el gobierno de los EE.UU. anunció acuerdos con distintas empresas por violación de la Ley; es el caso de Snamprogetti, empresa holandesa, por 365 millones de dólares, y Technip S.A., por valor de 338 millones de dólares (MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1234).

La empresa Siemens pagó 1,6 billones de euros a los gobiernos de EE.UU. y Alemania, como parte de un acuerdo llevado a cabo por la compañía con los dos Estados por violaciones de la FCPA. Si la denuncia la hubiera realizado un denunciante, habría percibido el 30% de la cantidad recaudada por los estados, que ascendió a 496 millones de dólares (MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., pp. 1234-1235).

<sup>311</sup>Public Service Integrity Office (Canadá), *A comparative international analysis of regimes for the disclosure of wrongdoing*. Gobierno de Canadá 2004, pp. 4 y 58.

<sup>312</sup>Public Service Integrity Office (Canadá) ob. cit. Gobierno de Canadá 2004, p. 58.



así, que durante la década de 1978 a 1988 tan solo cuatro de los 200 denunciantes ganaron sus casos.

En este contexto, en el año 1985, los senadores Grassley, Carl Levin, David Pryor y la representante Pat Schroeder lideraron una nueva ley que garantizase la verdadera defensa del denunciante. De esta forma, se incluyó la posibilidad de dar audiencia en el proceso administrativo, se suprimió el Consejero Especial y se eliminó cualquier tipo de represalia contra los denunciantes.

Pese a que la nueva ley fue aprobada por unanimidad en el Congreso, se vetó por el Presidente Reagan, por lo que fue necesario esperar hasta marzo de 1989, para que una nueva versión más reforzada fuera aprobada también por unanimidad en el Congreso y, posteriormente firmada el 10 de abril de 1989 por el presidente George Bush.

En 1994 la ley exigió una nueva revisión tras las discrepancias de criterio surgidos entre el Congreso y el Tribunal del Circuito Federal de Apelaciones, por lo que la modificación de la misma respondió a las necesidades de: corregir los fallos de la anterior, ampliar su ámbito de aplicación y reforzar la libertad de expresión de los empleados.

Sin embargo, con esta nueva versión de la ley tampoco se resolvieron los problemas que su aplicación planteaba, puesto que el Tribunal del Circuito Federal de Apelaciones consideraba que mediante la misma no se protegía cualquier divulgación de creencia razonable sino que debía acreditarse mediante pruebas irrefutables.

En el año 2000, el senador Daniel Akaka lideró nueva campaña por su reforma que duró 13 años con el apoyo de otros denunciantes e incluso de organizaciones no gubernamentales, lo que puso de manifiesto la verdadera voluntad de garantizar la protección real de los denunciantes. Tras el voto por unanimidad del Congreso se instauró en el año 2012 la conocida como Ley

de Mejora de Protección de Denunciantes (Whistleblower Protection Enhancement Act) que incluyó un programa piloto para el acceso a los tribunales de apelación.

#### 2.2.1.4 Códigos Éticos

En Estados Unidos, tras el caso político Watergate, y otros escándalos financieros, numerosas empresas decidieron incorporar entre su normativa interna códigos éticos de conducta, señalando como principios fundamentales de la empresa los valores éticos y la integridad. Los códigos éticos y de conducta describían una amplia variedad de conductas prohibidas dentro de la empresa, estableciendo los límites de conducta que no podían traspasar los empleados y disponiendo sanciones ante su incumplimiento<sup>313</sup>.

The U.S. Federal Organizational Sentencing Guidelines (OSG)<sup>314</sup>, con objeto de evitar escándalos financieros y prácticas delictivas corporativas, introdujo en el año 1991 una norma relativa a la implantación de los códigos éticos en las empresas de cierto tamaño, en el sentido de sancionar incluso penalmente a aquellas empresas que no ejercieran un control a sus empleados a través de la figura del *compliance officer* (oficial de cumplimiento normativo). Se estableció la obligatoriedad en la difusión y formación de los empleados acerca del contenido del código ético y las sanciones por violar su contenido, asimismo se introdujo la figura del whistleblower, por la cual se contemplaba la posibilidad de que cualquier trabajador o directivo denunciara

---

<sup>313</sup>NWEBERG, J. A., "Corporate Codes of Ethics, Mandatory Disclosure, and the Market for Ethical Conduct". *Vermont Law Review*, nº 29, 2005, pp. 253-295.

CALDERÓN, R./ FERRERO, I./ REDIN, D., "Ethical Codes and Corporate Responsibility of the Most Admired Companies of the World: Toward a Third Generation Ethics?", *D. Business and Politics*. Vol. 14 (4), 2012, pp. 1-24.

FRANCÉS, P./ BORREGO, A./ VELAYOS, C., *Códigos éticos en los negocios. Creación y ampliación en empresas e instituciones*, Madrid, 2003.

<sup>314</sup>Us Sentencing Guidelines Manual. 1991. Extraído de: [http://www.ussc.gov./Guidelines/1991\\_guidelines/manua\\_pdf/chapter\\_8.pdf](http://www.ussc.gov./Guidelines/1991_guidelines/manua_pdf/chapter_8.pdf).

hechos contrarios a la ley y/o al código ético, garantizando la protección del whistleblower ante posibles represalias del empleador<sup>315</sup>.

### **2.2.1.5 Sarbanes-Oxley Act 2002**

El 30 de julio de 2002, la SOX entró en vigor tras su aprobación en el Congreso (impulsada por el senador Paul Sarbanes y el representante Michael G.Oxley) durante el gobierno de George W. Bush. Esta ley tuvo por objeto evitar cualquier tipo de alteración fraudulenta de las acciones de las sociedades cotizadas en Bolsa así como proteger a los inversores. Además, respondió a la necesidad de lavar la imagen de las instituciones y del gobierno americano<sup>316</sup>.

De esta forma, trata de evitar los escándalos financieros de las compañías y de recuperar la confianza de los inversores, para lo cual configuró unos patrones de actuación para los consejos de administración y de dirección de las sociedades (incorporando incluso responsabilidades penales) y estableció nuevos mecanismos contables para aquellas sociedades de Estados Unidos que cotizaran en Bolsa, limitando su aplicación a asuntos financieros. Con la misma se garantiza la protección del denunciante que puede reclamar ante una Agencia Federal (con competencias para aplicar la ley), ante cualquier miembro o comité del Congreso o ante cualquier persona con facultades de supervisión sobre el trabajador, lo que evita al denunciante la presentación de la queja directamente ante su empleador.

Es cierto que con esta ley no se garantiza que la sociedad no emita una contabilidad fraudulenta pero sí se exige la responsabilidad de asegurar a la compañía auditora que la información sea veraz y completa, a través de una serie de requerimiento por parte de la SEC.

---

<sup>315</sup>MOBERLY, R. Y WYLIE, L., "An Empirical Study of Whistleblower Policies in United States Corporate Code of Ethics". Extraído de <http://ssrn.com/>.

<sup>316</sup>Sarbanes Oxley Act. Extraído de: <http://www.cftc.gov/ConsumerProtection/WhistleblowerProgram/index.htm>

Es evidente que tras los escándalos financieros ocurridos en Estados Unidos, esta ley se planteaba como una verdadera necesidad. No obstante, ha sido objeto de numerosas críticas por los costes que ha supuesto su implementación, así como por el hecho de que no incluye ni la reubicación del denunciante ni ningún tipo de indemnización.

#### **2.2.1.6 Dodd-Frank Wall Street Reform and Consumer Protection Act**

La *Dodd-Frank Wall Street Reform and Consumer Protection Act* es una norma federal de los Estados Unidos de América que fue promulgada definitivamente el 21 de julio de 2010. La citada ley nace promovida por el representante Barney Frank y el senador Chris Dodd y pone en práctica la reforma de la regulación financiera patrocinada por el gobierno del presidente Barack Obama; aquélla fue propuesta inicialmente por la Administración demócrata a principios de junio de 2009, cuando la Casa Blanca envió al Congreso una serie de proyectos de ley relativos a la cuestión que aquí nos ocupa. Más de un año después, el texto definitivo se aprobó de modo mayoritario por parte de ambas instancias legislativas (la Cámara de Representantes y el Senado) sin apenas modificaciones sustanciales<sup>317</sup>.

Introducida como una respuesta a la grave recesión económica y a las crisis financieras de los últimos años, la *Dodd-Frank Wall Street Reform and Consumer Protection Act* incorpora los cambios más significativos en la regulación financiera de los Estados Unidos desde la reforma que siguió a la Gran Depresión del año 1929. Ello representa un cambio significativo en el contexto económico, empresarial y regulatorio estadounidense, cosa que afecta a todos los organismos federales de regulación financiera y a casi todos los aspectos de la industria de los servicios financieros del país.

---

<sup>317</sup>GONZALEZ DE LEON BERINI, A., "El criminal compliance en la reforma norteamericana de la Dodd-Frank Act", en AA.VV., *Criminalidad de empresa y compliance. Prevención y reacciones corporativas*, dir. J.M. Silva, Barcelona, 2013, p. 131.

Esta ley supone un profundo cambio en el modo en que se regula el sistema bancario, mercantil y cambiario de los Estados Unidos de América para evitar casos como el de Lehman Brothers o la burbuja hipotecaria<sup>318</sup>. A modo de resumen, y sin ánimo de ser en absoluto exhaustivos, podemos pues identificar aquí las siguientes siete líneas maestras que sirven de verdadero *leitmotiv* de la reforma económica y financiera introducida por la *Dodd-Frank Wall Street Reform and Consumer Protection Act*<sup>319</sup>:

a) Un sistema independiente y ampliado de protección al consumidor: así, se crea un nuevo e independiente organismo gubernamental de control, con sede en la Reserva Federal, al que se atribuyen todas las competencias necesarias para garantizar que los consumidores tengan la información clara y precisa que requieren a la hora de realizar operaciones de carácter financiero (como -por ejemplo-constituir una hipoteca, obtener tarjetas de crédito o bien comprar otros productos financieros), y para protegerles de posibles cargos ocultos, términos abusivos y otras prácticas engañosas.

b) La supresión del mecanismo del "rescate" gubernamental (*bailout*) a las entidades llamadas TBTF (*too big to fail*): se descarta definitivamente la posibilidad de usar el dinero que proviene de los impuestos de los contribuyentes para rescatar a aquellas compañías financieras que amenazan a la economía americana. En este sentido, pues, la ley crea un procedimiento especial para la liquidación de todas aquellas entidades financieras que quiebren. Además, también se añaden las siguientes medidas: la imposición de requisitos muy exigentes para las ampliaciones de capital, la actualización de las competencias de la Reserva Federal para garantizar así el establecimiento y el cumplimiento de estándares rigurosos y la supervisión del sistema en general, todo

---

<sup>318</sup>Ley Dodd Frank. Extraído de <http://www.cftc.gov/ConsumerProtection/WhistleblowerProgram/index.htm>

<sup>319</sup>GONZALEZ DE LEON BERINI, A., "El criminal compliance...", ob. cit., pp. 133-134.

ello con el fin de proteger a los consumidores, a los inversores y a las empresas.

c) Un sistema avanzado de prevención: se crea un consejo para identificar y abordar los riesgos sistémicos planteados por las entidades financieras grandes y complejas y también por parte de los productos financieros de riesgo novedosos, antes de que puedan llegar a amenazar realmente la estabilidad de la economía americana<sup>320</sup>.

d) Una mayor garantía de transparencia y rendición de cuentas para los instrumentos financieros no comunes (*exotic*): la citada ley elimina las lagunas que permitían que las prácticas de riesgo y abusivas (especialmente los llamados *hedge funds* -fondos de cobertura-) pasaran inadvertidas y no reguladas.

e) Las provisiones sobre las compensaciones económicas a los ejecutivos y la Gobernabilidad Corporativa: la reforma proporciona a los accionistas de las entidades financieras la posibilidad de decidir sobre los salarios de los ejecutivos de dichas instituciones, así como también sobre la totalidad de los asuntos corporativos -así, como mínimo con una votación no vinculante para el Consejo de Administración.

f) Las medidas de protección de los inversores: la *Dodd-Frank Wall Street Reform and Consumer Protection Act* establece además la adopción de todo un conjunto de estrictas reglas para la mayor transparencia y para la implantación eficaz de los correspondientes mecanismos de rendición de cuentas para las agencias de calificación crediticia, todo ello con el fin de proteger a los inversores y a las empresas.

---

<sup>320</sup>GONZALEZ DE LEON BERINI, A., "El criminal compliance...", ob. cit., p. 134.

g) La aplicación efectiva de la regulación existente en materia de contabilidad financiera: la ley fortalece la supervisión y faculta a los organismos gubernamentales reguladores para perseguir de manera real y firme (incluso con *mecanismos sancionatorios graves*) *el fraude financiero, los conflictos de interés y, de igual modo, todas aquellas manipulaciones del sistema que beneficien intereses particulares a expensas de los de los accionistas*<sup>321</sup>.

La profunda reforma económica y financiera del año 2010 también introduce determinados cambios significativos en el ámbito de la regulación de los llamados whistleblowers. La Dodd-Frank Wall Street Reform and Consumer Protection Act crea un programa –en el marco de las competencias de la SEC – con el fin de promover que los trabajadores del sistema financiero informen convenientemente a las agencias gubernamentales de las posibles infracciones de la normativa. Y para ello se prevén recompensas de un 10% a un 30% de la cuantía total recuperada que la SEC obtenga (siempre que exceda más de un millón de dólares) gracias a la información proporcionada<sup>322</sup>.

La citada ley confiere a los *whistleblowers* un papel central en la articulación del sistema de cumplimiento efectivo de la normativa económica y financiera y establece importantes medidas de protección a los denunciantes<sup>323</sup>, ya que entre los poderes de la SEC se incluye la posibilidad de premiar a los denunciantes internos con incentivos económicos muy sustanciosos. Esta medida se basa en un programa muy similar establecido en el año 2006 por el IRS, y que ha conducido a resultados muy exitosos en la lucha contra el fraude fiscal en el ámbito federal.

---

<sup>321</sup> GONZALEZ DE LEON BERINI, A., "El criminal compliance...", ob. cit., pp. 134-135.

<sup>322</sup> GONZALEZ DE LEON BERINI, A., "El criminal compliance...", ob. cit., pp. 136-137.

<sup>323</sup> Ley Dodd Frank. Extraído de <http://www.cftc.gov/ConsumerProtection/WhistleblowerProgram/index.htm>

La *Dodd-Frank Wall Street Reform and Consumer Protection Act* establece el citado programa de *whistleblowing* con el objetivo previsto de fortalecer así la protección general de los inversores mediante una mayor disuasión a las entidades financieras para evitar que lleven a cabo infracciones de la legislación vigente. En este sentido, pues, el régimen previsto en la ley respecto de los denunciantes internos pretende estar al servicio de una aplicación más eficaz y eficiente de la normativa federal por parte de la Comisión de Valores y Bolsa de los Estados Unidos<sup>324</sup>. Mediante el programa de *whistleblowing* se atribuye recompensa a aquellos denunciantes que de forma voluntaria pongan en conocimiento de la SEC nueva información que sirva como instrumento para ejercer acciones legales contra los que cometan infracciones de las leyes de mercados de valores. Este programa supuso por un lado, que todos aquellos que estuviesen dispuestos a violar las leyes de mercado tuvieran que hacer frente a la posibilidad de que alguien dentro de la propia empresa pueda ser un denunciante y, por otro, ha generado incentivos suficientes para que se denuncie la infracción cometida. Además, este sistema beneficia a las instituciones encargadas de velar por el funcionamiento de los mercados financieros al garantizar el aumento de las denuncias de las infracciones en el mercado financieros sin tener que aumentar el importe de las inversiones para que las mismas tengan lugar.<sup>325</sup>

Sin embargo, como sucede en muchos otros aspectos de la reforma financiera, la ley sólo contiene pautas generales que necesitan de un posterior desarrollo. Así, la SEC propuso un catálogo de reglas para la aplicación de las disposiciones legales previstas en el marco del programa de *whistleblowing* el 3 de noviembre de 2010, y se inició entonces un proceso de audiencia pública para recoger comentarios y sugerencias al respecto. Las reglas finales se aprobaron con ligeras modificaciones el 25 de mayo de

---

<sup>324</sup>GONZALEZ DE LEON BERINI, A., "El criminal compliance...", ob. cit., p. 137.

<sup>325</sup>TALADRIZ, C., "Mercados de Capitales. Whistleblowers en los mercados financieros", 21 de noviembre de 2011. Extraído de <http://mercapuc.blogspot.com.es/2011/11/whistleblowers-en-los-mercados.html>



2011, por un margen estrecho de votación, y entraron en vigor el 11 de agosto de 2011<sup>326</sup>.

Existen dos puntos de vista imperantes en la discusión sobre el probable impacto de las nuevas disposiciones relativas a los denunciantes internos. Los defensores del sistema actual sostienen que el programa mejorará la protección de los accionistas al permitir que la SEC aproveche sus recursos limitados para contactar con los *insiders* que tengan un conocimiento directo acerca de la ilicitud de las conductas intraempresariales. En cambio, quienes se oponen a las nuevas normas argumentan que se socavan así los programas ya existentes de cumplimiento interno (*compliance*), por lo que en el futuro será más difícil de detectar y disuadir el fraude corporativo.

Como ya dijimos antes, la ley exige que la SEC recompense a los denunciantes internos que voluntariamente proporcionan una información desconocida por parte de los organismos de control gubernamental acerca de una infracción de las leyes federales del sistema financiero, siempre que dicha revelación conduzca a descubrir con éxito una conducta ilícita por parte de la entidad en cuestión. Los incentivos económicos van desde el 10% hasta el 30% de las sanciones pecuniarias impuestas -con sujeción al umbral de 1.000.000 de dólares, que debe ser la cuantía mínima defraudada que sale a la luz con la revelación.

Como ya hemos puesto de manifiesto, la *Dodd-Frank Wall Street Reform and Consumer Protection Act* establece el requisito de que las sanciones monetarias impuestas a la entidad financiera gracias a la información proporcionada por el denunciante interno deben sumar por lo menos la nada despreciable cantidad de 1.000.000 de dólares. En efecto, se trata de un umbral mínimo que sólo se explica en la medida en que permite una asignación más eficiente de los recursos limitados de la SEC, ayudando a

---

<sup>326</sup>GONZALEZ DE LEON BERINI, A., "El criminal compliance...", ob. cit., p. 137.

identificar y a perseguir aquellas infracciones de la normativa federal que se catalogan como potencialmente más graves<sup>327</sup>.

La historia reciente de los Estados Unidos de América demuestra claramente que los empleados de una compañía que se convierten en *whistleblowers* tienen un papel clave a la hora de detectar y prevenir eficazmente las conductas corporativas fraudulentas o ilícitas. Por eso se amplía la protección legal de los denunciantes internos, prohibiendo así las represalias contra quienes proporcionan a la SEC cualquier información sobre una infracción, independientemente de si se impone finalmente una sanción pecuniaria o de si el sujeto reúne todas las condiciones para recibir una recompensa económica.

Sin embargo, la diferencia más importante y controvertida entre las disposiciones del programa de *whistleblowing* de la *Dodd-Frank Wall Street Reform and Consumer Protection Act* se refiere al medio a través del cual inicialmente el informador puede proporcionar información acerca de las posibles infracciones de la empresa. En la regulación anterior se exigía utilizar previamente los canales establecidos en el sistema interno de control y de cumplimiento (*compliance*), mientras que la reforma de 2010 permite al denunciante eludir por completo dichos mecanismos, y acudir directamente a la SEC (tal y como el presidente de esta institución declaró "*para una agencia con limitados recursos como la SEC, es crítico ser capaz de aprovechar los recursos que nos puede proveer la gente directamente respecto a las violaciones que se estén cometiendo de las leyes de mercado de valores*"<sup>328</sup>).

En este sentido, la propia SEC reconoce explícitamente que su propuesta regulatoria implica el claro peligro potencial de "*reducir la efectividad de los programas de cumplimiento existentes en las entidades financieras, tales como la auditoría legal y los procesos internos similares para investigar y para*

---

<sup>327</sup>GONZALEZ DE LEON BERINI, A., "El criminal compliance...", ob. cit., pp. 137-138.

<sup>328</sup>TALADRIZ, C., "Mercados de Capitales...", ob. cit.

*perseguir las posibles infracciones de la normativa federal*". A pesar de ello, dicho organismo de control gubernamental indica que la reforma no pretende disuadir a los denunciantes que trabajan para empresas que cuentan con sólidos y eficaces programas de *compliance* a que informen primero de la infracción al personal interno competente<sup>329</sup>.

En función de los debates internos que se produjeron en el seno de la propia SEC y de las sugerencias y de los comentarios realizados por quienes participaron del trámite de audiencia pública, podemos identificar dos puntos de vista contrapuestos respecto a los posibles efectos del nuevo régimen legal del *wistleblowing*. A favor de la reforma se esgrime que maximiza la presentación de denuncias mejor fundamentadas y promueve una actitud corporativa de mayor cumplimiento interno; ello tiene como consecuencia una aplicación más eficaz y eficiente de la normativa federal por parte de la agencia.

La visión de los detractores sugiere que las nuevas disposiciones aprobadas hacen más difícil detectar y detener las conductas ilícitas o fraudulentas intraempresariales, al socavar los ya existentes programas de cumplimiento de las empresas, establecidos en virtud de la legislación anterior. Se argumenta, en este sentido, que un sistema efectivo de *compliance* interno permite a los responsables de la entidad financiera identificar y gestionar a tiempo los riesgos de posibles infracciones intraempresariales, incluso ya antes de que dichas acciones se materialicen o se conviertan en un defecto estructural.

El punto más controvertido de la propuesta, y el tema abordado con mayor frecuencia en los comentarios recogidos en el trámite de audiencia pública, es el hecho de que los denunciantes internos no estén obligados a informar de la infracción en primer lugar a través de los sistemas de control internos de la empresa, antes de acudir a la SEC. Los sujetos individuales apoyaron

---

<sup>329</sup>GONZALEZ DE LEON BERINI, A., "El criminal compliance...", ob. cit., p. 138.

mayoritariamente la disposición finalmente adoptada. En cambio, las entidades financieras se opusieron por unanimidad a la propuesta, los 283 comentarios recibidos expresan reparos y críticas al respecto<sup>330</sup>.

Otro de los aspectos interesantes de la propuesta es que no ofrece una amnistía general para las personas que proporcionen información relevante a la Comisión de Valores y Bolsa de los Estados Unidos; así pues, el programa de *whistleblowing* de la *Dodd-Frank Wall Street Reform and Consumer Protection Act* permite a la SEC emprender acciones legales contra un denunciante interno si su conducta en relación con la infracción reportada pone de manifiesto una actuación personal ilícita o fraudulenta. El 87% de los participantes en el trámite de audiencia pública apoyaron esta cláusula.

A modo de conclusión parcial, podemos señalar que el análisis de las sugerencias y de los comentarios formulados en el trámite de audiencia pública está en consonancia con la postura de los defensores de la nueva regulación, según la cual los accionistas gozan de una mayor protección con el programa de *whistleblowing* de la reforma de 2010. A tales efectos, recordemos que las observaciones a título individual fueron abrumadoras en favor de la aplicación de las disposiciones de la SEC; en contraste, las entidades financieras expresaron su desaprobación unánime de la propuesta.

La investigación empírica también ha llevado a algunos autores a afirmar que la nueva regulación de la figura del *wistleblower* en el ámbito de la reforma financiera se valora muy positivamente por parte de los accionistas; así, el hecho de que el índice bursátil fuera al alza en los días posteriores a la aprobación se interpretó entonces como un síntoma de que los mercados consideraron potencialmente efectivo el actual escenario regulatorio. Y es que el análisis ponderado de la reforma y la reacción de sus destinatarios sugiere

---

<sup>330</sup>GONZALEZ DE LEON BERINI, A., "El criminal compliance...", ob. cit., pp. 138-139.

un incremento en la protección legal de los accionistas y los inversores, tal y como se pretendía<sup>331</sup>.

Una conclusión que también se apoya en otro dato relevante: las entidades financieras con programas internos de cumplimiento más débiles- y en particular aquellas que no tienen procedimientos adecuados para que los empleados denuncien los actos ilícitos o fraudulentos intraempresariales- han sido más propensas a manifestarse en contra de la reforma finalmente introducida por la SEC. En sentido contrario, las empresas que demuestran tener sistemas de *compliance* más eficaces aceptan la nueva regulación de la figura del *wistleblower* de la *Dodd-Frank Wall Street Reform and Consumer Protection Act*.

Para evitar consecuencias tales como el abuso de la relación de confidencialidad entre abogado y cliente, o la creación de incentivos inadecuados para los responsables de los programas de cumplimiento interno, la propuesta restringe el acceso a la condición de *whistleblower*. Así, no gozan de protección legal los abogados externos de las entidades financieras, los funcionarios que obtienen información en el desempeño de su cargo, y quienes tienen conocimiento de la infracción por ser parte integrante del sistema de *compliance* intraempresarial, de una auditoría legal o tienen funciones similares.

Por otra parte, la *Dodd-Frank Wall Street Reform and Consumer Protection Act* exime a la Comisión de Valores y Bolsa de los Estados Unidos de la obligación de revelar la información obtenida por cualquier procedimiento de acuerdo a los fines de la reforma, así las cosas, la supervisión del cumplimiento de la normativa, la evaluación de riesgos u otras actividades de control. A este respecto, la SEC afirma que la reforma citada sirve para garantizar la confidencialidad de los informantes; sin embargo, el nuevo

---

<sup>331</sup>GONZALEZ DE LEON BERINI, A., "El criminal compliance...", ob. cit., p. 139.

marco legal ha sido criticado por constituir una excepción a la regla general de divulgación aplicable a las agencias federales.

En definitiva, es importante destacar que las nuevas previsiones normativas modifican la legislación anterior de los Estados Unidos de América para permitir que la Comisión de Valores y Bolsa no revele datos o información que se haya obtenido en el ejercicio de sus funciones de control, excepto mediante un exhorto judicial (referido a una causa concreta, especificando el contenido de la indagatoria) o un requerimiento del Congreso. Así las cosas, la regla general es ahora que la SEC puede negarse a suministrar todos aquellos documentos que considere como parte integrante de sus actividades de supervisión<sup>332</sup>.

## **2.3 El whistleblowing en la Unión Europea y en la normativa nacional europea**

### **2.3.1 Unión Europea. Grupo de Trabajo Directiva 95/46/CE**

Un documento importante para el diseño de los procedimientos de denuncia es el elaborado por el Grupo de Trabajo del Artículo 29 sobre Protección de Datos<sup>333</sup>, denominado Dictamen 1/2006 sobre la aplicación de las normas de la UE relativas a la protección de datos a programas internos de denuncia de irregularidades en los campos de la contabilidad, controles contables internos, asuntos de auditoría, lucha contra el soborno, delitos bancarios y financieros<sup>334</sup>.

Este Grupo emitió el día 1 de febrero de 2006 un Dictamen sobre la aplicación de las normas de la UE relativas a la protección de datos a

---

<sup>332</sup>GONZALEZ DE LEON BERINI, A., "El criminal compliance...", ob. cit., pp. 139-140.

<sup>333</sup>Es un órgano consultivo europeo e independiente sobre intimidad y protección de datos. En el artículo 30 de la Directiva 95/16/CE y en artículo 15 Directiva 2002/58/CE se describen sus competencias".

<sup>334</sup>Texto localizable en [www.agpd.es/.../WP-117-sarbanes-ES.pdf](http://www.agpd.es/.../WP-117-sarbanes-ES.pdf). Según se dice en la portada del propio documento "el Grupo de Trabajo se creó en virtud del Artículo 29 de la Directiva 95/46/CE.

programas internos de denuncia de irregularidades en los campos de la contabilidad, controles contables internos, asuntos de auditoría, lucha contra el soborno, delitos bancarios y financieros, en el que analiza (i) la cuestión de la legitimidad de los sistemas de denuncia de irregularidades; (ii) la aplicación de los principios de calidad de datos y proporcionalidad; (iii) la provisión de una información clara y completa sobre el programa; (iv) los derechos de la persona inculpada; (v) la seguridad de las operaciones de tratamiento; (vi) la gestión de los programas de denuncia de irregularidades internos; (vii) las cuestiones relativas a la transferencia de datos internacionales; y (viii) los requisitos de comprobación previa y notificación<sup>335</sup>.

Este Dictamen se elaboró para establecer unas pautas en materia de protección de datos a las empresas que, por influencia de la regulación estadounidense, estaban implantando procedimientos internos de denuncia y se encontraban a menudo ante el dilema de dar preferencia a las disposiciones de la SOX o a la normativa europea en materia de protección de datos<sup>336</sup>. Este texto no tiene como objeto directo valorar la efectividad de estos sistemas desde una perspectiva jurídico-penal y no tiene carácter vinculante. Al aconsejar limitar ciertos usos de dichos procedimientos supone de facto un elemento a tener en cuenta a efecto de hacer apreciaciones acerca de validez y efectividad de las medidas implantadas por una empresa<sup>337</sup>.

Este Dictamen se limita exclusivamente a los programas en los que se denuncien irregularidades en las áreas de contabilidad, auditoría, lucha contra el soborno y delitos bancarios y financieros, y entiende que para que la política de denuncia sea correcta el tratamiento de los datos personales debe

---

<sup>335</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1225-1226.

<sup>336</sup>Como se afirma en el propio Dictamen (pp. 6-7), "la puesta en marcha de programas de denuncia de irregularidades, en la gran mayoría de los casos, estará basada en el tratamiento de datos personales "es decir, en la recopilación, registro, almacenamiento, difusión y cancelación de datos relacionados con una persona identificada o identificable), lo que significa que son de aplicación las normas sobre protección de datos".

<sup>337</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. p. 166.

ser legítimo y satisfacer uno de los motivos establecidos en el artículo 7<sup>338</sup> de la Directiva 95/46/CE. En relación con los principios de calidad y de proporcionalidad de los datos a los canales de denuncia, el Dictamen plantea la posible limitación del número de personas autorizadas para informar de supuestas incorrecciones o mala conducta, y, fundamentalmente, la promoción de informes identificados y confidenciales, frente a los informes anónimos<sup>339</sup>.

En cuanto al suministro de información clara y completa sobre el programa de denuncias, el Dictamen considera que, en aplicación del artículo 10<sup>340</sup> de la Directiva 95/46/CE, el responsable del tratamiento tiene el deber de informar a los interesados (a) sobre la existencia, objetivo y funcionamiento del

---

<sup>338</sup>El artículo 7 de la Directiva 95/46/CE establece que los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

- a) el interesado ha dado su consentimiento de forma inequívoca,
- b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o
- c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
- d) es necesario para proteger el interés vital del interesado, o
- e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o
- f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la Directiva 95/46/CE.

<sup>339</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1226.

<sup>340</sup>El artículo 10 de la Directiva 95/46/CE en relación con la información en caso de obtención de datos recabados del propio interesado, establece que los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernen, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:

- a) la identidad del responsable del tratamiento y, en su caso, de su representante;
- b) los fines del tratamiento de que van a ser objeto los datos;
- c) cualquier otra información tal como: 1) los destinatarios o las categorías de destinatarios de los datos, 2) el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder, y 3) la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.



programa; (b) los destinatarios de los informes, y (c) los derechos de acceso, rectificación, cancelación y oposición de las personas de quienes se informa. El Dictamen advierte también de que los responsables del tratamiento deben ofrecer información sobre el hecho de que la identidad del denunciante se mantendrá confidencial durante todo el proceso, que el abuso del sistema podría tener como consecuencia acciones contra el autor del abuso y, por último, que podrá informarse a los usuarios del sistema de que no se enfrentarán a ninguna sanción si utilizan el sistema de buena fe<sup>341</sup>.

Con respecto a los derechos de la persona inculpada, el Dictamen pone un especial énfasis en el derecho de información, y señala que conforme al artículo 11<sup>342</sup> de la Directiva 95/46/CE es obligatorio informar a las personas siempre que los datos se recaben de un tercero –en este caso el denunciante– y no de ellas directamente. Más concretamente, indica que "... el empleado en cuestión deberá ser informado de: [1] la entidad responsable del programa de denuncia de irregularidades, [2] los hechos de los que se le acusa, [3] los departamentos y servicios que podrían recibir el informe dentro de su propia sociedad o en otras entidades o sociedades del grupo del que forma parte su sociedad, y [4] cómo ejercer sus derechos de acceso y rectificación". Así mismo consideró que bajo ninguna circunstancia la persona acusada en el informe de denuncia de irregularidades podrá obtener información sobre la identidad del denunciante por parte del programa

---

<sup>341</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1226.

<sup>342</sup>El artículo 11 de la Directiva 95/46/CE en relación con la información cuando los datos no han sido recabados del propio interesado establece que los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello:

a) la identidad del responsable del tratamiento y, en su caso, de su representante;

b) los fines del tratamiento de que van a ser objeto los datos;

c) cualquier otra información tal como: 1) las categorías de los datos de que se trate, 2) los destinatarios o las categorías de destinatarios de los datos, 3) la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

basándose en el ejercicio de su derecho de acceso, salvo cuando el denunciante realice una manifestación falsa de mala fe; en cualquier otro caso, siempre se respetará la confidencialidad del denunciante<sup>343</sup>.

Para las medidas de seguridad el Dictamen se remite directamente a los reglamentos de seguridad establecidos en los diferentes Estados miembros, indicando que se deberán tomar todas las precauciones técnicas con el fin de garantizar la seguridad de los datos en el momento de su recopilación, circulación y conservación, y subrayando la exigencia de la confidencialidad de los informes realizados en los programas.

Merece también la pena mencionar de manera brevísima la importancia en cuanto a la regulación de los instrumentos de whistleblowing en Europa, de la Recomendación de la Comisión de 15 de febrero de 2005, relativa al papel de los administradores no ejecutivos o supervisores y al de los comités de consejos de administración o de supervisión, aplicables a las empresas que cotizan en bolsa. Este texto establece que el comité de auditoría (anexo 1, apartado 4.3) *"debe controlar el procedimiento en virtud del cual la empresa se atiene a las disposiciones en vigor relativas a la posibilidad de que los empleados señalen las irregularidades importantes que consideren se han podido cometer en la empresa presentando una reclamación o una denuncia anónima, normalmente a un administrador independiente, y garantizar que disponga lo necesario para una investigación proporcionada e independiente a este respecto, seguida de una actuación apropiada"*.<sup>344</sup>

Además de las anteriores iniciativas, como consecuencia de la grave crisis financiera que hemos atravesado, la figura del whistleblowing ha comenzado a regularse de manera explícita en el ámbito de los mercados de valores. En concreto en el Reglamento (UE) nº 596/2014 del Parlamento Europeo y del Consejo, de 16 de abril, sobre el abuso de mercado (Reglamento sobre

---

<sup>343</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., pp. 1226-1227.

<sup>344</sup>Publicado en el Diario Oficial de la Unión Europea de 15/02/2005.

abuso de mercado) y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión.

El Reglamento (UE) nº 596/2014 del Parlamento Europeo y del Consejo sobre abuso de Mercado entró en vigor el 2 de julio de 2014 y regula la comunicación de las infracciones en su artículo 32 en donde se establece que los Estados miembros velarán por que las autoridades competentes establezcan mecanismos eficaces para permitir la comunicación de posibles infracciones o infracciones reales del Reglamento a las autoridades competentes. Dichos mecanismos deben incluir al menos lo siguiente:

- a) procedimientos específicos para la recepción de comunicaciones de infracciones y su seguimiento, incluido el establecimiento de canales de comunicación seguros para tales comunicaciones de infracciones;
- b) en el marco de su actividad laboral, la protección adecuada de las personas que trabajen en virtud de un contrato de trabajo que comuniquen infracciones o sean acusadas de cometerlas, frente a represalias, discriminación u otros tipos de trato injusto;
- c) la protección de los datos personales tanto de la persona que comunique la infracción como de la persona física presuntamente responsable de su comisión, incluida la protección en relación con la preservación de la confidencialidad de su identidad, en todas las fases del procedimiento, sin perjuicio de que dicha información tenga que ser comunicada en virtud de la normativa nacional, en el marco de investigaciones o procedimientos judiciales posteriores.

El artículo 32 además dispone que los Estados miembros exigirán a los empleadores dedicados a actividades reguladas de servicios financieros que dispongan de procedimientos internos adecuados para que sus empleados puedan notificar las infracciones del presente Reglamento y señala que los

Estados miembros podrán prever, de acuerdo con la normativa nacional aplicable, la concesión de incentivos económicos a las personas que ofrezcan información relevante sobre posibles infracciones del citado Reglamento, siempre que esas personas no estén sometidas a otras obligaciones legales o contractuales previas de facilitar tal información, que esta sea nueva y que dé lugar a la imposición de una sanción administrativa o penal, o a la adopción de otra medida administrativa por infracción del citado Reglamento.

En el Reglamento (UE) nº 596/2014 también se establece que la Comisión adoptará actos de ejecución en los que se especifiquen los procedimientos mencionados anteriormente, incluidas las disposiciones para comunicar infracciones y para el seguimiento de estas, y las medidas de protección de las personas que trabajen en virtud de un contrato de trabajo, así como las medidas de protección de los datos personales. Recordemos que los Reglamentos emitidos por la Unión son de la aplicación directa en los Estados miembros.

En este sentido también es necesario mencionar la citada Directiva 2014/65/ del Parlamento Europeo y del Consejo de 15 de mayo de 2014 relativa a los mercados de instrumentos financieros, conocida como MIFID II y al Reglamento 600/2014, que la acompaña, constituyendo de manera conjunta el marco jurídico que regula los requisitos aplicables a las empresas de servicios de inversión, a los mercados regulados y a los prestadores de servicio de suministro de datos. En el artículo 73 también se señala que los Estados miembros velarán por que las autoridades competentes establezcan mecanismos eficaces para posibilitar la notificación a estas autoridades de las infracciones potenciales o efectivas de las disposiciones del Reglamento (UE) no 600/2014 y de las disposiciones nacionales adoptadas en aplicación de la Directiva y prevé unos requisitos prácticamente idénticos a los del Reglamento 596/2014 para dichos mecanismos.

Por último destacar que la Directiva señala como obligación a los Estados miembros la de exigir a las empresas de servicios de inversión, organismos rectores del mercado, proveedores de servicios de suministro de datos, entidades de crédito en relación con servicios o actividades de inversión o con actividades y servicios auxiliares y sucursales de empresas de terceros países que dispongan de procedimientos adecuados para que sus empleados puedan notificar infracciones potenciales o efectivas a nivel interno a través de un canal específico, independiente y autónomo.

### **2.3.2 Normativa en el Reino Unido: la Public Interest Disclosure Act**

La regulación anglosajona del Reino Unido entiende de otra manera la figura del *whistleblowing*. A continuación se analizará la legislación que regula dicha materia incluyendo sus principales características.

La *Public Interest Disclosure Act 1998*, Ley de revelación de información de Interés Público (PIDA) fue aprobada el 2 de julio de 1998, entrando en vigor un año después, el 2 de julio de 1999, siendo de aplicación en Inglaterra, Escocia y Gales. Dicha ley ha sido modificada en dos ocasiones, por un lado por la Ley de Relaciones Laborales de 1999 y por otro por la Ley de Reforma de la Policía de 2002.

Como consecuencia de varios desastres y tragedias ocurridos a finales de los años 80, surgió en el Reino Unido la necesidad de legislar el *whistleblowing*, puesto que los trabajadores de las organizaciones afectadas por fraude o malas prácticas no encontraron la confianza suficiente para revelar la información, o bien no se les escuchó<sup>345</sup>.

La sociedad impulsó la búsqueda de soluciones a dicha situación. Se creó en 1995 una Comisión Parlamentaria denominada *Committee on Standards in Public Life* (Comisión sobre Normas en la Actividad Pública, CSPL) que se

---

<sup>345</sup>MYERS, A., "Whistleblowing- The UK Experience", en AA.VV., *Whistleblowing Around The World: Law, Culture and Practice*, dirs. R. Calland y G. Dehn, London, 2004, pp. 101-103.

encargaba de examinar la conducta de personas en puestos oficiales y de los organismos públicos en general. La CSPL estudió los efectos de la cultura del silencio en el sector público respaldando la postura de la sociedad sobre el establecimiento de mecanismos de *whistleblowing* y en especial de las formas de revelar información sobre riesgos o malas prácticas en el interior de las organizaciones. Esta Comisión a su vez creó unas directrices para establecer dichos mecanismos, los cuales actualmente se consideran los elementos esenciales del sistema interno de denuncias del Reino Unido<sup>346</sup>. La PIDA siguiendo la línea de la CSPL proponía sistemas de denuncia o revelación de información, que si bien no disponía obligaciones expresas para los órganos u organizaciones de establecer dichos sistemas internos, otorgaba el derecho a los denunciantes de llevar el asunto a instancias externas con potenciales consecuencias no favorables para el empleador o entidad afectada<sup>347</sup>.

La PIDA se centra en la revelación y no en la persona que la efectúa al contrario de la regulación existente en Estados Unidos, que se centra en la situación particular de la persona del denunciante, no estableciendo protecciones especiales más allá del derecho a una compensación económica en razón del detrimento sufrido a causa de represalias<sup>348</sup>.

La PIDA se trata de una legislación de carácter laboral incluida en la *Employment Rights Act* (Ley de derechos del Empleo del Reino Unido, ERA). La PIDA forma parte de la ERA y por tanto su aplicación corresponde a situaciones incluidas en el marco de una relación de trabajo. Sin embargo, un elemento distintivo de esta legislación es su amplio marco de aplicación, en el sentido de que comprende las revelaciones y la protección contra represalias para trabajadores del sector público y privado, entendiéndose el término

---

<sup>346</sup>MYERS, A., "Whistleblowing...", ob. cit., p. 105.

<sup>347</sup>DREW, K., "Whistleblowing and Corruption", *An Initial and Comparative Review*. Public Services International Research Unit, University of Greenwich, London, 2003, p. 54.

<sup>348</sup>Public Service Integrity Office (Canada), "A Comparative International Analysis of Regimes for the Disclosure of Wrongdoing ("*Whistleblowing*")", Gobierno de Canadá, 2004, p. 25.

“trabajadores” en un sentido muy amplio, cubriendo prácticamente todas las situaciones de empleo<sup>349</sup>. Considero importante destacar el fuerte componente de la cobertura dual de la PIDA (sector público y privado) en el sistema de revelaciones del Reino Unido, pues demuestra que todos los trabajadores son iguales merecedores de protecciones contra represalias<sup>350</sup>.

De acuerdo con la PIDA, se considerará revelación protegida cualquier información que el trabajador considere que refleja alguna de las siguientes acciones<sup>351</sup>: 1) la comisión de una ofensa criminal; 2) el incumplimiento de una obligación legal (entendiendo dicha obligación en su sentido amplio de obligación jurídica, incluyendo también aquellas obligaciones que devienen de una ley); 3) un error judicial; 4) una amenaza contra la salud o seguridad de cualquier individuo (independientemente de que se trate o no del trabajador que realiza la denuncia); 5) deterioro del medio ambiente y 6) ocultación deliberada de información que pueda llevar a demostrar alguno de los puntos anteriores.

En todos los casos el hecho puede ser pasado, presente o que exista probabilidad de que ocurra en un futuro. En cualquier caso, estos seis puntos podrían superponerse entre sí y darse simultáneamente.

Se considerará protegida a la revelación que cumpla determinados criterios, como por ejemplo que se realice de buena fe<sup>352</sup> y en la creencia de certeza

---

<sup>349</sup>Public Concern At Work, Nota Explicativa a la sección 43A ERA, Employment Rights Act (Ley de derechos del Empleo).

<sup>350</sup>Public Service Integrity Office (Canada), A Comparative International Analysis of Regimes for the Disclosure of Wrongdoing (“Whistleblowing”), Gobierno de Canadá, 2004, p. 26.

<sup>351</sup>Public Concern At Work, Nota Explicativa ERA sección 43B (1) Employment Rights Act (Ley de derechos del Empleo).

<sup>352</sup>Public Concern At Work, Nota Explicativa ERA secciones 43C y 43E a 43H. Employment Rights Act (Ley de derechos del Empleo).

sobre dicha información<sup>353</sup>, y además debe tratar sobre las materias específicas establecidas en la Ley.

Con el fin de determinar la relevancia de la información facilitada, el tribunal deberá tener en consideración aspectos como la identidad del informante, su nivel de preocupación y si dicha mala práctica denunciada ha finalizado o continúa existiendo<sup>354</sup>. Con respecto a “creencia razonable” entendemos que no tiene por qué ser necesariamente cierta, sino que el empleado cree que lo es y le parece posible; de modo que la revelación se puede calificar como protegida incluso si el trabajador, de forma equivocada, cree en la existencia de una mala práctica.

La actuación de buena fe implica que la información se revele de forma sincera, aun cuando se haga de forma negligente. En el caso de que pudiera demostrarse que dicha información se revela con un propósito posterior deshonesto, los Tribunales estimarán que ha habido mala fe.

La PIDA también tiene en cuenta elementos adicionales respecto de las revelaciones de información; así, considera irrelevante el hecho de que dicha información esté o no en poder del receptor de la misma; también considera irrelevante que dicha conducta se produzca dentro o fuera del Reino Unido.

El único caso en que la revelación quedaría sin protección que exceptúa la ley se da en el supuesto en que dicha información se haya obtenido bajo secreto profesional. No obstante, la revelación sí estaría protegida en el caso de que se hubiera obtenido mediante un asesoramiento legal.

En caso de que la persona actuara ilegalmente para obtener información, la revelación de la misma no estará protegida, por ejemplo en el caso de la

---

<sup>353</sup>Employment Rights Act (Ley de derechos del Empleado).ERA sección 43B; Public Service Integrity Office (Canada), ob. cit., p. 27.

<sup>354</sup>MYERS, A., “Whistleblowing...”, ob. cit., p. 109.



Official Secrets Act (Ley de Secretos Oficiales). Sin embargo, hay que destacar que sólo la Official Secrets Act prevalece sobre la PIDA.

El sistema de procedimientos de revelación de la PIDA establece niveles escalonados en cuanto a la posibilidad de revelar. Los niveles identifican de forma creciente a las personas o entidades ante las cuales se puede efectuar la revelación y coinciden con distintas categorías de revelación, según la fuerza de la prueba del denunciante respecto a la información y a la seriedad o gravedad de la misma<sup>355</sup>.

El trabajador que denuncia es libre de decidir en cuál de los niveles efectúa la revelación. No se requiere que el trabajador necesariamente haya presentado la denuncia internamente, previo a acceder a los niveles superiores<sup>356</sup>. La revelación se considerará protegida, en cada caso, si cumple con los criterios de cada nivel. El sistema escalonado va aumentando la carga de la prueba del trabajador, a medida que se le va otorgando un derecho de revelación más amplio con cada nivel superior, siguiendo la lógica de que las denuncias deberían poder resolverse perfectamente internamente.

Existen niveles de revelación que se describen a continuación<sup>357</sup>:

- I. Revelaciones internas: el trabajador debe acudir en primer lugar ante su propio empleador o ante alguna otra persona responsable dentro de la organización<sup>358</sup>. En este nivel, la

---

<sup>355</sup>Public Service Integrity Office (Canada), A Comparative International Analysis of Regimes for the Disclosure of Wrongdoing ("Whistleblowing"), Gobierno de Canadá, 2004, p. 28. ROHDE-LIEBENAU, B., "Whistleblowers Rules: Best practice. Assessment and Revision of rules existing in EU Institutions", Estudio solicitado por el Parlamento de la Unión Europea, Comisión de Control Presupuestario, Bruselas, 2006, p. 28 (extraído de <http://www.europarl.europa.eu/document/activities/cont/200907/20090728ATT59162/20090728ATT59162EN.pdf>).

<sup>356</sup>MYERS, A., "Whistleblowing...", ob. cit., p. 108.

<sup>357</sup>ROHDE-LIEBENAU, B., "Whistleblowers Rules...", ob. cit., pp. 28-29 (extraído de <http://www.europarl.europa.eu/document/activities/cont/200907/20090728ATT59162/20090728ATT59162EN.pdf>).

<sup>358</sup>Public Concern At Work, Nota Explicativa ERA sección 43C Employment Rights Act (Ley de derechos del Empleo). Los Trabajadores de órganos de Gobierno pueden efectuar la revelación protegida, en forma alternativa y equivalente al empleador directo, al Departamento de Estado

revelación se considera protegida si el trabajador de buena fe revela información que en su propia creencia razonable tiende a mostrar una o más de las conductas denunciables<sup>359</sup>.

II. Revelaciones regulatorias: el trabajador puede acudir ante algún órgano o autoridad externa designada para ello como un Secretario de Estado, o un órgano regulatorio del sector o actividad respectiva<sup>360</sup>. El trabajador tiene que tenerla creencia razonable de que la información relevante recae dentro de la descripción de las materias para las cuales la persona o entidad ha sido especialmente designada y que la información revelada y cualquier alegación contenida en ella son sustancialmente verdaderas<sup>361</sup>.

III. Revelaciones amplias: el trabajador puede acudir a otras personas o entidades, tales como la policía, los miembros del Parlamento o incluso los medios de comunicación. No podrá efectuar una revelación para propósitos de beneficio personal y ésta debe serle razonable y conforme a las circunstancias del caso<sup>362</sup>.

---

respectivo (al Ministro de la Corona o las personas por él designadas), aunque esta revelación no se considerará como efectuada al empleador para los propósitos de una revelación amplia posterior (sección 43E). Aunque no se le imponen deberes al Ministro responsable para manejar la revelación, la disposición tiende a fortalecer la rendición de cuentas de los Ministros por la conducta de los órganos de los que son responsables.

<sup>359</sup>Public Concern At Work, Nota Explicativa ERA sección 43B (1). Employment Rights Act (Ley de derechos del Empleo).

<sup>360</sup>Public Concern At Work, Ob. Cit., nota explicativa sección 43F. Estas personas- llamadas generalmente reguladores-son designadas por el Secretario de Estado en el área de comercio o industria relevante.

<sup>361</sup>ERA sección 43F (1). Este requisito implica una carga de la prueba más fuerte para el trabajador; requiere de cierta evidencia fáctica para sustanciar la revelación. Aun así el trabajador no perderá su protección si su creencia finalmente resulta errada.

<sup>362</sup>Public Concern At Work, Ob. Cit., nota explicativa sección 43F (1) (c). MYERS, A., "Whistleblowing...", ob. cit., pp. 108 – 109.

Adicionalmente la revelación debe cumplir con alguna de las siguientes condiciones: a) creencia razonable del trabajador de que sería victimizado si denunciara el asunto internamente o ante un órgano regulador prescrito en la Ley; o b) inexistencia de un órgano regulador recogido en la Ley y la creencia razonable de que la evidencia probablemente sería ocultada o destruida si se efectuara la revelación ante el empleador; o c) que el trabajador haya efectuado previamente la misma revelación ante el empleador o ante la entidad regulatoria pertinente.

Para determinar la razonabilidad de efectuar la revelación en este nivel, se tendrá particularmente en consideración<sup>363</sup>: a) la identidad de la persona; b) que la falta sea relevante; c) que la falta persista o pueda ocurrir en el futuro; d) si la revelación es efectuada con infracción al deber de confidencialidad hacia el empleador o hacia cualquier otra persona; e) si se hubiera efectuado previamente la revelación interna ante el empleador o la revelación regulatoria, cualquier acción que el empleador o el regulador haya tomado o pudiera razonablemente haber tomado como resultado de la revelación previa; f) en el caso de que previamente se hubiera efectuado la revelación interna ante el empleador, si el trabajador ha cumplido con cualquier procedimiento cuya utilización le haya sido autorizada por el empleador.

IV. Revelaciones de asuntos excepcionales graves: Además de las categorías descritas se puede identificar una cuarta categoría de “revelaciones de asuntos excepcionalmente graves” que se calificarán como protegidas aún si no cumplen los requisitos de “las revelaciones amplias” pero que deben reunir las siguientes condiciones<sup>364</sup>: a) buena fe del trabajador; b) creencia razonable del trabajador de que la información revelada y cualquier alegación contenida en ella es sustancialmente verdadera; c) que

---

<sup>363</sup>Public Concern At Work, Nota Explicativa ERA Sección 43G (3).

<sup>364</sup>Public Concern At Work, Nota Explicativa ERA Sección 43H

se efectúe la revelación para propósitos de beneficio personal; d) que sea de naturaleza excepcionalmente seria; e) que en las circunstancias del caso sea razonable para el trabajador el efectuar la revelación

Para determinar si es razonable para el trabajador el efectuar la revelación, se tendrá en cuenta la identidad de la persona ante la que se efectúa.

Pueden existir dentro de la empresa diversos procedimientos de *whistleblowing*. Dado que la complejidad de los procedimientos se puede considerar como una limitación a los denunciantes, se ha destacado las posibilidades con que cuenta el trabajador con un fuerte incentivo para el establecimiento de procedimientos adecuados de *whistleblowing* en el interior de las organizaciones. La PIDA no impone a los empleadores u organizaciones el requerimiento de establecer ningún mecanismo interno de denuncias, -tampoco se establecen protecciones especiales para el denunciante, ni sanciones legales a las represalias-, pero en cierta forma y automáticamente la fuerza de esta Ley o del sistema contenido en ella, implica que si la organización no puede abordar eficaz y responsablemente una revelación seria y sustentada por la vía interna, el trabajador tendrá la posibilidad de recurrir al *whistleblowing* externo.

Esto puede llevar a consecuencias altamente indeseables para el empleador u organización, que se expone a la expansión del daño a instancias más públicas y al pago de reparaciones e indemnizaciones. Por tanto, es del propio interés de la organización, y no un requerimiento especial de la legislación, el establecer mecanismos que permitan manejar y resolver las inquietudes o revelaciones presentadas por sus propios trabajadores. La administración luego es libre de escoger soluciones para que el proceso comunicativo se ajuste a su situación<sup>365</sup>.

---

<sup>365</sup>ROHDE-LIEBENAU, B., "Whistleblowers Rules...", ob. cit., p. 29, con referencia al Anexo IV.

Además de las regulaciones de la PIDA existe el *Civil Service Code* (Código del Servicio Civil) que establece normas específicas para los trabajadores del sector público con respecto a las conductas denunciables, las revelaciones y la protección de los mismos ante las consecuencias de dicha revelación.

Por último mencionar, aunque queda fuera de este estudio, la UK Bribery Act<sup>366</sup> británica, que entró en vigor el 1 de julio del año 2011, es la ley anticorrupción por excelencia, superando a la FCPA norteamericana. Introduce nuevos aspectos corporativos para prevenir el cohecho y el soborno, respecto a un trabajador o directivo que tenga relación directa o indirecta con la empresa. La ley prohíbe ofrecer, entregar, solicitar, recibir o aceptar favores o dinero que produzca una ventaja frente al resto de los competidores<sup>367</sup>. La Bribery Act, a diferencia de la FCPA<sup>368</sup>, establece una pena de prisión similar para las empresas que violen la norma y, respecto a las personas físicas, una pena de prisión de 10 años y una pena de multa económica ilimitada.

### **2.3.3 Referencia a Francia (Especial referencia a la *Commission Nationale de l'informatique des libertés*)**

La *Commission Nationale de l'informatique e des libertés* (CNIL) regula la figura del whistleblowing en el seno de las empresas que operan exclusivamente en Francia. Los canales de denuncia están restringidos a los casos de contabilidad fraudulenta, auditoría, irregularidades financieras y prácticas de corrupción como sobornos y conflictos de interés. La denuncia debe realizarse a través de los canales establecidos por la CNIL<sup>369</sup>.

---

<sup>366</sup><http://www.transparency.org.uk/our-work/bribery-act>.

<sup>367</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1216.

<sup>368</sup>FOX, T., *Best Practices Under the FCPA and Bribery Act*, 2013.

<sup>369</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1237.

### 2.3.4 Alemania

En Alemania estos sistemas se han extendido a raíz de ciertas previsiones legales. El § 91.2 de la Aktiengesetz impone a los consejos de administración el deber de introducir medidas adecuadas, en especial un sistema de vigilancia, para advertir lo antes posible los riesgos que amenacen la continuidad de la compañía<sup>370</sup>. Otra de las razones fundamentales para su implantación como elemento habitual de los “programas de cumplimiento normativo” es el § 130 de la Ley de Contravenciones (OWiG) que sanciona la infracción de deberes de vigilancia en el marco de la actividad empresarial<sup>371</sup>. Ninguno de estos preceptos impone necesariamente la implantación de un sistema de whistleblowing interno, pero la práctica ha propiciado la proliferación de tales sistemas en las empresas alemanas<sup>372</sup>.

## 3. El whistleblowing en el ordenamiento jurídico español

### 3.1 Consideraciones generales

El ordenamiento jurídico Español no cuenta con una norma que de manera general regule la figura del whistleblower o la obligación de las empresas de implantar un canal de denuncias sino que dicha obligación se encuentra regulada de manera sectorial, como a continuación analizaremos.

---

<sup>370</sup>Con todo, según datos citados por LUTTERBACH, C., “Die Strafrechtliche Würdigung des Whistleblowings”, disertación (tesis doctoral) defendida en la Facultad de Derecho de la Universidad de Bremen (Alemania), el 27 de julio de 2011. Extraído de: <http://elib.suub.uni-bremen.de/edocs/00102123-1.pdf>, p. 47, solo un 34% de las empresas alemanas de más de mil trabajadores cuentan con tales sistemas, mientras que a nivel mundial el porcentaje es del 60%.

<sup>371</sup>BOCK, D., “Strafrechtliche Aspekte der Compliance-Diskussion – § 130 OWiG als zentrale Norm der Criminal Compliance”, ZfS, nº 2, 2009, pp. 68-81 (esp. p. 79).

<sup>372</sup>STRACK, “Whistleblowing in Germany”, p. 5. Sobre la expansión del fenómeno en Alemania cfr. KOCH, ZfS 10/2008, pp. 501-502 Y LUTTERBACH, C. “Die strafrechtliche Würdigung...”, ob. cit., pp. 21 ss.

## **3.2 En la actividad empresarial**

### **3.2.1 La legislación penal**

La LO 5/2010 de reforma del Código Penal, que entró en vigor el 23 de diciembre de 2010, introdujo en la legislación penal española una de las modificaciones más sustanciales en el derecho penal empresarial desde la aprobación del Código Penal de 1995.

La modificación legal más relevante consistió en la abolición de nuestro ordenamiento jurídico penal del viejo aforismo romano *societas delinquere non potest*, según el cual una persona jurídica no podía cometer delitos. Con ello, la reforma convierte a las personas jurídicas en sujetos inmediatos del Derecho Penal susceptibles de cometer delitos, al margen de las concretas personas físicas que las integren, y de ser por ello sancionadas con auténticas penas.

Otros países habían optado por esta fórmula con anterioridad, como Inglaterra, Estados Unidos, Japón, Holanda, Noruega o Francia. En la Exposición de Motivos de la Ley española, sin embargo, no se encontraron motivos o razones de política criminal que aconsejaran esa decisión de incluir en el Código Penal un modelo de responsabilidad criminal de las personas jurídicas. Tal decisión, según dicha Exposición, parecía haber sido tomada por la necesidad de cumplir con las obligaciones derivadas de los tratados internacionales y del denominado Derecho Penal de la Unión Europea. Así, países como Alemania o Italia habían agravado el ámbito de las contravenciones, pero sin salirse del ámbito del Derecho administrativo sancionador.

La Ley española puede tener su fuente de inspiración en los siguientes antecedentes, instrumentos de política criminal internacional: la Recomendación 18/88, de 20 de octubre, del Comité de Ministros de los Estados Miembros del Consejo de Europa; la Convención de Bruselas de 26

de mayo de 1997 sobre la lucha contra la corrupción en el ámbito de la función pública de la Unión Europea; la Convención de Nueva York de 9 de diciembre de 1999 sobre terrorismo; la Decisión Marco 2002/629/JAI del Consejo, actualmente sustituida por la Directiva 2011/36/UE del Parlamento Europeo y del Consejo de 5 de abril de 2011, relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas; la Directiva 2008/99/CE del Parlamento Europeo y del Consejo de 19 de noviembre de 2008 relativa a la protección del medio ambiente mediante el Derecho Penal, y las Decisiones Marco de la Unión Europea 2005/222 sobre ataques a los sistemas informáticos, 2004/757 sobre punición del tráfico de drogas, la Decisión Marco sobre explotación sexual y pornografía infantil y el Convenio de Cibercriminalidad de Budapest de 23 de noviembre de 2001, entre otras, además de la Convención y los Protocolos de Naciones Unidas contra el crimen organizado transnacional y las propuestas del corpus iuris de disposiciones penales para la protección de los intereses financieros en la Unión Europea<sup>373</sup>.

La responsabilidad penal de las personas jurídicas se introdujo en nuestro ordenamiento jurídico por medio de una doble vía de imputación según se tratara de delitos cometidos por (i) el representante legal, administrador de hecho o de derecho de la entidad, o (ii) de los actos delictivos realizados por las personas sometidas a la autoridad de los anteriores por un defecto del debido control por parte de tales representantes legales, administradores de hecho o de derecho. De un modelo basado en el principio *societas delinquere non potest* se pasó a otro en el que, a partir de un sistema mixto de imputación, se asume la responsabilidad penal de determinadas entidades con personalidad jurídica y por consiguiente, la posibilidad de imponerles sanciones penales.

---

<sup>373</sup>ALONSO DE ESCAMILLA, A., "La responsabilidad penal de los administradores de sociedades mercantiles. Una aproximación desde la perspectiva del compliance", en AA.VV., *Gobierno corporativo: la estructura del órgano de gobierno y la responsabilidad de los administradores. Adaptado a la Ley 31/2014, de 3 de diciembre*, dir. A. Martínez-Echevarría, Pamplona, 2015, pp. 881-882.



En la Exposición de Motivos de la LO 5/2010 se afirma haber optado por esta doble vía de imputación mediante la atribución de responsabilidad por la actuación delictiva del “*representante legal, administrador de hecho o de derecho*” por actos realizados “*en nombre o por cuenta de la persona jurídica y en su provecho*”; y asimismo, se establece la transferencia de responsabilidad por un defecto del debido control o “*culpabilidad de organización*” en el que se sanciona a la persona jurídica por los delitos cometidos por las personas que estén sometidas a la autoridad de los anteriores siempre que hayan podido realizar su acción “*por no haberse ejercido sobre ellos el debido control, atendiendo las circunstancias de cada caso*”. En todo caso, se exige la existencia de un hecho punible como presupuesto habilitante para que pueda surgir la responsabilidad penal de las personas jurídicas. Ahora bien, para poder apreciar una posible responsabilidad penal de las personas jurídicas se hace necesario realizar una interpretación de dicho precepto penal a fin de determinar su alcance, requisitos y presupuestos de aplicación. Sin embargo, esta redacción presentó para los Tribunales una parquedad en su regulación, a diferencia de la redacción impuesta por la modificación de 2015.

De conformidad con lo establecido en la Circular 1/2011 relativa a la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por LO 5/2010, la responsabilidad de la persona jurídica sería consecuencia de un funcionamiento defectuoso o de una mala organización de la misma. Esta interpretación no aparece recogida de manera expresa en el artículo 31 bis del Código Penal en su redacción original, y han sido nuestros tribunales quienes han interpretado la “*falta de debido control*” en este sentido. De hecho, una de las razones que motivaron la reforma operada por la LO 1/2015 fue la imprecisión y vaguedad con que algunos aspectos de la responsabilidad penal de las personas jurídicas aparecía definida en la redacción original del artículo 31 bis del Código Penal.

La LO 5/2010 introdujo por primera vez la referencia a una política corporativa criminal o una mala organización de la empresa, como criterios determinantes de la responsabilidad penal de las personas jurídicas.

La Circular 1/2011 la elaboración y el cumplimiento de las normas de autorregulación o *compliance guide* resultan relevantes en la medida en que respondan a la necesidad de adoptar un modelo de organización cuya observancia exonere de responsabilidad a la persona jurídica por los delitos cometidos por las personas físicas en el seno de la sociedad.

Su formalización no aporta ni su inexistencia resta la capacidad potencial de incurrir en responsabilidad penal, porque lo determinante no es si se actuó de acuerdo con la guía o si esta era hipotética u objetivamente apta para evitar el delito, sino si con guía o sin ella, procede atribuir a la persona jurídica la responsabilidad penal derivada de los delitos cometidos por sus gestores, por haber tenido lugar dichas conductas ilícitas cuando los mismos actuaban en nombre, por cuenta y en provecho de la entidad, o como consecuencia de haber omitido aquellos el debido control sobre sus subordinados jerárquicos en el ejercicio de actividades sociales y por cuenta y en provecho de la entidad.

El anterior modelo de responsabilidad penal de las personas jurídicas ha sido modificado por la LO 1/2015 dotando a artículo 31 bis del CP de la siguiente redacción:

*“1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables:*

*a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la*

*persona jurídica u ostentan facultades de organización y control dentro de la misma.*

*b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.*

*2. Si el delito fuere cometido por las personas indicadas en la letra a) del apartado anterior, la persona jurídica quedará exenta de responsabilidad si se cumplen las siguientes condiciones:*

*1ª el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión;*

*2ª la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica;*

*3ª los autores individuales han cometido el delito eludiendo fraudulentamente los modelos de organización y de prevención y*

*4ª no se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2ª.*

*En los casos en los que las anteriores circunstancias solamente puedan ser objeto de acreditación parcial, esta circunstancia será valorada a los efectos de atenuación de la pena.*

*3. En las personas jurídicas de pequeñas dimensiones, las funciones de supervisión a que se refiere la condición 2.<sup>a</sup> del apartado 2 podrán ser asumidas directamente por el órgano de administración. A estos efectos, son personas jurídicas de pequeñas dimensiones aquellas que, según la legislación aplicable, estén autorizadas a presentar cuenta de pérdidas y ganancias abreviada.*

*4. Si el delito fuera cometido por las personas indicadas en la letra b) del apartado 1, la persona jurídica quedará exenta de responsabilidad si, antes de la comisión del delito, ha adoptado y ejecutado eficazmente un modelo de organización y gestión que resulte adecuado para prevenir delitos de la naturaleza del que fue cometido o para reducir de forma significativa el riesgo de su comisión.*

*En este caso resultará igualmente aplicable la atenuación prevista en el párrafo segundo del apartado 2 de este artículo.*

*5. Los modelos de organización y gestión a que se refieren la condición 1.<sup>a</sup> del apartado 2 y el apartado anterior deberán cumplir los siguientes requisitos:*

*1º Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.*

*2º Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.*

*3º Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.*

*4º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.*

*5º Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.*

*6º Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.*

De acuerdo con la nueva reforma, la adopción de un modelo de prevención de riesgos podría considerarse como una medida atenuante o eximente si cumple con los requisitos adecuados y es que la LO 1/2015 supuso la incorporación de requisitos y condiciones que deben cumplir los modelos de organización a los efectos de exonerar de responsabilidad penal a las personas jurídicas.

Haciendo un estudio conjunto del apartado 5 del artículo 31 bis y de la "Circular 1/2016 sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por LO 1/2015" publicado por la Fiscalía General del Estado<sup>374</sup>, podemos analizar cada uno de los requisitos que deben contener los modelos de organización y gestión a los efectos de poner exonerar de responsabilidad penal a las personas jurídicas siempre que se ajusten a la normativa. Estos requisitos son las siguientes:

---

<sup>374</sup>Disponible en <https://www.fiscal.es>

1º. Identificación de las actividades en que se ha cometido el delito como actividad susceptible de prevención. La persona jurídica debe identificar y controlar los riesgos reales y potenciales derivados de sus actividades, teniendo en cuenta variables como la relación del negocio, el volumen de sus operaciones, la duración, los indicadores de riesgo interno o externo, el entorno, los empleados o los procesos de trabajo internos.

2º. Establecimiento de protocolos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas. Tales procedimientos deben garantizar altos estándares éticos así como la obligación de atender a los criterios de idoneidad fijados por la normativa sectorial. Se trata de documentar todos los trámites internos seguidos en los procedimientos de preparación, discusión y toma de acuerdos societarios.

3º. Disponer de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos. Deberán contener la dotación de medios, la información y la formación necesarias.

4º. Imponer la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención. Debe posibilitar la detección de conductas criminales, a través de canales de denuncia de incumplimiento internos o de actividades ilícitas de la empresa. Para ello es imprescindible que la entidad cuente con una regulación protectora específica del denunciante (*whistleblower*), con el objeto de facilitar la confidencialidad y sin riesgo de sufrir represalias.

5º. Establecer un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo. Este requisito se refiere a la necesidad de implantar un catálogo de sanciones internas que afecten tanto a empleados como a directivos.

6º. Realizar una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios. Aunque el texto no establece plazo ni procedimiento alguno de revisión, un adecuado modelo de organización debe contemplarlos expresamente. Además el modelo deberá ser revisado inmediatamente si concurren determinadas circunstancias que puedan influir en el análisis de riesgo, que habrán de detallarse y que incluirán, además, otras situaciones que alteren significativamente el perfil de riesgo de la persona jurídica.

Por último destacar que la Circular 1/2016 proporciona unas pautas de carácter general para valorar la adecuación y eficacia de los modelos de organización y gestión, estableciendo que deberán estar redactados por escrito, ser claros, precisos y eficaces así como perfectamente adaptados a la empresa y a sus riesgos. Configura por otra parte, la presunción de que el programa no resulta eficaz si un alto responsable de la compañía participó, consintió o toleró el delito. De esta forma viene a exigirse en cierta medida: (i) una valoración de las circunstancias concretas del caso tales como la gravedad de la conducta, el número de empleados implicados y la duración de la actividad criminal; (ii) una valoración del comportamiento de la compañía en relación con anteriores conductas; (iii) una valoración de la existencia de anteriores procedimientos penales o en trámite o sanciones administrativas; y (iv) una valoración de la concreta actuación tras la comisión del delito.

La STS 154/2016, de 29 de febrero, profundiza en el fundamento material de la responsabilidad penal de la persona jurídica introduciendo el concepto de imputabilidad empresarial, con la consiguiente distinción de las personas jurídicas imputables e imputables, de tal manera que solo serán penalmente responsables aquellas personas jurídicas que tengan un sustrato material suficiente. Y en estos términos, se pronuncia la Circular 1/2016 reconociendo

tres categorías de persona jurídica desde el punto de vista de su responsabilidad organizativa:

- (i) Las sociedades que operan con normalidad en el mercado y a las que se dirigen las disposiciones sobre los modelos de organización y gestión de los apartados 2 a 5 del artículo 31 bis del nuevo Código Penal.
- (ii) Las sociedades que desarrollan una cierta actividad, en su mayor parte ilegal, como son las utilizadas habitualmente en esquemas de blanqueo de capitales o financiación del terrorismo.
- (iii) Las sociedades consideradas como personas jurídicas inimputables, aquellas cuyo *“carácter instrumental exceda del referido, es decir, que lo sean totalmente, sin ninguna otra clase de actividad legal o que lo sea solo meramente residual y aparente para los propios propósitos delictivos”*.

En definitiva, la LO 1/2015 no viene a instaurar un nuevo modelo de responsabilidad penal de las personas jurídicas sino que viene a matizar el modelo establecido en 2010 tratando de aclarar conceptos oscuros que podían dar lugar a una excesiva vaguedad (por ejemplo, la exigencia de *“en su provecho”* sustituida por la expresión de *“beneficio directo o indirecto”*) y, principalmente a determinar los requisitos exigidos en los programas de cumplimiento normativo a efectos de exonerar de responsabilidad penal a la persona jurídica.

Por último destacar que se puede exigir responsabilidad criminal a las personas jurídicas respecto de un número limitado de delitos, vinculados al Derecho penal económico y que están previstos en la parte especial del Código Penal. Se trata de las figuras delictivas que se recogen a continuación: a) tráfico ilegal de órganos humanos (artículo 156 bis); b) trata de seres humanos (artículo 177 bis); c) prostitución y corrupción de menores



(artículo 189 bis); d) descubrimiento y revelación de secretos (artículo 197); e) estafa (artículo 251); f) insolvencias punibles (artículo 261 bis); g) daños informáticos (artículo 264); h) delitos contra la propiedad intelectual, industrial, el mercado y los consumidores (artículo 288); i) blanqueo de capitales (artículo 302); j) delitos contra la Hacienda Pública y la Seguridad Social (artículo 310 bis); k) delitos contra los derechos de los ciudadanos extranjeros (artículo 318 bis); l) delitos urbanísticos (artículo 319); m) delitos contra los recursos naturales y el medio ambiente (artículos 327 y 328); n) delitos relativos a la energía natural y a las radiaciones ionizantes (artículo 343); ñ) delitos de riesgo provocado por explosivos (artículo 348); o) delitos contra la salud pública (artículo 369 bis); p) falsificación en medios de pago (artículo 399 bis); q) cohecho (artículo 427 bis); r) tráfico de influencias (artículo 430); s) corrupción de funcionarios públicos extranjeros e internacionales (artículo 445); t) delitos de terrorismo (artículos 570 quáter y 576).

Este sistema de *numerus clausus*, que no permite añadir ningún otro, plantea ausencias notables y sorprendentes, como son los delitos de corrupción entre particulares o los delitos contra los derechos de los trabajadores, o los llamados fraudes alimenticios o relativos a los medicamentos, entre otros. También resulta sorprendente y criticable que la cláusula de responsabilidad penal societaria abarque muy pocas modalidades de comisión imprudente. A la vista de todo ello, cabe afirmar que se pierde de nuevo la oportunidad de añadir un catálogo de delitos más coherente y que responda a la realidad de la actuación de las personas jurídicas<sup>375</sup>.

### **3.2.2 Protección de Datos: La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales**

La Agencia Española de Protección de Datos (AEPD) ha tenido ocasión de pronunciarse con respecto a la creación de sistemas de denuncias internas en las empresas en su Informe 128/2007, que fue emitido en respuesta a una

---

<sup>375</sup>ALONSO DE ESCAMILLA, A., "La responsabilidad penal...", ob. cit., pp. 892-893.

consulta planteada por una empresa farmacéutica que tenía el propósito de implantar un sistema de whistleblowing. En este Informe, la Agencia analiza la habilitación o legitimación de la empresa para el concreto tratamiento de datos de carácter personal que implica el canal de denuncias y estima que, a falta de un consentimiento inequívoco del afectado o de una norma legal habilitadora (como puede ser la Ley del Mercado de Valores, aunque no aplicable al supuesto analizado), puede entenderse que existe habilitación para el tratamiento sobre la base de lo dispuesto en el artículo 6.2 LOPD, donde se establece que no es necesario el consentimiento cuando los datos de carácter personal "*se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento*". Por lo que estima que pueden establecerse canales de denuncia con respecto a personas con los que la sociedad mantenga un vínculo contractual de derecho laboral, civil o mercantil y si existe pleno conocimiento por parte de las personas cuyos datos puedan ser tratados. La Agencia entiende que es preciso que el sistema "*se circunscriba a las denuncias referidas a materias o normas internas o externas cuyo incumplimiento tiene una consecuencia efectiva sobre el mantenimiento de la relación contractual entre la empresa y el denunciado*", sin que sea suficiente su establecimiento en relación con incumplimientos genéricos<sup>376</sup>.

El Informe exige que se identifique siempre al denunciante (prohibición de denuncias anónimas), permitiendo sólo procedimientos confidenciales de denuncias, sobre la base de la exactitud e integridad de la información contenida en los sistemas. Así, la Agencia Española de Protección de Datos va más allá de lo que había opinado el Grupo de Trabajo del artículo 29 en su Dictamen 1/2006 puesto que, pese a la preferencia por la confidencialidad,

---

<sup>376</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1232.

éste entendía que si *"la persona que informa al programa sigue queriendo permanecer en el anonimato, el informe se aceptará en el programa"*<sup>377</sup>.

En cuanto al derecho de acceso del denunciado y en relación con el tratamiento confidencial de la denuncia presentada, el Informe de la Agencia señala que queda prohibido el acceso por parte del denunciado a los datos del denunciante, porque sería una comunicación o cesión de datos no consentida y no amparada en los supuestos del artículo 11 LOPD.

Respecto al deber de información al afectado sobre la existencia del tratamiento de sus datos y sobre la posibilidad de ejercicio de los derechos de acceso, rectificación, cancelación y oposición, la Agencia entiende que no debe sobrepasarse en ningún caso el plazo de tres meses previsto en el artículo 5.4 LOPD, por tratarse de un supuesto en el que los datos no han sido recabados del titular de los mismos<sup>378</sup>.

### **3.2.3 Transparencia: La Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno**

La Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, se fundamenta en reforzar la transparencia en la información, evitar fraudes en la Administración Pública y establecer sanciones, constituyendo uno de sus principios de actuación denunciar irregularidades (whistleblowing). La Ley establece que los miembros del Gobierno, los Secretarios de Estado y el resto de los altos cargos de la Administración General del Estado y de las entidades del sector público estatal, de Derecho público o privado, vinculadas o dependientes de aquella estarán obligados a poner "en conocimiento de los órganos

---

<sup>377</sup>[http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes\\_juridicos/otras\\_cuestiones/common/pdfs/2007-0128\\_Creaci-oo-n-de-sistemas-de-denuncias-internas-en-las-empresas-mecanismos-de-whistleblowing.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2007-0128_Creaci-oo-n-de-sistemas-de-denuncias-internas-en-las-empresas-mecanismos-de-whistleblowing.pdf), p. 8.

<sup>378</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., pp. 1232-1233.

competentes cualquier actuación irregular de la cuál tengan conocimiento” (arts. 25 y 26.2.b.3º).

### **3.2.4 El Mercado de Valores: la notificación de infracciones en las empresas de servicios de inversión (art. 197 TRLMV)**

La Ley 37/1998, de 16 de noviembre (art. 6.3), dispuso que el artículo 79.d de la Ley 24/1988, de 28 de julio, del Mercado de Valores estableciese la obligación para las empresas de servicios de inversión, las entidades de crédito y las personas o entidades que actuasen en el Mercado de Valores de *“... tener establecidos los controles internos oportunos para garantizar una gestión prudente y prevenir los incumplimientos de los deberes y obligaciones que la normativa del Mercado de Valores les impone”*<sup>379</sup>. Esta disposición puede ser considerada como una primera previsión dentro del ordenamiento jurídico español que podría amparar los mecanismos de whistleblowing, si bien referido a las empresas señaladas<sup>380</sup>.

En el TRLMV se dedica el Título VII a las “Normas de conducta”. En él se establece que las entidades que presten servicios de inversión deben observar las normas de conducta aplicables a quienes presten servicios de inversión (art. 208.1). Así mismo, se dispone que las empresas de servicios de inversión, las entidades de crédito, las instituciones de inversión colectiva, los emisores, los analistas y, en general, cuantas personas o entidades realicen, de forma directa o indirecta, actividades relacionadas con los mercados de valores, deben respetar las normas relativas al abuso de mercado (art. 225.1).

El Título V del TRLMV se dedica a las empresas de servicios de inversión y dentro de él, su Capítulo VI a los “Sistemas, procedimientos y mecanismos de

---

<sup>379</sup>La Ley 44/2002, de 22 de noviembre, renumeró este artículo de la LMV, pasando el precepto reproducido en el texto a encontrarse en el art. 79.1.d. Posteriormente, con la modificación de la LMV por la Ley 47/2007, de 19 de diciembre, desapareció este texto.

<sup>380</sup>MESIA MARTÍNEZ, C., “El procedimiento...”, ob. cit., p. 1227.

gestión". En este Capítulo se encuentra el artículo 197<sup>381</sup> cuyo epígrafe es "Notificaciones de infracciones", en el que se establece la obligación para las empresas de servicios de inversión de disponer de procedimientos adecuados para que sus empleados puedan notificar infracciones a nivel interno a través de un canal independiente, específico y autónomo. La Ley también señala que estos procedimientos deben garantizar la confidencialidad tanto de la persona que informa de las infracciones como de las personas físicas presuntamente responsables de la infracción. Asimismo, la Ley impone como obligación garantizar que los empleados que informen de las infracciones cometidas en la entidad sean protegidos frente a represalias, discriminaciones y cualquier otro tipo de trato injusto.

### **3.2.5 Blanqueo de capitales. Ley 10/2010, de 28 de abril, de Prevención y Blanqueo de Capitales y de la Financiación del Terrorismo**

Sin duda, la prevención de blanqueo de capitales es una de las normativas con más trayectoria y repercusión en el ámbito de competencias de los Departamentos de *Compliance* en España, ya que cuenta con normativa europea desde hace 10 años y se establecen criterios de control interno muy alineados y extrapolables a otro tipo de medidas para la gestión de riesgos de cumplimiento.

El blanqueo de capitales es el proceso a través del cual los bienes de origen delictivo se integran en el sistema económico legal con apariencia de haber sido obtenidos de forma lícita<sup>382</sup>. Se puede definir el blanqueo de capitales como el "*proceso tendente a obtener la aplicación en actividades económicas ilícitas de una masa patrimonial derivada de cualquier género de conductas ilícitas, con independencia de cuál sea la forma que esa masa adopte,*

---

<sup>381</sup>La Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito introdujo en la Ley del Mercado de Valores por medio de su Disposición Final 1.16 el artículo 70 sexies de la Ley 24/1998, titulado "Notificación de infracciones", que actualmente está recogido en el artículo 197 TRLMV.

<sup>382</sup>BLANCO CORDERO, I., "La prevención del blanqueo de capitales", en AA.VV., *Manual de cumplimiento penal en la empresa*, dir. A. Nieto Martín, Valencia, 2015, pp. 433-435.

*mediante la progresiva concesión a la misma de una apariencia de legalidad."*<sup>383</sup>

La Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo regula la exigencia de establecimiento de canales de *whistleblowing* aunque sin mencionarlos expresamente, ya que habla de "obligaciones de información" y de "comunicación por indicio", limitando estas exigencias a los sujetos obligados por esta Ley.

El blanqueo de capitales es, ante todo, un delito que se encuentra regulado en el art. 301 del Código Penal y del que pueden responder tanto las personas físicas como las jurídicas<sup>384</sup>. Dicho delito comenzó a tipificarse a finales de la década de 1980, y ya está castigado en casi todos los ordenamientos jurídicos del mundo. Paralelamente a la creación de la figura delictiva, se han aprobado normas administrativas para prevenir su comisión, que persiguen impedir el acceso del dinero delictivo a la economía lícita. Como consecuencia de la aprobación de estas normas, se ha creado en el sector público un sistema administrativo encabezado por las Unidades de Inteligencia Financiera (UIF), cuya función esencial es recibir, analizar y transmitir a las autoridades competentes (policía, fiscalía) información sobre las operaciones sospechosas de estar vinculadas al blanqueo de capitales. Además de estos organismos públicos (en España el SEPBLAC, Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias), la estrategia de prevención de este fenómeno criminal ha consistido en imponer deberes de colaboración a determinadas entidades del sector privado. Estas se han visto obligadas a realizar enormes inversiones para crear sistemas internos dirigidos a detectar y evitar el blanqueo.

---

<sup>383</sup>OTERO SALGADO, L. D., "Prevención del blanqueo de capitales", AA.VV., *Compliance. Cómo gestionar los riesgos normativos en la empresa*, coord. C.A. Sáiz Peña, Pamplona, 2015, pp. 177-178.

<sup>384</sup>BLANCO CORDERO, I., "La prevención del blanqueo de capitales", ob. cit. p. 440.

En este sentido, el blanqueo de capitales suele estar asociado a actividades criminales muy lucrativas entre las que destacan, el narcotráfico, la prostitución, el tráfico de armas o la inmigración ilegal. El tremendo auge de la primera de esas actividades, el narcotráfico, en la década de los ochenta, y sobre todo, la enorme trascendencia económica, política y social que afectó a un gran número de países en todo el mundo, fue el principal detonante para que se establecieran a nivel internacional los primeros pasos de la lucha contra el blanqueo de capitales. Fue a finales de la mencionada década, cuando se llevó a cabo la primera Convención de Naciones Unidas<sup>385</sup> donde se trató este fenómeno tan relevante y cuando se constituyó el organismo internacional de referencia en esta materia a nivel internacional, el denominado Grupo de Acción Financiera Internacional<sup>386</sup> (GAFI) siendo su expresión más elaborada la expresada en las 40 Recomendaciones del GAFI del año 1990, con una importante modificación en el año 2012. Tras los ataques terroristas del 11 de septiembre de 2001, el GAFI publicó otras nueve recomendaciones centradas en la lucha contra la financiación del terrorismo<sup>387</sup>.

Estas recomendaciones constituyen el modelo a seguir por los Estados en materia de blanqueo de capitales. Las Recomendaciones del GAFI fueron tomadas como modelo en Europa, donde se han elaborado distintas Directivas relativas a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo, que intensifica las obligaciones.

Como decimos, el eje fundamental de estas normas es la imposición de obligaciones a los denominados sujetos obligados, que no sólo se limita a

---

<sup>385</sup>Convención de Viena de 1988, contra el tráfico ilícito de estupefacientes y sustancias psicotrópicas ([https://www.unodc.org/pdf/convention\\_1988\\_es.pdf](https://www.unodc.org/pdf/convention_1988_es.pdf))

<sup>386</sup>Creación en 1989 del Grupo de Acción Financiera Internacional (GAFI) o en inglés, Financial Action Task Force on Money Laundering (FATF) [www.fatf-gafi.org](http://www.fatf-gafi.org).

<sup>387</sup>OTERO SALGADO, L. D., "Prevención del blanqueo de capitales", ob. cit., p. 177 y BLANCO CORDERO, I., "La prevención del blanqueo de capitales", ob. cit. pp. 433-434.

bancos e instituciones financieras. En este sistema de prevención del blanqueo de capitales los sujetos obligados tienen la obligación de detectar e informar sobre cualquier operación que pueda estar vinculada al blanqueo de capitales y la financiación del terrorismo.

El cumplimiento de esta obligación puede chocar con los intereses de algunos de sus clientes que estarán interesados en realizar sus operaciones económicas de manera discreta o confidencial. A su vez, los sujetos obligados se encuentran en una situación en la que son objeto de máxima vigilancia por parte de las autoridades para comprobar que cumplen con sus deberes.

En España las obligaciones de prevención del blanqueo de capitales se encuentran contenidas en la ya citada Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. El 6 de mayo de 2014 se publicó en el BOE el Real Decreto 304/2014, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo que desarrolla la citada Ley y deroga el Real Decreto 925/1995, de 9 de junio<sup>388</sup>.

Las obligaciones que se imponen a los sujetos obligados son básicamente de tres tipos: aplicar medidas de diligencia debida, obligaciones de información y aplicar medidas de control interno<sup>389</sup>. En este análisis vamos sólo a centrarnos en las obligaciones de información, al ser las mismas el fenómeno más cercano al whistleblowing en relación al blanqueo de capitales.

Pues bien, la Ley impone que si se determina la concurrencia en la operativa de indicios o certeza de relación con el blanqueo de capitales o la financiación del terrorismo, el sujeto obligado por iniciativa propia y sin dilación debe efectuar la comunicación por indicio al SEPBLAC.

---

<sup>388</sup>BLANCO CORDERO, I., "La prevención del blanqueo de capitales", ob. cit. pp. 434-435.

<sup>389</sup>BLANCO CORDERO, I., "La prevención del blanqueo de capitales", ob. cit. p. 444.



La comunicación debe realizarse en el soporte y formato establecido por el SEPBLAC y de acuerdo con los procedimientos establecidos al respecto, y ha de contener la siguiente información:

- Relación e identificación de las personas físicas o jurídicas que participan en la operación y concepto de su participación en ella.
- Actividad conocida de las personas físicas o jurídicas que participan en la operación y correspondencia entre la actividad y la operación.
- Relación de operaciones vinculadas y fechas a que se refieren con indicación de su naturaleza, moneda en que se realizan, cuantía, lugar o lugares de ejecución, finalidad e instrumentos de pago o cobro utilizados.
- Gestiones realizadas por el sujeto obligado comunicante para investigar la operación comunicada.
- Exposición de las circunstancias de toda índole de las que pueda inferirse el indicio o certeza de relación con el blanqueo de capitales o con la financiación del terrorismo o que pongan de manifiesto la falta de justificación económica, profesional o de negocio para la realización de la operación<sup>390</sup>.
- Cualesquiera otros datos relevantes para la prevención del blanqueo de capitales o la financiación del terrorismo que se determinen reglamentariamente.
- La comunicación por indicio ha de incluir información sobre la decisión adoptada o que previsiblemente se adoptará por el sujeto obligado respecto a la continuación o interrupción de la relación de negocios con el cliente o clientes que participen en la operación, así como la justificación de esta decisión. Si la decisión es la no interrupción de la relación de negocios y esta viene determinada por la necesidad de no interferir en una entrega

---

<sup>390</sup>BLANCO CORDERO, I., "La prevención del blanqueo de capitales", ob. cit. pp. 466-467.

vigilada acordada conforme a lo dispuesto en el artículo 263 bis de la Ley de Enjuiciamiento Criminal (LECr), ha de hacerse constar este hecho de forma expresa (art. 26.3 Reglamento de la Ley 10/2010).

Para garantizar la calidad de las comunicaciones, se exige que a estas les preceda un proceso estructurado de examen especial de las mismas. Cuando a juicio del SEPBLAC el examen especial realizado sea insuficiente, ha de devolver la comunicación al sujeto obligado para que profundice en el examen de la operación, indicando los motivos de la devolución y el contenido a examinar. Si se trata de una operación meramente intentada, por ejemplo, el cliente, a la vista de las informaciones solicitadas por el sujeto para cumplir con sus obligaciones, decide no establecer una relación de negocio, el obligado debe registrarla como no ejecutada y comunicar al SEPBLAC la información que haya logrado obtener.

Se permite asimismo a los directivos o empleados del sujeto obligado que comuniquen directamente al SEPBLAC aquellas operaciones que conozcan y respecto de las cuales estimen que concurren indicios o certeza de estar relacionadas con el blanqueo de capitales, cuando, habiendo sido puestas de manifiesto internamente, el sujeto obligado no hubiese informado al directivo o empleado comunicante del curso dado a su comunicación.

No basta solo con efectuar la comunicación por indicio al SEPBLAC, sino que el sujeto obligado debe adoptar de manera inmediata medidas adicionales de gestión y mitigación del riesgo, que han de tomar en consideración el riesgo de revelación (art. 26.2 Reglamento de la Ley 10/2010)<sup>391</sup>.

Además de lo anterior, el artículo 27 del Reglamento de la Ley 10/2010 establece que los sujetos obligados deben comunicar mensualmente en todo caso al SEPBLAC una serie de obligaciones listadas en el Reglamento. En caso de no existir operaciones susceptibles de comunicación sistemática, los

---

<sup>391</sup>BLANCO CORDERO, I., "La prevención del blanqueo de capitales", ob. cit. pp. 467-468.

sujetos obligados comunicarán semestralmente esta circunstancia al SEPBLAC, excepto determinados sujetos que la Ley señala.

Las operaciones que han de comunicarse son:

a) Las operaciones que lleven aparejado movimiento físico de moneda metálica, papel moneda, cheques de viaje, cheques u otros documentos al portador librados por entidades de crédito, con excepción de las que sean objeto de abono o cargo en la cuenta de un cliente, por importe superior a 30.000 euros o su contravalor en moneda extranjera.

b) Los sujetos obligados que realicen envíos de dinero en los términos establecidos en el artículo 2 de la Ley 16/2009, de 13 de noviembre, de servicios de pago, deben comunicar al SEPBLAC las operaciones que lleven aparejado movimiento físico de moneda metálica, papel moneda, cheques de viaje, cheques u otros documentos al portador, por importe superior a 1.500 euros o su contravalor en moneda extranjera.

c) Las operaciones realizadas por o con personas físicas o jurídicas que sean residentes, o actúen por cuenta de estas, en territorios o países que al efecto se designen por Orden del Ministro de Economía y Competitividad, así como las operaciones que impliquen transferencias de fondos a o desde dichos territorios o países, cualquiera que sea la residencia de las personas intervinientes, siempre que el importe de las referidas operaciones sea superior a 30.000 euros o su contravalor en moneda extranjera.

d) Las operaciones que supongan movimientos de medios de pago sujetos a declaración obligatoria de conformidad con el artículo 34 de la Ley 10/2010, de 28 de abril.

e) La información agregada sobre la actividad de envíos de dinero, definida en el artículo 2 de la Ley 16/2009, de 13 de noviembre, de servicios

de pago, desglosada por países de origen o destino y por agente o centro de actividad.

f) La información agregada sobre la actividad de transferencias con o al exterior de las entidades de crédito, desglosada por países de origen o destino.

g) Las operaciones que se determinen mediante Orden del Ministro de Economía y Competitividad.

Es fundamental resaltar que el sujeto obligado no puede revelar al cliente ni a terceros que se ha comunicado información al SEPBLAC, o que se está examinando o puede examinarse alguna operación por si pudiera estar relacionada con el blanqueo de capitales o con la financiación del terrorismo (art. 24 de la Ley 10/2010). Esta obligación tiene una serie de excepciones:

a) Su cumplimiento puede entrar en conflicto con el deber de comunicar al SEPBLAC las operaciones sospechosas. Por eso, esta prohibición no comprende la revelación a las autoridades competentes, que incluye los órganos centralizados de prevención, o la revelación por motivos policiales en el marco de una investigación penal.

b) La comunicación de información entre entidades financieras pertenecientes al mismo grupo.

c) La comunicación de información entre los auditores de cuentas, contables externos, asesores fiscales, abogados, procuradores y otros profesionales independientes cuando ejerzan sus actividades profesionales, ya sea como empleados o de otro modo, dentro de la misma entidad jurídica o en una red. Se entiende por red la estructura más amplia a la que pertenece la persona y que comparte una propiedad, gestión o supervisión de cumplimiento comunes.

d) La comunicación de información, referida a un mismo cliente y a una misma operación en la que intervengan dos o más entidades o personas, entre entidades financieras o entre los profesionales citados en el apartado anterior, siempre que pertenezcan a la misma categoría profesional y estén sujetos a obligaciones equivalentes en lo relativo al secreto profesional y a la protección de datos personales. La información intercambiada se utilizará exclusivamente a efectos de la prevención del blanqueo de capitales y de la financiación del terrorismo<sup>392</sup>.

Las tres últimas excepciones también se aplican a la comunicación de información entre personas o entidades domiciliadas en la Unión Europea o en países terceros equivalentes. Sí que se prohíbe la comunicación de información con personas o entidades domiciliadas en países terceros no calificados como equivalentes o respecto de los que así lo decida la Comisión Europea.

En definitiva, si durante la relación de negocios o la ejecución de operaciones aparecen indicios o certeza de blanqueo de capitales o de financiación del terrorismo, los sujetos obligados deben identificar y verificar la identidad del cliente y del titular real con carácter previo al cumplimiento de las obligaciones de examen y comunicación por indicio. En estos casos se debe tener en cuenta el riesgo de revelación, pudiendo omitir la práctica de las medidas de diligencia debida cuando consideren razonablemente que revelarán al cliente o potencial cliente el examen o comunicación de la operación (art. 12 Reglamento). Está prohibido todo comportamiento consistente en la puesta en aviso a los clientes o a terceros de las actuaciones que se están llevando a cabo. El sujeto obligado que, a la vista del carácter sospechoso de una operación, le indica al cliente que ha de proceder obligatoriamente a su comunicación, está infringiendo su deber de confidencialidad al dar a conocer datos confidenciales, y puede dar lugar a

---

<sup>392</sup>BLANCO CORDERO, I., "La prevención del blanqueo de capitales", ob. cit. pp. 469 a 471.

que el delincuente rompa la relación de negocios y se evada con el dinero. Tal conducta constituye una infracción administrativa muy grave según el art. 51.1 c) de la Ley 10/2010. Sin embargo, tales conductas podrían ser también subsumibles en diversos tipos penales, por lo que en virtud del art. 62.3 de la Ley 10/210, si los hechos pudieran ser constitutivos de delito se dará traslado al Ministerio Fiscal y se ordenará la suspensión del expediente sancionador.

No constituye revelación la conducta de los auditores de cuentas, contables externos, asesores fiscales, abogados, procuradores y otros profesionales independientes cuando intenten disuadir a un cliente de una actividad ilegal<sup>393</sup>.

Por último debe mencionarse la consiguiente importancia que tiene la protección a los denunciantes. Por un lado, a los sujetos obligados se les impone el deber de garantizar la confidencialidad sobre la identidad de los empleados, directivos o agentes que hayan realizado una comunicación a los órganos de control interno. Se persigue así que de puertas para fuera del sujeto obligado no se conozca el nombre del comunicante, algo que sí ocurrirá normalmente dentro del propio sujeto obligado en la medida en que este intervendrá normalmente en el proceso de verificación de los indicios o sospechas de blanqueo que se lleven en los distintos niveles de la organización interna. Esto supone, por lo tanto, que el sujeto obligado no está obligado a revelar la identidad de aquellos sujetos en el marco de los procesos judiciales o administrativos que surjan como consecuencia de la comunicación presentada. Cuestión que no deja de plantear dudas, sobre todo en los procesos penales, donde parece que el juez no puede hacer comparecer al empleado comunicante.

Como la identidad del empleado comunicante queda protegida incluso en los procedimientos judiciales o administrativos que se ventilen, el precepto dispone entonces quién ha de comparecer en los mismos en representación

---

<sup>393</sup>BLANCO CORDERO, I., "La prevención del blanqueo de capitales", ob. cit. pp. 471-472.

del sujeto obligado. De acuerdo con el precepto, quien ha de comparecer es el representante ante el SEPBLAC del sujeto obligado. Esta comparecencia, con todo, parece tener carácter excepcional, pues solo procede “cuando se estime imprescindible obtener la aclaración, complemento o confirmación del propio sujeto obligado”, algo que corresponderá valorar al juez o al instructor del correspondiente procedimiento administrativo.

Asimismo se impone a las autoridades o funcionarios el deber de adoptar medidas dirigidas a proteger de cualquier amenaza o acción hostil a los empleados, directivos o agentes de los sujetos obligados que comuniquen indicios de blanqueo de capitales o de financiación del terrorismo. Esto significa que la obligación de protección surge una vez constatada la amenaza o acción hostil, lo que no da cabida, en principio, a actuaciones dirigidas a prevenir tales situaciones<sup>394</sup>.

### **3.2.6 Defensa de la Competencia. Programas de Clemencia**

En el ámbito del derecho de la competencia el *whistleblower* juega un papel esencial ya que constituye una de las principales fuentes de información para detectar infracciones de la normativa de la competencia<sup>395</sup>. La Ley 15/2007 de 3 de julio, de Defensa de la Competencia dispone que cualquier persona, física o jurídica, interesada o no, puede formular una denuncia de las infracciones de las conductas prohibidas por la Ley.

El Reglamento de Defensa de la Competencia de 2008<sup>396</sup>, establece que las denuncias debe incluir, como mínimo, la siguiente información: a) nombre o razón social, domicilio, teléfono y número de fax del/de los denunciante/s y, en el caso de que éstos actúen por medio de representante, acreditación de la representación y domicilio a efectos de notificaciones; b) nombre o razón social, domicilio y, en su caso, número de teléfono y de fax o cualquier otro

---

<sup>394</sup>BLANCO CORDERO, I., "La prevención del blanqueo de capitales", ob. cit. pp. 486-487.

<sup>395</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1230.

<sup>396</sup>Aprobado por el Real Decreto 261/2008, de 22 de febrero.

medio electrónico pertinente de los denunciados; c) hechos de los que se deriva la existencia de una infracción y pruebas, en su caso, de los mismos, así como definición y estructura del mercado relevante; d) en su caso, justificación de los intereses legítimos<sup>397</sup>, para ser considerado interesado en el eventual expediente sancionador<sup>398</sup>.

Una de las novedades de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia fue la introducción en nuestro sistema de los programas de clemencia, ya puestos en práctica con éxito en Estados Unidos y en la Unión Europea.

El programa de clemencia es un poderoso instrumento en manos de las autoridades de defensa de la competencia para la detección de los cárteles, en cuanto atentados más dañinos contra la competencia. En relación a la exención del pago de la multa, la Comisión Nacional de los Mercados y de la Competencia (CNMC) eximirá a una empresa o persona física del pago de la multa que hubiere podido imponerle cuando sea la primera en aportar elementos de prueba, siempre y cuando la Comisión Nacional de la Competencia, en el momento de aportarse aquellos, no disponga de elementos suficientes para ordenar la misma (art. 65.a LDC).

Los programas de clemencia nacen con el fin de eximir de la multa a la que tendrían que hacer frente determinadas empresas que hayan incurrido en ilícitos relativos al derecho de la competencia o para obtener una reducción de la misma (en Estados Unidos solamente la primera empresa que acuda a la autoridad administrativa es eximida del pago de la multa, no existen las reducciones). Por esta razón, otra de las funciones principales de los programas de cumplimiento en materia de competencia es permitir que la empresa conozca cuanto antes la existencia de la práctica y pueda comunicarla en primer lugar a las autoridades.

---

<sup>397</sup>De acuerdo con el artículo 4 de la LPACAP.

<sup>398</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1231.



Siguiendo el ejemplo estadounidense, donde la política de clemencia se puso por vez primera en práctica en 1978, la Comisión Europea introdujo mediante la Comunicación de 18 de julio de 1996 un sistema que preveía la exención o la reducción en el pago de las multas a las empresas que colaborasen con las autoridades de la competencia para la persecución de un cártel del que formaran parte<sup>399</sup>. En esta Comunicación se contempló la posibilidad de tres niveles de reducción de multas (del 75 al 100%, del 50 al 75% y del 10 al 50%), en función de las características que concudiesen en un determinado supuesto. La mayor reducción se obtenía cuando la empresa informase acerca de la existencia del cártel, sin que la Comisión hubiese realizado alguna investigación. La empresa debe probar la existencia del acuerdo y poner fin a su participación en el mismo, manteniendo una cooperación permanente y total durante la investigación. Un requisito previo para beneficiarse de la exención es que no hubiese obligado a otra empresa a participar en el mismo, no desempeñando además ningún papel determinante en la actividad ilícita.

El principal inconveniente de esta primera Comunicación fue que la Comisión Europea tenía un amplio margen de apreciación y no se les garantizaba a las empresas infractoras una inmunidad automática, aún en el supuesto de que hubiesen colaborado con la Comisión cumpliendo todas las condiciones requeridas. Por este motivo, esta Comunicación se sustituyó por la Comunicación de 19 de febrero de 2002, dirigida a mejorar la seguridad jurídica, la predecibilidad y transparencia de su programa de clemencia, con el fin de hacerlos más atractivo para las empresas que quisieran colaborar con la Comisión<sup>400</sup>.

---

<sup>399</sup>Comunicación relativa a la no imposición de multas o a la reducción de su importe en los asuntos relacionados con acuerdos entre empresas, DOCE núm. C 207/4, de 18 de julio de 1996.

<sup>400</sup>Comunicación relativa a la dispensa del pago de las multas y la reducción de su importe en casos de cártel, DOCE núm. C 45/3, de 19 de febrero). Según esta Comunicación, para obtener la dispensa plena, las empresas deberán ser las primeras en acudir a la autoridad administrativa, colaborar plena, continua y diligentemente con la Comisión, facilitándole todos los elementos de prueba que obren en su poder, poner fin inmediatamente a su infracción y no haber obligado a otras empresas

Actualmente en España, a través de la presentación de una solicitud de clemencia, las empresas o personas físicas que participen en un cártel pueden beneficiarse de una exención, o de una reducción del importe de la multa que se les impondría en caso de ser sancionados por su conducta.

La exención del importe total de la multa podría concederse a condición de que se aporten al regulador elementos de prueba que posibiliten la detección del cártel. Una vez en conocimiento del regulador, aquellos que aporten elementos de prueba que por su naturaleza o por su nivel de detalle, permitan al regulador aumentar su capacidad para probar el cártel podrían beneficiarse de una reducción del importe de la sanción de hasta un 50%. La reducción sería de hasta el 30% para el siguiente y hasta el 20% para los sucesivos solicitantes de clemencia<sup>401</sup>.

De especial interés es la Comunicación de 19 de junio de 2013, de la Comisión Nacional de la Competencia, sobre el Programa de Clemencia<sup>402</sup>

### **3.2.7 Ámbito societario en los Códigos de Buen gobierno**

Dentro del ámbito empresarial no se observa referencia expresa alguna a la implantación de canales de denuncias internas hasta la publicación del Código Unificado de Buen Gobierno de las Sociedades Cotizadas de 2006<sup>403</sup>. Entre las recomendaciones de este Código se encuentra la de que sociedades cotizadas encomienden al Comité de Auditoría el establecimiento y seguimiento de cauces internos para que los empleados puedan denunciar irregularidades ("whistleblowing") que protejan la identidad del denunciante y

---

para que participen en el cártel. En el supuesto de no cumplir alguno de estos requisitos, la empresa podrá obtener un grado de clemencia inferior siempre y cuando finalice su participación en el cártel y sea capaz de aportar pruebas con un valor añadido significativo respecto de los que ya tenía la Comisión.

<sup>401</sup><https://www.cnmc.es/Portals/0/Ficheros/Competencia/clemencia/diptico%20programa%20de%20clemencia.pdf?timestamp=1397478425762>

<sup>402</sup>BOE nº 196, de 16 de agosto de 2013, pp. 60718-60734.

<sup>403</sup>Acuerdo del Consejo de la CNMV por el que se aprueba el Documento Único de Recomendaciones de Gobierno Corporativo, de 22 de mayo de 2006. En su Anexo I se recoge el Código Unificado de Buen Gobierno de 19 mayo de 2006.

se considera oportuno, permitan su anonimato. Estos mecanismos se destinarán preferentemente a la denuncia de irregularidades financieras y contables y respetarán escrupulosamente las limitaciones establecidas en la LOPD<sup>404</sup>. Este Código Unificado de Buen Gobierno Corporativo recomienda la aplicación del procedimiento de whistleblower, es decir, la existencia de un procedimiento (canal de denuncia, email, correo certificado) de presentación de denuncias confidenciales o anónimas cuando el trabajador o directivo observe que se han producido irregularidades de cierta entidad, refiriéndose al código ético de conducta, especialmente financieras y contables, sin que se mencione expresamente delitos económicos, corruptos o de acoso<sup>405</sup>.

A partir de la crisis financiera internacional, han surgido numerosas iniciativas relacionadas con las buenas prácticas en materia de gobierno corporativo. En España ha habido avances muy apreciables en materia de buen gobierno corporativo. El Consejo de Ministros de 10 de mayo de 2013, acordó la creación de una Comisión de Expertos en materia de gobierno corporativo<sup>406</sup>, para proponer las iniciativas y las reformas normativas que se considerasen adecuadas para garantizar el buen gobierno de las empresas y para prestar apoyo y asesoramiento a la CNMV en la modificación del Código Unificado de Buen Gobierno de las Sociedades Cotizadas de mayo de 2006. La Comisión de Expertos, en atención al mandato recibido, desarrolló su trabajo distinguiendo entre las mejoras de gobierno corporativo que debían ser incorporadas a normas legales, y aquellas otras que debían mantenerse

---

<sup>404</sup>La Recomendación 50 dispone que corresponde al Comité de Auditoría en relación con los sistemas de información y control interno "establecer y supervisar un mecanismo que permita a los empleados comunicar, de forma confidencial y, si se considera apropiado, anónima las irregularidades de potencial trascendencia, especialmente financieras y contables, que adviertan en el seno de la empresa" (Recomendación 50, 1º.d).

<sup>405</sup>MATEU DE ROS CEREZO, R., *El Código Unificado de Buen Gobierno: Estudio del Informe del Grupo Especial de Trabajo sobre Buen Gobierno de las sociedades cotizadas aprobado por la CNMV el 22 de Mayo de 2006*, edit. Thomson-Aranzadi, Pamplona, 2007, pp. 355-356.

KUHLEN, L./ MONTIEL, J. P./ ORTIZ DE URBINA GIMENO, I., *Compliance y Teoría del Derecho Penal*, edit. Marcial Pons, Madrid, 2013, pp 22-46.

<sup>406</sup>Orden ECC/895/2013, de 21 de mayo, por la que se publica el Acuerdo del Consejo de Ministros de 10 de mayo de 2013, por el que se crea una Comisión de expertos en materia de gobierno corporativo.

como recomendaciones de buen gobierno de carácter voluntario, sujetas al principio conocido internacionalmente como "cumplir o explicar".

La Comisión de Expertos en materia de Gobierno Corporativo elaboró el "Estudio sobre propuestas de modificaciones normativas" de fecha 14 de octubre de 2013<sup>407</sup>. La Ley 31/2014, de 3 de diciembre, por la que se modificó la Ley de Sociedades de Capital para la mejora del gobierno corporativo, reconoció expresamente que su articulado se basaba en este "Estudio de la Comisión de Expertos", respetando la práctica totalidad de sus recomendaciones (Preámbulo III). Se dispone que el Consejo de Administración de una sociedad anónima cotizada debe constituir una comisión de auditoría (art. 529 terdecies.2 TRLSC). Entre las funciones de esta comisión está la de supervisar la eficacia del control interno de la sociedad y los sistemas de gestión de riesgos, así como gestionar con el auditor de cuentas las debilidades significativas del sistema de control interno detectadas en el desarrollo de la auditoría, sin quebrantar su independencia (art. 529 quaterdecies.3 y 4 TRLSC). Las sociedades anónimas cotizadas deben hacer público un informe anual de gobierno corporativo (arts. 540.1 y 538 TRLSC). El informe de gobierno corporativo debe incluir un apartado dedicado a sistemas de control del riesgo (art. 540.4.e TRLSC); así mismo, debe consignarse el grado de seguimiento de las recomendaciones de gobierno corporativo o, en su caso, la explicación de la falta de seguimiento de dichas recomendaciones (art. 540.4.g TRLSC), atendiendo al principio de "cumplir o explicar"<sup>408</sup>.

---

<sup>407</sup> *Estudio sobre propuestas de modificaciones normativas. Comisión de Expertos en materia de Gobierno Corporativo (creada por Acuerdo del Consejo de Ministros, de 10 de mayo de 2013, publicado por Orden ECC/895/2013, de 21 de mayo), Madrid, 14 de octubre de 2013, en [http://www.cnmv.es/docportal/publicaciones/codigogov/cegc\\_estmodif\\_20131014.pdf](http://www.cnmv.es/docportal/publicaciones/codigogov/cegc_estmodif_20131014.pdf), p. 4.*

Este estudio se apoyó en la Propuesta de Código Mercantil, elaborada por la Sección de Derecho Mercantil de la Comisión General de Codificación de 17 de junio de 2013.

<sup>408</sup> Cada sociedad es libre de seguir estas recomendaciones de gobierno corporativo, pero se exige que, cuando no se cumplan, se expliquen los motivos de no hacerlo, al objeto de que los accionistas, los inversores y los mercados lo valoren.

La Comisión de Expertos elaboró y la CNMV aprobó el "Código de buen gobierno de las sociedades cotizadas", de 18 de febrero de 2015<sup>409</sup>, el cual está dirigido a las sociedades cotizadas<sup>410</sup> y se caracteriza por la voluntariedad, con sujeción al principio de "cumplir o explicar"<sup>411</sup>.

El Código recomienda reforzar las normas legales en relación con la función de la auditoría interna y ampliar las funciones de la comisión de auditoría. Así, en relación con los sistemas de información y control interno se recomienda que a la comisión de auditoría además de las funciones previstas en la Ley, le corresponda entre otras la función de *"establecer y supervisar un mecanismo que permita a los empleados comunicar, de forma confidencial y, si resulta posible y se considera apropiado, anónima, las irregularidades de potencial trascendencia, especialmente financieras y contables, que adviertan en el seno de la empresa"* (Recomendación 42.1.c).

En lo relativo al acoso sexual, la Ley Orgánica 3/2007, de 22 de marzo, para la Igualdad Efectiva de Mujeres y Hombres establece que "las empresas deberán promover condiciones de trabajo que eviten el acoso sexual y el acoso por razón de sexo y arbitrar procedimientos específicos para su prevención y para dar cauce a las denuncias o reclamaciones que puedan formular quienes hayan sido objeto del mismo"<sup>412</sup> (art. 48.1). La Ley no prevé

---

<sup>409</sup>Código del buen gobierno de las sociedades cotizadas, CNMV, 18 de febrero de 2015, disponible en [https://www.cnmv.es/docportal/publicaciones/codigogov/codigo\\_buen\\_gobierno.pdf](https://www.cnmv.es/docportal/publicaciones/codigogov/codigo_buen_gobierno.pdf).

<sup>410</sup>Se entiende por tales aquellas cuyas acciones están admitidas a negociación en un mercado secundario oficial de valores (art. 495.1 LSC).

<sup>411</sup>La utilización de códigos de buen gobierno de carácter voluntario junto con el principio de "cumplir o explicar" es el sistema seguido de forma consistente en los principales países de la Unión Europea y en otros países desarrollados. La Unión Europea ha recogido expresamente en su normativa la validez de este principio de actuación, confirmado en el Libro Verde de la Unión Europea sobre gobierno corporativo de las sociedades cotizadas (Código del buen gobierno de las sociedades cotizadas, CNMV).

<sup>412</sup>La posibilidad de vincular esta previsión legal con los procedimientos de denuncia interna en general se admite en GOÑI SEIN, J.L., "Sistemas de denuncia interna de irregularidades ("Whistleblowing")", AA.VV., *Ética empresarial y códigos de conducta*, dir. J.L. Goñi, Madrid, 2011, p. 323. También existen algunos puntos de conexión con algunas medidas previstas en la Ley 10/2010 de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo (esp. arts. 26 y ss.), que otorgan protección a los empleados de las entidades obligadas a prevenir tales comportamientos que denuncien conductas sospechosas. Con todo, la diferencia radica en que en este caso se trata

consecuencia sancionadora alguna para las empresas que no establezcan esos mecanismos de prevención del acoso sexual, un delito que no da lugar en el vigente Derecho español a responsabilidad penal de las personas jurídicas<sup>413</sup>.

### 3.2.8 Derecho Nuclear

Tal y como destaca el maestro en la materia nuclear A. MORALES<sup>414</sup> una de las novedades más significativas que introdujo la Ley 33/2007 de 7 de noviembre de reforma de la Ley 15/1980, de 22 de abril, que crea el Consejo de Seguridad Nuclear es el mecanismo de whistleblowing. En efecto, según su artículo 13:

*" 1. Las personas físicas o jurídicas al servicio de las instalaciones nucleares y radiactivas, cualquiera que sea la relación laboral o contractual que mantenga con éstas, deberán poner en conocimiento de los titulares cualquier hecho conocido que afecte o pueda afectar al funcionamiento seguro de las mismas y al cumplimiento de la normativa vigente en materia de seguridad nuclear o protección radiológica.*

*En caso de que los titulares no tomen diligentemente medidas correctoras, deberán ponerlo en conocimiento del Consejo de Seguridad Nuclear.*

*2. Los empleadores que tomen represalias contra los trabajadores que pongan en conocimiento del Consejo de Seguridad Nuclear hechos relacionados con la seguridad de las instalaciones serán sancionados con arreglo a lo previsto en la legislación sobre energía nuclear.*

---

de la denuncia de hechos cometidos por personas en principio ajenas a la propia empresa (por ejemplo, clientes en una entidad bancaria que operan a través de ésta).

<sup>413</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. p. 168.

<sup>414</sup>MORALES PLAZA, A., *La regulación nuclear globalizada*, Madrid, 2009, pp 771 y ss

3. *Reglamentariamente se desarrollarán los mecanismos administrativos necesarios para facilitar el ejercicio de este derecho.*

4. *El ejercicio de este derecho no podrá reportar efectos adversos para el trabajador en su puesto de trabajo salvo en los supuestos en que se acredite mala fe en su actuación.*

*Se entenderán nulas y sin efecto las decisiones del titular tomadas en perjuicio o detrimento de los derechos laborales de los trabajadores que hayan ejercitado el derecho previsto en este artículo".*

Este precepto debe ser completado con su desarrollo reglamentario, que se plasma en el artículo 8 bis del Real Decreto 1836/1999, de 3 de diciembre, que aprueba el Reglamento de Instalaciones Nucleares y Radiactivas. Según dicho precepto (Comunicación de deficiencias):

*“De acuerdo con lo previsto en el artículo 13 de la Ley 15/1980, de 22 de abril, de Creación del Consejo de Seguridad Nuclear, a efectos del deber de las personas al servicio de las instalaciones nucleares y radiactivas de poner en conocimiento de los titulares cualquier hecho que pueda afectar al funcionamiento seguro de las mismas o a la protección radiológica:*

*a) El titular establecerá un procedimiento para garantizar que todo el personal de la organización de la instalación, así como el de las empresas contratadas y el de las externas que prestan sus servicios en la misma, comunique al titular aquellas deficiencias o disfunciones que, a juicio del comunicante, pudieran afectar a la seguridad nuclear o a la protección radiológica, todo ello sin perjuicio de los derechos generales del ciudadano establecidos en las leyes correspondientes.*

*Este procedimiento será adicional a los canales habituales de comunicación y podrá ser utilizado a elección del comunicante. Asimismo, el comunicante deberá recurrir a este procedimiento si, tras comunicar alguna deficiencia por los canales habituales de comunicación, llegara a la conclusión de que su denuncia o reclamación no había sido suficientemente atendida.*

*En el procedimiento se deberán atender a todas las comunicaciones, tanto si provienen de comunicantes identificados como anónimos, y dichas comunicaciones deberán incluirse en un registro numerado y fechado con copia de las comunicaciones recibidas, y referencia de las informaciones facilitadas en respuesta a las mismas y de las diligencias de verificación o las medidas adoptadas en su virtud. Las instalaciones radiactivas con fines científicos, médicos, agrícolas, comerciales o industriales, según se definen en el Título III de este Reglamento, podrán optar por registrar dichas comunicaciones y las respuestas y diligencias de verificación o medidas adoptadas en el diario de operación a que se hace referencia en el Título VI de este Reglamento.*

*El comunicante, si se ha identificado, deberá recibir respuesta por escrito en menos de 7 días hábiles por parte del titular de la instalación con la información sobre las medidas adoptadas o las previstas.*

*Transcurrido dicho plazo sin que el titular remita respuesta escrita al comunicante, éste deberá transmitir al Consejo de Seguridad Nuclear la información de que se trate.*

*El procedimiento garantizará la existencia de un trámite abreviado para aquellos supuestos en que el comunicante aprecie razones de urgencia, para lo cual se establecerá la obligación del titular de contestar al comunicante de forma inmediata, pudiendo éste transmitir, si lo considera oportuno, la información al Consejo de Seguridad*



*Nuclear en el momento en que advirtiera la deficiencia o disfunción apreciada.*

*Sin perjuicio de lo anterior, en esta materia será de aplicación supletoria la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.*

*b) El ejercicio de este derecho no podrá reportar efectos adversos para el trabajador en su puesto de trabajo, salvo en los supuestos en que se acredite mala fe en su actuación.*

*Se entenderán nulas y sin efecto las decisiones del titular tomadas en detrimento o perjuicio de los derechos laborales de los trabajadores que hayan ejercitado el derecho previsto en este artículo.*

Asimismo debe destacarse que cualquier ciudadano puede denunciar una infracción ante el Consejo de Seguridad Nuclear, que es a quien corresponde la iniciación del expediente sancionador de conformidad con lo dispuesto en el artículo 91 de la Ley 25/1964, de 29 de abril, de Energía Nuclear. Además, hay que tener en cuenta que, tal y como sostiene A. MORALES<sup>415</sup> los primeros interesados en la denuncia de infracciones en materia de seguridad en las instalaciones nucleares serán los propios trabajadores de las mismas expuestos a los riesgos derivados de las supuestas infracciones de las que sean conscientes.

---

<sup>415</sup>MORALES PLAZA, A., *La regulación nuclear globalizada*, ob. cit. 771 y ss

#### **4. Figuras similares en el sector financiero: los servicios de atención al cliente de las entidades y los servicios de reclamaciones de los organismos reguladores**

Existen tres tipos de instituciones de protección de la clientela financiera: dos privadas, que son los servicios o departamentos de protección de la clientela de las entidades de crédito y los defensores del cliente u organismos similares que pueden tener establecidos las entidades de crédito o las asociaciones de entidades; y otra pública, que son los Servicios de Reclamaciones de los organismos reguladores<sup>416</sup>.

En relación con los servicios de las entidades financieras debe destacarse la Orden ECO/734/2004<sup>417</sup>, de 11 de marzo, sobre los departamentos y servicios de atención al cliente y el defensor del cliente de las entidades financieras, la cual regula los requisitos y procedimientos que deben cumplir los departamentos y servicios de atención al cliente, así como los del defensor del cliente. En este sentido, la Orden dispone que estarán obligadas a atender y resolver las quejas y reclamaciones que sus clientes les presenten, relacionadas con sus intereses y derechos legalmente reconocidos las siguientes entidades:

- a) las entidades de crédito,
- b) las empresas de servicios de inversión,
- c) las sociedades gestoras de instituciones de inversión colectiva,
- d) las entidades aseguradoras,
- e) las entidades gestoras de fondos de pensiones, con las precisiones establecidas en la disposición adicional primera de esta Orden.

---

<sup>416</sup>TAPIA HERMIA, A.J., *Manual...*, ob. cit., p. 168.

<sup>417</sup>Orden ECO/734/2004, de 11 de marzo, sobre los departamentos y servicios de atención al cliente y el defensor del cliente de las entidades financieras.

f) las sociedades de correduría de seguros,

g) las sucursales en España de las entidades enumeradas en los párrafos anteriores con domicilio social en otro Estado.

Asimismo, la Orden obliga a las anteriores entidades a disponer de un departamento o servicio especializado de atención al cliente, que tenga por objeto atender y resolver las quejas y reclamaciones que presenten sus clientes.

Las entidades podrán designar un defensor del cliente, al que corresponderá atender y resolver los tipos de reclamaciones que se sometan a su decisión, así como promover el cumplimiento de la normativa de transparencia y protección de la clientela y de las buenas prácticas y usos financieros.

La designación del defensor del cliente podrá efectuarse conjuntamente con otras entidades, de manera que aquél atienda y resuelva las reclamaciones de los clientes de todas ellas, de acuerdo con lo que disponga su reglamento de funcionamiento.

El defensor del cliente es una institución de naturaleza privada que tiene por función la tutela de los intereses de los clientes de las entidades de crédito en sus relaciones con las mismas y que persigue que tales relaciones se desarrollen conforme a los principios de la buena fe, la equidad y la confianza recíproca. Se excluyen de sus competencias los conflictos derivados de las relaciones laborales de las entidades con sus empleados y de las relaciones societarias de las entidades con sus socios o accionistas, así como las decisiones de concesión de crédito, las cuestiones que estén "sub iudice", etc. Los procedimientos que siguen estos defensores del cliente se establecen en sus respectivos reglamentos y procuran un arreglo amistoso y

una solución equitativa del conflicto planteado mediante la aplicación de normas jurídicas y usos o prácticas bancarias<sup>418</sup>.

En relación con los servicios de reclamaciones de los organismos reguladores del sector financiero debe destacarse que la disposición adicional undécima de la Ley 2/2011 de Economía Sostenible (Ley de Economía Sostenible) vino a modificar el régimen español de atención de las reclamaciones del sector financiero para proteger los derechos de los clientes en cada uno de los tres ámbitos que configuran la actividad financiera, esto es, banca, valores y seguros.

No obstante, con carácter previo a la modificación practicada por la Ley de Economía Sostenible, la Ley 44/2002 de 22 de noviembre de Medidas de Reforma del Sistema Financiero (Ley 44/2002) regulaba la figura de los Comisionados como aquellos órganos encargados de la labor de protección de los usuarios de los servicios financieros. Sin embargo, este órgano nunca se desarrolló normativamente y fueron los propios servicios de reclamaciones del Banco de España, la Comisión Nacional del Mercado de Valores y de la Dirección General de Seguros y Pensiones los que desarrollaron la tarea de protección y de resolución de las reclamaciones de los clientes.

Como consecuencia de lo anterior, la normativa exigía una reforma y fue la Ley de Economía Sostenible la que al modificar los artículos 30 y 31 de la Ley 44/2002, suprimió la figura del Comisionado y atribuyó la protección de los usuarios directamente a los servicios de reclamaciones del Banco de España, la Comisión Nacional del Mercado de Valores y la Dirección General de Seguros y Fondos de Pensiones.

De esta forma, el artículo 30 de la Ley 44/2002 constituye uno de los puntos de partida en materia de servicios de reclamaciones y establece que serán los servicios de reclamaciones ante el Banco de España, la Comisión

---

<sup>418</sup>TAPIA HERMIA, A.J., *Manual...*, ob. cit., p. 168.

Nacional del Mercado de Valores y la Dirección General de Seguros y Fondos de Pensiones los que resolverán las quejas y reclamaciones que presenten los usuarios de servicios financieros. El artículo 31 de la misma ley habilita al Ministro de Economía para establecer los requisitos y el procedimiento al que se someta la resolución de las reclamaciones.

Así pues, la Orden ECC/2502/2012 de 16 de noviembre da cumplimiento a esta última obligación y regula el procedimiento de presentación de reclamaciones y hace una distinción entre queja, reclamación y consulta.

Considera como queja las que son presentadas por los usuarios de los servicios financieros como consecuencia de cualquier demora, desatención o actuación deficiente.

Las reclamaciones, en cambio, son las presentadas por los usuarios para obtener la restitución de su interés o derecho como consecuencia de las acciones u omisiones que supongan para quien las formula un perjuicio para sus intereses o derechos, y que deriven de presuntos incumplimientos por parte de las entidades de la normativa de transparencia y protección de la clientela o de las buenas prácticas y usos financieros.

Las consultas son definidas como las solicitudes de asesoramiento e información relativas a cuestiones de interés general en relación con los derechos de los usuarios en materia de transparencia, protección de la clientela o el cauce legal para su ejercicio.

Se entiende por buenas prácticas aquellas que son razonablemente exigibles para la gestión responsable, diligente y respetuosa con la clientela de los negocios financieros, mientras que las normas de transparencia y protección de la clientela son aquellas que contienen preceptos específicos referidos a las entidades supervisadas con la finalidad de proteger los legítimos intereses de la clientela.

El artículo 3 de la Orden se refiere a la legitimación para formular quejas, reclamaciones y consultas y reconoce que podrán presentarlas cualquier persona física o jurídica, española o extranjera, que esté debidamente identificada como usuario de los servicios financieros prestados por cualquiera de las entidades supervisadas por el Banco de España, la Comisión Nacional del Mercado de Valores y la Dirección General de Seguros y Fondos de Pensiones.

Asimismo, pueden presentarlas las personas o entidades que actúen en defensa de los intereses particulares de sus clientes, partícipes o inversores, los tomadores de seguros, asegurados, beneficiarios, terceros perjudicados o derechohabientes de cualquiera de ellos, así como los partícipes y beneficiarios de planes de pensiones.

Por último también legitima a las asociaciones y organizaciones representativas de legítimos intereses colectivos de los usuarios de servicios financieros, siempre que tales intereses resulten afectados. Estas asociaciones y organizaciones deben estar habilitadas para su defensa y protección y deben reunir los requisitos establecidos en el Real Decreto Legislativo 1/2007, de 16 de noviembre por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios.

Cualquier reclamación o queja podrá ser presentada indistintamente ante cualquiera de los tres servicios de reclamaciones con independencia de su contenido, y se podrá efectuar en soporte papel o por medios electrónicos, a través de los registros habilitados al efecto.

Se podrán presentar conforme al formulario que a tal efecto desarrollan los servicios de reclamaciones con el siguiente contenido: (i) datos identificativos del reclamante; (ii) identificación de la entidad reclamada; (iii) motivo de la reclamación o queja; (iv) acreditación de que ha transcurrido el plazo de dos meses desde la fecha de presentación de la reclamación o queja ante el

servicio de atención al cliente correspondiente; (v) lugar, fecha y firma; y (vi) toda la documentación necesaria para resolver la cuestión que se plantea.

De todas las reclamaciones y quejas se debe dejar constancia formal en el servicio de reclamaciones en que se reciba y para la admisión y tramitación de las mismas será requisito imprescindible acreditar haberlas formulado previamente al departamento o servicio de atención al cliente.

El artículo 9 de la Orden contempla las reclamaciones y quejas colectivas de tal forma que podrá presentarse una única reclamación o queja conjunta por parte de distintos reclamantes, cuando éstos se vean afectados por conductas que tengan un contenido y fundamento idéntico o sustancialmente similar.

Las causas de inadmisión de las reclamaciones o quejas serán las siguientes: (i) cuando se pretenda tramitar acciones y recursos cuya competencia corresponda a órganos administrativos, arbitrales o judiciales; (ii) cuando se planteen controversias sobre determinados hechos cuya prueba únicamente pueda ser realizada en vía judicial; (iii) cuando se planteen controversias sobre la cuantificación económica de los daños y perjuicios que eventualmente se hayan podido ocasionar a los usuarios de los servicios financieros; (iv) cuando se fundamente en una controversia cuya resolución requiera necesariamente la valoración de expertos con conocimientos especializados en una materia técnica ajena a la normativa de transparencia y protección de la clientela o a las buenas prácticas y usos financieros; (v) cuando se advierta carencia de fundamento o inexistencia de pretensión por omitirse datos esenciales para la tramitación; (vi) cuando los hechos, razones o la solicitud no se refieran a operaciones concretas o sean distintos de los alegados en el departamento o servicio de atención al cliente; (vii) cuando lo que se plantee como una queja o reclamación sea en realidad una consulta; (viii) cuando se presenten quejas o reclamaciones sobre cuestiones ya resueltas con anterioridad y que tengan un contenido y fundamento idéntico o

sustancialmente igual; (ix) cuando se presenten ante la Dirección General de Seguros y Fondos de Pensiones en relación con contratos de grandes riesgos, seguros colectivos o planes de pensiones que instrumenten compromisos por pensiones de las empresas con sus trabajadores o beneficiarios que no se refieran a la condición de usuario de servicios financieros de las entidades aseguradoras o gestoras de fondos de pensiones; (x) cuando haya transcurrido el plazo de prescripción de acciones o derechos conforme a la normativa o contrato correspondiente y, en todo caso, hasta transcurridos seis años desde que se produjo el hecho sin haber presentado la queja o reclamación.

En el supuesto de que se inadmitan se deberá poner de manifiesto al interesado mediante informe motivado otorgándole el plazo hábil de diez días para alegar. Si el interesado ha contestado y se mantiene la causa de inadmisión, se le comunicará la decisión final adoptada.

En cuanto a la tramitación de las reclamaciones, el artículo 11 de la Orden reconoce que una vez que se abra un expediente por cada una de las reclamaciones, en el plazo de diez días hábiles se informará al interesado de las acciones que le asisten para hacer valer sus derechos así como de los plazos y cauces para su ejercicio. Dentro de ese mismo plazo, se remitirá a la entidad contra la que se dirija una copia de la reclamación para que en el plazo de quince días hábiles presente alegaciones. De éstas últimas, se remitirá copia al reclamante quien podrá pronunciarse sobre las mismas en el plazo de quince días hábiles.

En el caso de que se plantee en la reclamación controversia entre las alegaciones de la reclamante y la entidad reclamada, corresponderá a la entidad fundamentar las suyas.

Transcurrido el plazo sin que la entidad haya formulado contestación o, transcurrido el plazo de alegaciones sin que, la entidad reclamada conteste o



bien alguna de las partes no muestre su disconformidad, se emitirá el informe que dará por terminado el expediente.

El expediente concluye a través de un informe que deberá emitirse en el plazo máximo de cuatro meses, a contar desde la fecha de presentación de la reclamación en el servicio de reclamaciones correspondiente. El informe será motivado y deberá contener unas conclusiones claras de las que resulte si de lo actuado hay un quebrantamiento de normas de transparencia y protección, y si la entidad se ha ajustado o no a las buenas prácticas y usos financieros. El expediente debe pronunciarse sobre todas las cuestiones que planteen las reclamaciones.

El informe se notifica a los interesados y a la entidad reclamada en el plazo de diez días hábiles a contar desde su emisión. Éste no tiene carácter vinculante y tampoco tiene consideración de acto administrativo recurrible.

En el caso de presentar una queja, su tramitación seguirá el mismo procedimiento que las reclamaciones pero con la particularidad de que los plazos son menores (el plazo para emitir el informe es de tres meses como máximo desde la fecha de presentación de la queja al servicio de reclamaciones competente).

Si el informe emitido en el expediente fuera desfavorable a la entidad reclamada, deberá comunicar en el plazo de un mes desde la notificación, si acepta o no los criterios manifestados en el mismo. Y en el caso de que los acepte, deberá acreditar documentalmente haber rectificado la situación. El incumplimiento de este deber, se entiende como que la entidad rechaza el informe. Una vez que la comunicación ha sido recibida o que el plazo ha transcurrido, las reclamaciones se archivan.

Se contempla la posibilidad de que los interesados desistan de las reclamaciones en cualquier momento del procedimiento. Este desistimiento supone la terminación del procedimiento sin perjuicio de la posibilidad de que

el servicio de reclamaciones competente acuerde su continuación por motivos de interés general.

En el caso de las consultas, de forma idéntica a lo que ocurre con las reclamaciones y las quejas, pueden plantearse ante cualquier servicio de reclamaciones con independencia de su contenido. Se podrán realizar en soporte papel o soporte electrónico por medio de los registros habilitados al efecto y deberán contener necesariamente: (i) identificación de la persona o entidad a que se refiere la consulta; (ii) los antecedentes y las circunstancias concurrentes; (iii) las dudas suscitadas; (iv) los datos y elementos que puedan contribuir a la formación de una opinión; y (v) el lugar, la fecha y la firma.

Las consultas no pueden referirse a una concreta operación con una entidad determinada, ni a las condiciones materiales de las operaciones siempre que se ajusten a las normas de transparencia y protección de la clientela ni a los contratos de seguros por grandes riesgos.

En el supuesto de que la solicitud no reúna los requisitos, se requerirá al interesado para que subsane la falta en el plazo de diez días hábiles, con indicación de que si no procede a su subsanación se archivará el escrito sin más trámites.

Una vez planteada, el servicio de reclamaciones deberá contestar en el plazo máximo de un mes desde la fecha de la presentación de la consulta en el servicio de reclamaciones correspondiente. Las consultas tienen carácter informativo y carecen de efectos vinculantes.

## 5. Concepto y Naturaleza del whistleblowing y el whistleblower

El whistleblowing<sup>419</sup> es uno de los métodos más efectivos para resolver y descubrir fraudes societarios, actos de corrupción, malas prácticas, abusos en las empresas y en general actos faltos de ética.

El whistleblowing consiste en denunciar un hecho ilegal y/o contrario a la normativa interna de la empresa, de buena fe, a sabiendas de su veracidad, con el propósito firme de actuar correctamente. El whistleblower puede ser cualquier trabajador, empleado, directivo de la empresa o terceras personas – física o jurídica– que, debido a su relación con la empresa, sea conocedor del hecho o acto denunciado y denunciante, siempre con el carácter de confidencial y ante la persona o personas que más confianza genere al whistleblower (superior en la empresa, oficial de cumplimiento normativo, director de recursos humanos, jurídico, director general)<sup>420</sup>.

El whistleblowing comprende aquellos actos de delación realizados por sujetos que están o han estado vinculados con una determinada organización, ya sea administrativa o empresarial, en la que se ha cometido una conducta ilícita<sup>421</sup>. Se distingue entre whistleblowers internos y externos, en función de si quien denuncia lo hace directamente ante terceros

---

<sup>419</sup>El Black's Law Dictionary define el Whistleblower como "An employee who reports employer wrongdoing to a governmental or law-enforcement agency. •Federal and state laws protect whistleblowers from employer retaliation. [Cases: Master and Servant 30 (6.35); Officers and Public Employees 66. C.J.S. Employer- Employee Relationship §§ 69, 78; Officers and Public Employees §§ 121, 150-158.] – whistleblowing, n.". Asimismo describe el Whistleblower act como "A federal or state law protecting employees from retaliation for disclosing employer wrongdoing, as during an investigation by a regulatory agency. • Federal laws containing whistleblower provisions include the Whistleblower Protection Act (5 USCA § 1211), the Occupational Safety and Health Act (29 USCA § 660), CERCLA (42 USCA § 9610), and the Air Pollution and Control Act (42 USCA § 7622). [Cases: Master and Servant 30 (6.35); Officers and Public Employees 69.7. C.J.S. Employer – Employee Relationship §§ 69, 78; Officers and Public Employees §§ 133, 164-166.]. Black's Law Dictionary, 8ª ed., edit. B.A. Garner, 2004, p. 1627.

<sup>420</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., pp. 1212-1214.

<sup>421</sup>Para más detalles sobre este fenómeno RAGUÉS I VALLÉS, "¿Héroes o traidores?...", ob. cit.

(autoridades o medios de comunicación) o si primero informa a los responsables de la organización<sup>422</sup>.

El canal de denuncias (o sistemas de whistleblowing) es el mecanismo interno establecido en una organización que permite comunicar de forma confidencial y, en consecuencia detectar o prevenir posibles irregularidades, actos indebidos, comportamientos contrarios a la legislación vigente y/o a la normativa interna de la compañía que se estén realizando dentro de la misma y que puedan suponer para ésta algún tipo de responsabilidad penal, civil o administrativa<sup>423</sup>. Una definición es la de "revelar información acerca de las malas prácticas, ilegales o inmorales llevadas a cabo por un directivo de una empresa, o por empleados bajo el control de los directivos sobre personas físicas o jurídicas y que dichas acciones pudieran provocar consecuencias negativas"<sup>424</sup>.

La implantación de este canal de denuncias internas posee doble vertiente: por permitir a la sociedad reaccionar ante el conocimiento de determinados actos irregulares o ilegales ya cometidos (reactivo); y puede ayudar a inhibir a una persona de realizar algún comportamiento irregular o ilegal que, sin la existencia de este canal de reporte, pudiera estar tentado a realizar (preventivo)<sup>425</sup>.

Se puede diferenciar dos conceptos distintos que pueden denominarse whistleblower y el informante.

El informante es la persona que ha estado o está relacionada directa o indirectamente con hechos ilegales o poco éticos y que, debido a su posición

---

<sup>422</sup>La distinción es aceptada también en los Estados Unidos y Alemania: para las oportunas referencias cfr. LUTTERBACH, C., "Die strafrechtliche Würdigung...", ob. cit., p. 38

<sup>423</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 613-614.

<sup>424</sup>MICELI, M./ NEAR, J./ DWORKIN, T.M., *Whistle-blowing in organizations*, edit., Routledge, New York, 2008, p. 6; JUBB, P., "Whistleblowing: A restrictive Definition and Interpretation", *Journal of Business Ethics*, nº 74, 1999, pp. 77-94.

<sup>425</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 614.

activa en los hechos, revela otras actuaciones llevadas a cabo por terceras personas para poder atenuar o eximir su responsabilidad. El whistleblower es la persona que, actuando de buena fe, de manera veraz, denuncia unos hechos contrarios a la ley y/o a las normas éticas de la empresa con objeto de hacer un bien a la sociedad, siendo necesaria una debida protección contra represalias del gobierno, empresarios y/o directivos o compañeros de trabajo, porque de lo contrario tendría poco sentido práctico, humano y personal la figura del whistleblower.

Al whistleblower, antes de proceder a denunciar un hecho o acto ilegal y/o contrario al código ético, se le presentan dos dilemas fundamentalmente: por un lado un conflicto entre lo personal (miedo a las represalias y al despido y a todo lo que pueda conllevar, miedo a no pagar las facturas, colegios e hipoteca de la vivienda, miedo a no poder volver a trabajar, etc.– y el deber de actuar correctamente, y un conflicto entre las obligaciones contraídas para con la empresa que le ha contratado y otras partes involucradas.

El término anglosajón "whistleblowing" es una palabra compuesta por el nombre "whistle" (silbato) y el verbo "to blow" (soplar), y literalmente significa "tocando el silbato", hay autores que sostienen que hace referencia al silbato utilizado por la policía londinense y otros se refieren al que utilizan los árbitros en las competiciones deportivas para advertir de la comisión de faltas o jugadas ilegales. Por lo tanto, parece bastante evidente que responde a la finalidad de dignificar la figura del denunciante o "whistleblower" frente a otras posibles definiciones tales como "soplón", "delator" o "chivato", que resultan manifiestamente peyorativas<sup>426</sup>.

Las palabras whistleblower o whistleblowing no debieron ser utilizadas en sentido despectivo, con connotaciones de "traidor" "chivato". Es un instrumento para descubrir hechos graves, malas prácticas llevadas a cabo

---

<sup>426</sup>KOHN, S. M., *The Whistleblower Handbook. A step-by-step Guide to Doing What's Right and Protecting yourself*, edit., Lyon Press, 2011, p. 5.

en las empresas, perjudican a ciudadanos y/o trabajadores o que pueden llegar a provocar en la sociedad riesgos contra la salud, el medioambiente, la alimentación, la energía, la banca, la economía, etc.<sup>427</sup>.

C. Fred Alford describe en su libro *"Broken lives and organizational power"* cómo la mayoría de los autores que han escrito sobre whistleblowers relatan a unos héroes nobles que están orgullosos de lo que han hecho y volverían a hacerlo sin dudarlo, sin embargo él al entrevistarse con muchos de ellos tuvo una experiencia muy contraria: personas que habían roto su vida y que su familia y amigos les habían dado la espalda y que jamás tuvieron ningún reconocimiento público.<sup>428</sup>

Hay incluso quien ha manifestado su escepticismo sobre la efectividad y legitimidad de estos instrumentos. Así el catedrático alemán R. HEFENDEBL, en su trabajo titulado irónicamente "Alle lieben Whistleblowing"<sup>429</sup>, publicado en 2009<sup>430</sup>, cuestiona con datos concretos que estos sistemas sean tan efectivos como suele mantenerse. Hefendehl sostiene que el fomento de las delaciones es contrario a valores esenciales que definen el modelo vigente de sociedad, en el que la imposición de deberes de solidaridad a ciudadanos es algo excepcional<sup>431</sup>. Según este autor, estos deberes de solidaridad no incluyen una obligación de denunciar dirigida a todos los ciudadanos cuando ya no existe ningún bien jurídico susceptible de salvación pues la persecución penal "es un dominio exclusivo del Estado" aun cuando el delito haya acontecido en una empresa y, este "modelo de vigilancia" no debería convertirse en la regla. Hefendehl considera que un modelo basado en la intromisión de los particulares en la actividad de persecución del delito es

---

<sup>427</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., pp. 1212-1213.

<sup>428</sup>ALFORD, C. F., *Whistleblowers: Broken Lives and Organizational Power*, edit. Cornell University, 2001.

<sup>429</sup>Cuya traducción sería "todos aman el Whistleblowing".

<sup>430</sup>HEFENDEHL, R., "Alle lieben Whistleblowing", en AA.VV., *Grundlagen des Straf- und Strafverfahrensrechts. Festschrift für Knut Amelung*, dirs. Böse/Sterneberg-Lieben, Berlín, 2009, pp. 617-643.

<sup>431</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 168-169.

antiliberal y resulta propio de la policía de sistemas totalitarios como ocurría en la antigua República Democrática Alemana, en la que la Stasi tenía una extensa red de informantes<sup>432</sup>.

En España Goñi Sein, pese a posicionarse en general a favor de la legitimidad de tales sistemas, han mostrado reticencias en consideración a los derechos del sujeto denunciado, poniendo en evidencia cómo "la denuncia conlleva el riesgo de estigmatización y exclusión"<sup>433</sup>.

En este documento el Grupo de Trabajo europeo *"enfatisa que los programas de denuncia de irregularidades conllevan un riesgo muy grave de estigmatización y vejación de dicha persona dentro de la organización a la que pertenece. La persona queda expuesta a esos riesgos incluso antes de saber que ha sido incriminada y de que los supuestos hechos se hayan investigado para determinar o no su fundamento"*<sup>434</sup>.

Más allá de las dudas de legitimidad que pueden suscitar estos sistemas, también su eficacia en términos preventivos es discutida. Existen estudios que les atribuyen gran parte del mérito en el descubrimiento de determinados delitos, mientras que otros trabajos cuestionan el que esa contribución sea real<sup>435</sup>. Aquellas empresas que ofrecen entre sus servicios la implantación de estos sistemas proclaman que estos son "el medio más efectivo de descubrir la criminalidad de cuello blanco", asegurando que en las compañías que no cuentan con ellos existe el doble de probabilidades de comisión de delitos, ya

---

<sup>432</sup>LUTTERBACH, C., "Die strafrechtliche Würdigung...", ob. cit., pp. 42 y ss., trata de matizar algunas de las críticas de Hefendehl.

<sup>433</sup>GOÑI SEIN, J. L., "Sistemas de denuncia...", ob. cit., p. 330. Por su parte, MORATO GARCÍA, R.M., "Incumplimiento de los códigos...", ob. cit., p. 442, alude a que "se corre el riesgo de que la política empresarial termine por producir un profundo desgarramiento a la solidaridad colectiva".

<sup>434</sup>AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Creación de denuncias internas en las empresas (mecanismos de whistleblowing)", Informe Jurídico 2007/128, p. 7.

<sup>435</sup>Ver, por ejemplo las referencias aportadas en tal sentido por HEFENDEHL, FS-Amelung, 2009, p. 625 y ss.

que la mera existencia de estos procedimientos ya tiene un efecto disuasorio para los potenciales infractores<sup>436</sup>.

El que numerosas instituciones recomienden la inclusión de estas medidas y el que cada vez más empresas cuenten con ellas, obliga a recomendar a cualquier compañía -sobre todo de tamaño mediano o grande- que se dote de estos procedimientos, pues a medio plazo el no tenerlos puede ser valorado por jueces o fiscales como un síntoma de escasa sensibilidad ante la necesidad de contribuir al descubrimiento y la prevención del delito. El que su coste económico no sea especialmente elevado es un argumento adicional a favor de su implantación. El no implantar este mecanismo puede suponer cargas alternativas de peso superior, como implantar otros medios más costosos de prevención del delito o tener que dar numerosas explicaciones en caso de imputación penal<sup>437</sup>.

---

<sup>436</sup> Así, por ejemplo, <http://www.business-keeper.com/whistleblowing-and-compliance.html>.

<sup>437</sup> RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 169-170.



## V. LAS DENUNCIAS INTERNAS COMO MANIFESTACIÓN DEL WHISTLEBLOWING

Como hemos visto, todo programa de cumplimiento destinado a la prevención del delito debe de incluir un mecanismo de *whistleblowing* o de denuncia interna. Las empresas establecen estos canales o cauces de información para que cualquier empleado, agente o representante que detecte alguna conducta potencialmente criminal o un incumplimiento grave del programa de cumplimiento de la compañía, pueda denunciar o poner el hecho en conocimiento del órgano encargado del control y supervisión de la prevención penal, con garantías de confidencialidad y sobre todo pudiendo garantizar el anonimato del denunciante.

Tal y como ha quedado señalado, los antecedentes de este mecanismo de denuncia interna los encontramos en la promulgación de la SOX de 2002 el 30 de julio de 2002 en Estados Unidos. Con esta ley se indujo al Gobierno estadounidense a adoptar medidas para combatir la corrupción, siendo una de ellas la obligación de las empresas de implantar un sistema de recepción y tramitación de denuncias internas, relativas a la gestión contable o de auditorías internas, garantizando a los denunciantes la protección frente a posibles represalias por parte de las compañías<sup>438</sup>.

En nuestro país, no es hasta el Código Unificado del Buen Gobierno de fecha 19 de mayo de 2006 de la Comisión Nacional del Mercado de Valores cuando se instaure la implantación de dicho canal como una recomendación. A su vez recogido en el Código de Buen Gobierno de las Sociedades Cotizadas de 2015.

No obstante, y aunque el sistema está establecido en muchas empresas tanto españolas como extranjeras (principalmente multinacionales), ya sea por los condicionantes impuestos para operar en los mercados de valores

---

<sup>438</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 395-396.

estadounidenses o por una cuestión de estética corporativa más que por convicción en su eficacia, lo cierto es que los sistemas de denuncias internas en España no terminan de arraigar.

Es una realidad que hay cierta resistencia interna a utilizar dichos mecanismos de denuncia en nuestro país, bien porque la delación de superiores y compañeros no está bien vista en nuestra cultura, o bien por el medio a las represalias, o por una mezcla de las anteriores razones.<sup>439</sup>

## **1. Las denuncias internas y la responsabilidad penal**

Hay una indudable conexión entre la implantación y el uso efectivo de un sistema interno de denuncias y la responsabilidad penal de la persona jurídica en la que se ha instaurado dicho procedimiento, pudiendo tener un impacto muy significativo sobre los administradores, cargos directivos o sobre aquellos que trabajan en ella<sup>440</sup>.

No podemos olvidar que, en términos jurídico-penales, la existencia de un sistema interno de denuncias puede tener una importante repercusión en las personas físicas que trabajan en una empresa, además de constituir un requisito que podría contribuir a atenuar o a eximir la responsabilidad de la persona jurídica.

En este análisis, es necesario distinguir entre aquellos casos en los que la conducta delictiva denunciada ya ha finalizado y aquellos otros en los que la denuncia se refiere a hechos ilícitos de comisión futura, continuada o permanente. Es por ello que tiene especial interés determinar la responsabilidad de los cargos superiores al sujeto que haya ejecutado materialmente la conducta delictiva.

---

<sup>439</sup>Para un análisis más detenido, RALLO LOMBARTE, A. "Whistleblowing" (sistemas internos de denuncia) y protección de datos", *Cuadernos de derecho para ingenieros*, vol. 14, Cumplimiento normativo. Compliance, coord. M. A. Agúndez, J. Martínez-Simancas Sánchez, pp. 97-118.

<sup>440</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. p. 170.

De esta forma, para poder configurar la vinculación que existe entre las denuncias internas y la posible responsabilidad penal, se debe partir de aquellos supuestos en los que el superior no tiene conocimiento de la conducta delictiva hasta que recibe la denuncia de un subordinado. Se considera que los superiores adquieren una posición de garantes ya que una vez que reciben la denuncia, adquieren el deber específico de evitar la comisión de delitos por parte de los empleados, en los términos del art. 11 CP.

A estos efectos, debe recordarse que la omisión del deber de denunciar delitos ya terminados no es constitutiva en España de infracción penal. La LECr establece (art. 264<sup>441</sup>) que quien por cualquier medio tiene conocimiento de la perpetración de algún delito de los que deben perseguirse de oficio debe denunciarlo, pero dicha previsión no viene acompañada de ninguna sanción si se incumpliese. Sólo en el caso de que los máximos responsables de la compañía colaboren con el sujeto responsable con conductas encuadrables en el delito de encubrimiento o de receptación, se les podrá atribuir a aquéllos algún tipo de responsabilidad penal<sup>442</sup>.

Es importante señalar que una vez que las empresas deciden dotarse de un procedimiento de denuncias internas, y los responsables recibir la información, si estos no actúan en consecuencia y no dan los pasos necesarios para obtener la información que dicho sistema les puede proporcionar, la mera obtención de la misma puede tener efectos incriminatorios.

---

<sup>441</sup>El artículo 264 LECr. Cuyo epígrafe es "Colaboración con la justicia" dispone que el que por cualquier medio diferente de los mencionados tuviere conocimiento de la perpetración de algún delito de los que deben perseguirse de oficio, deberá denunciarlo al Ministerio Fiscal, al Tribunal competente o al Juez de instrucción o municipal, o funcionario de policía, sin que se entienda obligado por esto a probar los hechos denunciados ni a formalizar querrela. El denunciador no contraerá en ningún caso otra responsabilidad que la correspondiente a los delitos que hubiese cometido por medio de la denuncia, o con su ocasión.

<sup>442</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 170-171.

De esta forma, en el caso de que la conducta se esté cometiendo de manera continuada o se trate de un delito permanente o futuro, a partir del momento en que los máximos responsables de la empresa y todos los que tengan el deber de evitar la conducta ilícita, tienen conocimiento del hecho delictivo, podría apreciarse que incurren en el dolo necesario para ser considerados corresponsables del delito del empleado, bien como autores accesorios o como cooperadores necesarios, según la posición que se defienda sobre el alcance de estas figuras. La responsabilidad puede darse incluso en los casos en los que la víctima de la conducta delictiva sea la propia empresa, pues en tal supuesto los socios podrían exigir responsabilidad al directivo o administrador que no hubiera evitado tales comportamientos.

Desde el punto de vista de la responsabilidad de las personas físicas, la previsión de canales de denuncia tiene fundamentalmente un efecto incriminatorio para los cargos directivos, pero solo cuando el objeto de la información sean conductas delictivas presentes o futuras. Por ello, su consecuencia principal es la de dotar a esos sujetos con aquellos conocimientos requeridos por el dolo como elemento imprescindible de la tipicidad subjetiva de la gran mayoría de delitos con trascendencia en la actividad empresarial<sup>443</sup>.

El Derecho español cuando se alude a las medidas de previsión que se consideran más adecuadas, no falta entre ellas la previsión de un procedimiento de denuncia<sup>444</sup>. El hecho de contar con un procedimiento interno de denuncia puede ser un factor a tener en cuenta tanto para atribuir

---

<sup>443</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 171-172.

<sup>444</sup>Entre los elementos comunes y más habituales en los diversos planes de prevención de riesgos de comisión delictiva Ortiz de Urbina Gimeno alude a los siguientes: 1) El análisis de riesgos penales; 2) La previsión de un código de conducta; 3) Un sistema de información para canalizar las denuncias de posibles whistleblowers; 4) La identificación de las líneas de responsabilidad; y 5) El seguimiento interno y externo del programa y su revisión periódica (ORTIZ DE URBINA GIMENO, I., "Responsabilidad penal de las personas jurídicas y programas de cumplimiento empresarial ("compliance programs")", en AA.VV., *Ética empresarial y códigos de conducta*, dir. J.L. Goñi, Madrid, 2011, pp. 128-129. También ALONSO GALLO, J., "Los programas de cumplimiento", ob. cit., p. 166, alude a estos procedimientos como elemento básico los programas de cumplimiento).

responsabilidad a la persona jurídica como para valorar esa responsabilidad y cuantificar la correspondiente sanción.

Además, la previsión de estos procedimientos puede tener relevancia con respecto a la posibilidad de atribuir responsabilidad penal a la persona jurídica.

La doctrina discute si los casos de omisión imprudente del debido control deben dar lugar a responsabilidad, pero existe consenso en que sancionar a la empresa por delitos imprevisibles de sus empleados supondría una vulneración del principio de culpabilidad por lo que sería un supuesto de mera responsabilidad objetiva<sup>445</sup>.

Ya hemos hecho referencia a que en el Derecho penal español adquiere especial importancia la disposición de canales de denuncia interna como uno de los instrumentos que, junto con otros, puede permitir al juez entender que la empresa ha contado efectivamente con esas medidas y que la realización de un concreto delito era algo imprevisible para la compañía (supuestos en los que habiendo procedido la empresa de manera plenamente diligente en la implantación de mecanismos de control para evitar la comisión de delitos por parte de sus trabajadores, dicho delito se habría cometido finalmente por razones que a priori cabría calificar de imprevisibles).

La eficacia de las medidas de descubrimiento y prevención previstas por una empresa no puede limitarse a la valoración de la efectividad de una sola medida, sino del conjunto de éstas, a través de una apreciación global.

---

<sup>445</sup>Que la responsabilidad de las personas jurídicas no puede concebirse de manera exclusivamente objetiva es algo que se admite abiertamente, por ejemplo, en la Circular 1/2011 de la Fiscalía General del Estado, p. 35. Cfr. asimismo las consideraciones al respecto de ALONSO GALLO, J., "Los programas de cumplimiento", ob. cit., pp. 156-159, a propósito de los llamados "programas de cumplimiento" como medidas de prevención del delito; señala este autor (ibídem, p. 159) que, a su juicio, aunque esta valoración deberá llevarse a cabo ex ante en la práctica muy probablemente tendrá lugar ex post, por lo que "el riesgo de condena existe aun con programa de cumplimiento efectivo".

No es suficiente la mera previsión formal de este procedimiento para que un juez pueda llegar a establecer que la existencia de un procedimiento de denuncia, junto con otras medidas, supone que la empresa está ejerciendo el debido control sobre sus empleados, sino que será necesario acreditar que el sistema realmente estaba disponible en el momento en el que hecho delictivo tiene lugar y que además, se estaba aplicando en unas circunstancias que permitan considerar que contribuía de manera efectiva al descubrimiento y prevención del delito. Para poder negar la responsabilidad de una persona jurídica, puede tener un interés notable, en caso de que sea posible, que la empresa pueda acreditar haber descubierto (y denunciado) el delito cometido por su empleado a través de este procedimiento; o bien, al menos, haber descubierto (y denunciado) otros hechos con anterioridad, aunque fueran distintos del caso concreto. Por ello, estos programas deben contener los elementos necesarios que permitan responder a la finalidad de desempeñar un papel importante en la valoración del juez sobre la efectividad de estos sistemas, contribuyendo a mostrar al juez el compromiso permanente de la empresa con el cumplimiento normativo y la eficacia del procedimiento de denuncia que cuando se trate de demostrar que la comisión puntual de un delito fue algo imprevisible para la compañía y sus directivos, adquiere una importancia esencial<sup>446</sup>.

## **2. Las denuncias internas y los derechos de los empleados**

A continuación se analizará la tensión que existe ente el objetivo legítimo de cumplir con las políticas y procedimientos de cumplimiento efectivo para reducir el riesgo de una posible responsabilidad penal y los derechos subjetivos fundamentales de los empleados, en la medida en que los primeros representan muchas veces una injerencia en la esfera de la autonomía e intimidad del personal de trabajo.

---

<sup>446</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. p. 174.

Por ello, interesa analizar como convive el canal de denuncias y su consiguiente procedimiento de investigación con los derechos de los trabajadores. Destacan especialmente la protección de la intimidad personal del whistleblower (singularmente, del derecho a la confidencialidad de la denuncia), y la protección de sus derechos laborales como veremos a continuación.

## **2.1 Derecho a la intimidad y la protección de datos**

Cuando los órganos de dirección de la empresa o, en su caso, el *compliance officer* tengan fundada sospecha de que alguno de los miembros de la compañía podría haber incurrido en alguna irregularidad o, incluso, en algún delito a través de los canales de denuncia por parte de trabajadores (*whistleblowing*) deben llevar a cabo una investigación interna para la averiguación de los hechos.

Dependiendo de cómo se realicen tales investigaciones, la prueba puede ser lícita o ilícita. Puede ser lícita en el sentido del art. 11.1 Ley Orgánica 6/1985 de 1 de julio del Poder Judicial y, por tanto, válida para fundamentar un despido disciplinario del trabajador objeto de la investigación o la condena por un delito, o bien todo lo contrario, esto es, ilícita, e, incluso, eventualmente constitutiva de un delito contra la intimidad o el secreto de las comunicaciones del trabajador.

Por tanto, resulta imprescindible establecer unos criterios claros en las investigaciones privadas de una compañía que permitan conocer con claridad cuándo la obtención de la prueba se ha realizado por medios lícitos y cuando no.

De especial importancia es el cuerpo jurisprudencial construido en España en el ámbito del Derecho laboral como consecuencia del análisis de si las pruebas obtenidas por el empresario a efectos de acreditar la existencia de motivos de despido disciplinario, vulneran o no algún derecho del trabajador.

A tales efectos, adquiere relevancia no sólo la jurisprudencia vertida sobre la materia por el Tribunal Supremo, sino, en especial, las numerosas resoluciones del Tribunal Constitucional por la hipotética vulneración de derechos fundamentales del trabajador, singularmente de su derecho a la intimidad y al secreto de las comunicaciones<sup>447</sup>. No olvidemos que la Constitución Española reconoce la dignidad de la persona en el art. 10 y que el art. 18.4 dispone que *“la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*.<sup>448</sup>

La complejidad de la gestión de estos canales y el tratamiento de información sensible que se llevaba a cabo como consecuencia de las investigaciones internas iniciadas para la averiguación de los supuestos delitos denunciados a través de los canales de denuncia, motivó la elaboración del ya citado estudio jurídico por parte de la AEPD, Informe Jurídico 128/2007 que plantea la conformidad del sistema interno de denuncia con lo dispuesto en la LOPD.

En dicho informe, la AEPD, inspirándose en la tratada Opinión 1/2006 (sobre aplicación de las normas de protección de datos de la Unión Europea a los mecanismos internos de whistleblowing en el ámbito de la contabilidad y los controles internos de auditoría, la lucha contra la estafa y los delitos bancarios y financieros) del Grupo de Trabajo del Artículo 29 creado por la Directiva 95/46/CE, concluye que el whistleblowing será conforme a la LOPD siempre que cumpla los siguientes requisitos:

- El sistema debe permitir la denuncia de *“comportamientos, acciones o hechos que puedan constituir violaciones tanto de las normas internas*

---

<sup>447</sup>GOMEZ MARTIN, V., "Compliance y derechos de los trabajadores", en AA.VV., *Responsabilidad de la Empresa y Compliance. Programas de prevención, detección y reacción penal*, dirs. S. Mir Puig, M. Corcoy y V. Gómez, Madrid, 2014, pp. 432-433.

<sup>448</sup>SARACIBAR, E./ GONZALEZ, C., "Privacidad y protección de datos", en AA.VV., *Compliance. Cómo gestionar los riesgos normativos en la empresa*, coord. C.A. Sáiz Peña, Pamplona, 2015, p. 211.



de la compañía como de las leyes, normativas o códigos éticos” que rigen su actividad.

- Todos los empleados de la empresa deben poder ser denunciados o denunciados por el canal de denuncias.
- Los empleados serán previamente informados de la existencia y objetivo del canal, de cómo funciona, de la garantía de confidencialidad de los datos del denunciante y la garantía de información al denunciado de la existencia de la denuncia. La información deberá figurar en el contrato de trabajo.
- El procedimiento de denuncia será telefónico o presencial.
- Sólo accederán, en principio, a los datos el responsable de *compliance counter* y las personas imprescindibles a fin de investigar los hechos denunciados.
- Además, el sistema incorporará los datos de denunciante y denunciado, los hechos denunciados y el resultado de las investigaciones.
- Se informará al denunciado en el plazo más breve posible de los hechos denunciados, los destinatarios de la información, el departamento responsable del sistema y sus derechos en materia de protección de datos.
- No se informará de la identificación del denunciante a menos que éste hubiera obrado con mala fe.
- Y, por último, los datos serán cancelados en un plazo máximo de dos meses tras el fin de las investigaciones si los hechos no hubieran sido probados. En caso de entablarse acciones, los datos se conservarán en tanto sea necesario para el ejercicio por la compañía de sus derechos en juicio<sup>449</sup>.

A juicio de la AEPD, debe partirse del establecimiento de procedimientos que garanticen el tratamiento confidencial de las denuncias presentadas a través

---

<sup>449</sup>AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Creación de denuncias internas en las empresas (mecanismos de Whistleblowing)", Informe Jurídico 2007/128, pp. 1 y ss.

de los sistemas de *whistleblowing*, de forma que se evite la existencia de denuncias anónimas, garantizándose así la exactitud e integridad de la información contenida en los mismos. En consecuencia, el establecimiento de mecanismos que garanticen la presentación de denuncias confidenciales, y no anónimas, no perjudicaría la operatividad del sistema, al deber quedar claramente planteada la conclusión de que los datos del denunciante en modo alguno podrían ser transmitidos al denunciado, con ocasión del ejercicio del derecho de acceso.

Según la LOPD, el tratamiento de datos de carácter personal requerirá el consentimiento inequívoco del afectado (art. 6.1), salvo que se refieran a las partes de un contrato o precontrato de una relación de negocios, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento (art. 6.2). La obtención de los datos deberá ser proporcionada, esto es, de datos *“adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido”*.

Como señala la AEPD, el sistema creado debe garantizar el ejercicio de los derechos establecidos en la LOPD, tanto en cuanto a la información específica referida al tratamiento de los datos y el posible ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición cuando proceda.

Resulta dudoso que el conjunto de presupuestos que debe concurrir para que los canales internos de denuncia no vulneren los derechos recogidos en la LOPD en favor del denunciante y el denunciado realmente garantice de forma suficiente tal protección. Por lo que, cabe preguntarse, por ejemplo, quién debe ser, en realidad, el receptor de la denuncia. Con otras palabras, a quién se está refiriendo la AEPD cuando se refiere al responsable del *compliance counter*. Podría concluirse que, muy probablemente, tal sujeto no es otro que el *compliance officer*, pero, a falta de regulación expresa de tal figura, otra

duda que se plantea es si el mismo puede ser un órgano interno de la empresa o debe encontrarse representado, en cambio, por un órgano externo. En el primer caso, será inevitable que la empresa tenga conocimiento de la identidad del denunciante (la denuncia es confidencial para el denunciado, no para su receptor); en el segundo caso, la identidad del denunciante permanecerá desconocida no sólo para el denunciado, sino también para el empresario. Además, en el supuesto de que los hechos denunciados den lugar a la incoación de un procedimiento penal, no es en absoluto obvio que el denunciante, que en un sistema de *compliance officer* externo tendría garantizada la reserva de su identidad, se encontrase legitimado para mantenerla frente al Ministerio Fiscal o el juez de instrucción. Con otras palabras: no es en modo alguno indiscutible que el *compliance officer* pueda dejar de informar -a requerimiento, por ejemplo, del juez de instrucción o del Ministerio Fiscal- sobre la identidad del denunciante, a efectos de una eventual declaración como testigo de los hechos denunciados. En tal caso, es evidente que la denuncia dejaría de ser confidencial.

En cuanto a los derechos del trabajador, la imposibilidad de conocer la identidad del denunciante a través del ejercicio del derecho de acceso reconocido por la LOPD podría suponer, a efectos prácticos, dejar prácticamente vacía de contenido su facultad de acceder al origen de la denuncia. Ciertamente, la AEPD establece una excepción a tal regla, consistente en los supuestos en que la denuncia ha sido formulada de mala fe. Sin embargo, se asiste, en relación a este particular, a una suerte de petición de principio: si el denunciado no puede conocer la identidad del denunciante, ¿cómo podrá demostrar (por ejemplo, por la existencia de una relación de enemistad entre ambos desconocida por la empresa) la concurrencia de motivos espurios reveladores de que la denuncia fue presentada de mala fe?<sup>450</sup>. De esta forma, el derecho a la intimidad y

---

<sup>450</sup>GOMEZ MARTIN, V., "Compliance y derechos de los trabajadores", ob. cit., pp. 449-450.

protección de datos se pone en relación con los derechos de los empleados y, en especial con los derechos de la persona inculpada.

En el contexto jurídico europeo, se ha interpretado que el mecanismo de denuncia interna de irregularidades afecta de lleno a la esfera del derecho a la protección de datos, toda vez que en él se recogen y se tratan datos de carácter personal, por lo general con absoluto desconocimiento del propio afectado. De ello se sigue que el sistema debe garantizar, en todo caso, a los empleados los derechos que reconoce la normativa de protección de datos LOPD.

En este sentido, el Grupo de Trabajo del Artículo 29, ha hecho especial hincapié en que, si bien la normativa y regulación sobre los procedimientos de denuncia omiten toda referencia a la protección de la persona denunciada, *“ésta tiene derecho a los beneficios que le conceden la Directiva 95/46/CE y las disposiciones correspondientes del Derecho nacional”*. Deja, así, muy claro que el establecimiento de sistemas de denuncia debe hacerse de acuerdo con los principios de protección de datos personales, según lo previsto en la Directiva 95/46/CE. Y ello porque *“los sistemas de denuncia de irregularidades implican un riesgo muy grave de estigmatización y persecución de esa persona en la organización a la que pertenece”*, pues *“quedará expuesta a tal riesgo incluso antes de que ella misma sea consciente de que ha sido inculpada y se hayan investigado los presuntos hechos para determinar si efectivamente se han producido”*<sup>451</sup>.

Por último, es importante hacer mención a que con fecha 21 de Abril de 2015 se celebró la 7ª Sesión Anual Abierta de la AEPD, planteándose la consulta de si la Agencia había cambiado las conclusiones en relación con el tratamiento de los datos en el marco de un canal de denuncias (informe 128/2007), tras la publicación de Ley Orgánica 1/2015 de 30 de marzo por la que se modifica el Código Penal. En particular, la consulta planteaba si

---

<sup>451</sup> GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 402-403.

estaría legitimado el tratamiento de los datos de clientes y proveedores en el marco de la prevención de delitos. A lo que respondió que *“ha venido considerando posible el establecimiento de los canales de denuncia siempre que se cumplan los requisitos establecidos en la Ley Orgánica de Protección de Datos de Carácter personal. La legitimación para el establecimiento de estos canales podría fundarse en el Art 7 f) de la Directiva 95/46/CE. Por ello, la mera referencia al colectivo afectado no sería suficiente para dar una respuesta definitiva a la cuestión, siendo necesario conocer qué tipo de actuaciones serían susceptibles de denunciarse en estos medios. La reforma de la legislación penal podría ayudar a justificar el interés legítimo prevalente, pero no bastaría por si sola para fundar el tratamiento. En particular la Agencia ha considerado necesario que las denuncias tengan carácter confidencial y no anónimo, si bien cabría la contratación de un encargado del tratamiento que conservase los datos identificativos de los denunciantes sin comunicarlos en ningún caso a la empresa”*.

## **2.2 Obligación de información previa**

Los empleados tienen el derecho a ser informados de la existencia de un mecanismo de supervisión y control del programa de ética para la detención de conductas criminales o de gravedad por parte de los propios empleados, siendo esta obligación de información previa un elemento verdaderamente ligado a la tutela de la intimidad y para la garantía de la protección de datos de carácter personal.

Ahora bien, esta supervisión del programa de cumplimiento no puede realizarse sin que, inevitablemente, suponga que el supervisor obtenga un cierto conocimiento directo de los comportamientos y circunstancias personales del trabajador. Y es que la verificación del cumplimiento implica, de alguna manera, entrar en la esfera de la intimidad de los empleados. De ahí que nuestra jurisprudencia requiera especial cautela como exigencia de una explicitación previa de la existencia de tales mecanismos de control como

condición de legitimidad del control, para evitar que se produzca una forma prohibida de control<sup>452</sup>.

En este sentido, el Tribunal Supremo en su sentencia de 26 de septiembre de 2007 valora con carácter decisivo la obligación de la empresa de cumplir (previamente a la adopción de la medida de control) con el deber de informar a los trabajadores de la existencia del control, con el fin de evitar cualquier expectativa de intimidad del empleado. La jurisprudencia considera que, si no se adopta una ética explícita sobre el uso y control de los medios facilitados por la empresa, algunos aspectos del comportamiento pueden caer en la esfera de protección del derecho a la intimidad, no excluyéndose del todo el carácter de intromisión ilegítima, de manera que el sistema de control realizado pueda no ser considerado conforme a derecho.

La decisión del Tribunal Supremo sobre el deber de informar<sup>453</sup>, avalada también por el Tribunal Constitucional<sup>454</sup>, debe ser tomada como punto de referencia para otras medidas de control sobre herramientas provistas de una especial intrusión, como, por ejemplo, el control sobre los trabajadores de telemarketing telefónico, consistente en la audición y grabación aleatorias de las conversaciones telefónicas entre trabajadores y los clientes para corregir los defectos de técnica comercial y disponer lo necesario para ello, porque constituye un imprescindible elemento de autocontrol en la conformación del espacio de intimidad en la relación laboral, al permitir que el funcionamiento del sistema de control dependa del propio sujeto pasivo de control, y éste pueda hacer un uso en todo momento coherente a la finalidad de los instrumentos manejados, evitando las actitudes de uso personales y preservando su intimidad en el lugar de trabajo.

A estos efectos resulta relevante en todo momento garantizar que la obtención de cualesquiera información relevante se ha llevado a cabo en

---

<sup>452</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 393-394.

<sup>453</sup>STS 5 de diciembre de 2013

<sup>454</sup>SSTC 241/2012 y 170/2013

cumplimiento de la legislación aplicable, incluyendo el establecimiento de las garantías procedimentales oportunas, los medios y protecciones pertinentes<sup>455</sup>.

Por otra parte, ha de tomarse en consideración que el sistema de control se basa, en la gran mayoría de las ocasiones, en el tratamiento de datos personales, esto es, en la recogida, registros y revelación de datos de los afectados. En este sentido, en virtud del art. 10 de la Directiva y el art. 5 de la LOPD, al regular la recogida de los datos, prevé que cuando los datos no son obtenidos directamente del interesado, el responsable del tratamiento deberá informar de forma expresa precisa e inequívoca acerca de la existencia, finalidad y funcionamiento del sistema, de los destinatarios de dicha información y de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación de los datos personales<sup>456</sup>.

Por todo ello, el responsable del programa de cumplimiento y quien preste dicho servicio por cuenta y orden del primero (*Compliance Officer*), tendrán el deber inexcusable de informar sobre la naturaleza y alcance de la supervisión puesta en marcha para el control del cumplimiento del plan de prevención de riesgos penales, especialmente sobre los gestores y destinatarios de dicha información<sup>457</sup>.

### **2.3 Protección al denunciante frente a un despido**

Por principio el trabajador y el empresario tienen una relación de desequilibrio de poder, el trabajador suele encontrarse en una situación de debilidad, lo que puede ser un elemento disuasorio a la hora de decidir denunciar una conducta irregular. Ante una situación así, no sería de extrañar que el trabajador tuviese miedo a que la empresa decidiera “reubicar” al trabajador

---

<sup>455</sup>LÓPEZ BARJA DE QUIROGA, J, “Las escuchas telefónicas y la prueba ilegalmente obtenida”. AKAL. 1989.

<sup>456</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 394-395.

<sup>457</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 395.

en un puesto de trabajo de peor condición (defraudando, de este modo, sus legítimas expectativas laborales) o, incluso, decidiera despedirlo.

Desde la perspectiva del trabajador denunciante, una de las cuestiones de mayor trascendencia reside, sin duda, en conocer cuáles pueden ser las consecuencias laborales de su denuncia. Se trata, en suma, de saber si se encuentra legitimado el empresario para despedir disciplinariamente (art. 54.2 TRLET) o reubicar en un puesto de trabajo de peor condición al trabajador que denuncia la existencia en la empresa de hechos que podrían ser constitutivos de delito, sobre la base de un supuesto quebrantamiento de la buena fe contractual (art. 5 TRLET)<sup>458</sup>.

En España, la cuestión se ha tratado a propósito de la reclamación por la vía del recurso de amparo ante el Tribunal Constitucional, de trabajadores despedidos por haber denunciado la comisión de irregularidades o, incluso, de delitos en la empresa para la que prestaban servicios. Salvo contadas excepciones<sup>459</sup>, la postura defendida de forma dominante por la jurisprudencia del Tribunal Constitucional ha sido la siguiente: atenta contra el derecho fundamental a la información (art. 20.1 d CE) el despido de un empleado por haber denunciado la existencia en la empresa de hechos noticiables y de interés general<sup>460</sup>. No obstante, si el empresario no trata de condicionar al trabajador antes de la denuncia para que no la interponga (en cuyo caso podría incurrir en un delito de obstrucción a la Justicia del art. 464 CP), sino que se limita a aplicar represalia al empleado después de que ésta

---

<sup>458</sup>RODRIGUEZ YAGÜE, C., "La protección de los *Whistleblowers...*", ob. cit., pp. 461 y ss. Sobre la buena fe contractual en las relaciones laborales, muy extensamente, CONDE MARIN, La buena fe en el contrato de trabajo. Un estudio de la buena fe como elemento de integración del contrato de trabajo, 2007, *passim*.

<sup>459</sup>Especialmente, STC 126/2003, de 30 de junio y votos particulares a la STC 57/1999, de 12 de abril.

<sup>460</sup>Por todas, SSTC 57/1999,12/4; 197/1998, 13/10; STCT 12/11/81; STSJ Baleares 21/9/05. En la doctrina, RAGUÉS I VALLES, *InDret* 3/2006, p. 11; RODRIGUEZ YAGÜE, C., "La protección de los *Whistleblowers...*", ob. cit., p. 464.



haya denunciado a la empresa, tal conducta es, desde la perspectiva del derecho positivo español, atípica<sup>461</sup>.

Puede concluirse, por tanto, que pese a la jurisprudencia constitucional y social en materia de despido, la posición del trabajador eventualmente denunciante de actividades ilícitas cometidas en el seno de la empresa es de franca debilidad frente a la misma, en especial cuando también él ha participado en la actividad que pretende denunciar. En tal caso, únicamente cuando el trabajador reciba la amenaza del empresario de ser denunciada la participación del primero en los hechos delictivos de referencia, quedará éste amparado por una eventual exención de responsabilidad criminal por su intervención en el delito objeto de revelación, siempre y cuando, además, denuncie las amenazas<sup>462</sup>. En ausencia de tal situación, el Código Penal apenas protege al delator, más allá de la presencia de contadas cláusulas de atenuación de la pena, como la circunstancia genérica del art. 21.4<sup>a</sup> CP<sup>463</sup>, o las previstas para supuestos de terrorismo o narcotráfico<sup>464</sup>.

## **2.4 Derecho a fiscalizar a un trabajador**

El Tribunal Constitucional español considera que la normativa laboral distingue en España entre dos casos radicalmente distintos. Por un lado, el registro de la persona del trabajador, su taquilla y sus efectos personales y, por otro, la supervisión de los medios que el empresario pone a disposición del trabajador para la producción (teléfono, ordenador, cuentas de correo

---

<sup>461</sup>RAGUÉS I VALLES, *InDret* 3/2006, p. 12.

<sup>462</sup>Tal posibilidad se encuentra recogida en el art. 171.4 CP, que dispone lo siguiente: "Si el hecho descrito en el apartado anterior consistiere en la amenaza de revelar o denunciar la comisión de algún delito el ministerio fiscal podrá, para facilitar el castigo de la amenaza, abstenerse de acusar por el delito cuya revelación se hubiere amenazado, salvo que éste estuviere castigado con pena de prisión superior a dos años. En este último caso, el juez o tribunal podrá rebajar la sanción en uno o dos grados".

<sup>463</sup>RODRIGUEZ YAGÜE, C., "La protección de los *Whistleblowers*...", ob. cit., 483 y ss.

<sup>464</sup>GOMEZ MARTIN, V., "Compliance y derechos de los trabajadores", ob. cit., pp. 451-452.

electrónico, etc.). El primer supuesto se encontraría recogido en el art. 18 del TRLET, el segundo, en el art. 20.3 del mismo texto legal<sup>465</sup>.

En el supuesto del registro personal a que se refiere el art. 18 del TRLET, se trata de una facultad excepcional del empresario sometida a una serie de estrictos límites. Por una parte se exige que el registro sea necesario *“para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa”*, y por otra, debe realizarse *“dentro del centro de trabajo y en horas de trabajo”*, para garantizar la presencia del trabajador o, en su caso, la *“asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible”*. Además, el registro habrá de *“respetar al máximo la dignidad e intimidad del trabajador”*.

De esta forma, la protección de la dignidad es genérica a todo tipo de intervención del empresario sobre la esfera del trabajador, mientras que la alusión a la intimidad se refiere a la taquilla ya que pese a ser titularidad de la empresa, se trata de un elemento cedido por ésta al trabajador para uso privado de éste, por lo que forma parte de su esfera de intimidad.<sup>466</sup>

Así pues, el registro corporal, el de la taquilla y el de los efectos del trabajador debe cumplir con una serie de exigencias tales como ser idóneo (útil para conseguir el fin legítimo pretendido), necesario (el mecanismo menos restrictivo para alcanzar el objetivo) y proporcionado en sentido estricto (que el objetivo perseguido, fundamento en la existencia de sospechas, compense

---

<sup>465</sup>Sobre el particular y en lo que sigue, por todos, OTERO GONZALEZ, "Delitos contra la intimidad, derecho a la propia imagen, inviolabilidad del domicilio de personas jurídicas y establecimientos abiertos al público", en *Memento Penal Económico y de la Empresa*, coord. Ortiz de Urbina Gimeno, 2011, pp. 341 y ss. En la doctrina laboral, destacadamente, MARTÍNEZ FONS, *El poder de control del empresario en la relación laboral*, 2002.

<sup>466</sup>GOMEZ MARTIN, V., "Compliance y derechos de los trabajadores", ob. cit., p. 433.

la restricción individual). Esto es, el registro personal debe ser en todo caso proporcionado en un sentido amplio<sup>467</sup>.

Respecto al segundo supuesto, la Sentencia del Tribunal Europeo de Derechos Humanos de 12 de enero de 2016<sup>468</sup>, reconoció como lícito el comportamiento de la empresa de ejercer un control sobre el uso por parte del empleado de las herramientas informáticas puestas a su disposición con el fin de desarrollar su actividad profesional, sin suponer dicha conducta una violación al derecho del respeto de la vida privada y familiar que establece el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, entendiendo el Tribunal que los mensajes instantáneos que el empleado intercambia con fines personales durante el horario de trabajo son material de la empresa.

En este sentido, la cuestión radica en delimitar hasta dónde puede llegar la empresa en su labor de control de cumplimiento normativo. La respuesta a la pregunta deviene compleja desde el momento en que las empresas se ven obligadas, por virtud del art. 31 bis CP, a adoptar un amplio espectro de comportamientos de control para alcanzar un nivel de seguridad razonable en cuanto a los niveles de cumplimiento en la empresa. Ante la ausencia de una norma que regule cómo deben ser esos controles, existe la tentación de apreciar en abstracto y de aplicar controles de alto nivel sin límite alguno a la posibilidad de accesos en las áreas de memorias del sistema informático.

---

<sup>467</sup>STC 26/9/07, F.J. 3º; 186/2000 un sentido parecido, ROMEO CASABONA, *Los delitos de descubrimiento y revelación de secretos*, 2004, p. 136. Acerca de la aplicación de este principio al ámbito laboral en supuestos de eventual restricción de derechos fundamentales, y, en particular, en los supuestos que nos ocupan, CONDE MARIN, *La buena fe en el contrato de trabajo. Un estudio de La buena fe como elemento de integración del contrato de trabajo*, 2007, pp. 354 y ss., en especial 365 y s. Para una exposición detallada del contenido del principio de proporcionalidad y su incidencia en todas las categorías del delito, por todos, MIR PUIG, "El principio de proporcionalidad como fundamento constitucional de límites materiales del Derecho penal", en *LH-Vives Antón*, II. 2009, pp. 1357 y ss.

<sup>468</sup>Caso Barbulescu contra Rumania. Sentencia de 12 enero 2016. TEDH 2016\1

El control legítimo de la actividad laboral es el que se conecta directa y exclusivamente al cumplimiento de la obligación del plan de actividades y no a cualquier otra actividad que exceda de tal cumplimiento.

Pero la facultad de control en el ámbito del cumplimiento normativo encuentra un límite en la investigación de todo aquello que tenga relación con los requisitos organizativos y obligaciones inherentes a la unidad de negocio o a la actividad prestacional del empleado, límite por otra parte nada fácil de determinar de antemano. Ello comporta que resulte prohibida la indagación de hechos que carezcan de esa conexión inmediata con las tareas y desempeños contractuales del empleado o con el fin último del sistema de control que es la identificación y persecución de conductas irregulares que atentan contra las normas éticas y los procedimientos internos de la empresa<sup>469</sup>.

## 2.5 La interpretación del deber de denunciar

La disciplina de los programas de *compliance* incluye a veces un *whistleblowing* obligatorio al configurar la denuncia de las irregularidades o prácticas detectadas por los empleados como un auténtico deber. De esta forma, en algunos programas, a la luz de los intereses generales preventivos de la compañía, se exige a los empleados denunciar ante los órganos de supervisión las posibles conductas irregulares, bajo amenaza de sanción disciplinaria, condicionando, así, la libre elección del empleado, por lo que al imponerse como un deber se crea un sistema de *whistleblowing* obligatorio<sup>470</sup>.

Pero cabe preguntarse qué legitimidad tienen las empresas para establecer dicha obligación. Es preciso señalar que en alguna sentencia se ha considerado justificada la sanción de despido impuesta a un empleado por haber silenciado las graves irregularidades acaecidas en la empresa. Así, en

---

<sup>469</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 390-391.

<sup>470</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 399-400.

la sentencia del TSJ de Cataluña de 15 de febrero de 2010, en la que el TSJ legitima la medida empresarial adoptada, por tratarse de un trabajador designado por la propia empresa para velar por el cumplimiento de los imperativos éticos y de transparencia en la empresa. En este caso, el trabajador había omitido comunicar al Consejo de Administración unos gastos de representación repercutidos a la empresa por el director general que resultaban exorbitados e infundados<sup>471</sup>.

Una primera lectura de dicha sentencia induce a creer que son legítimas estas medidas compulsivas de denuncia que pueden establecer los programas de cumplimiento. Debe ponerse de relieve, sin embargo, que el ámbito en el que se mueve la sentencia es el de una relación sustentada en la máxima confianza<sup>472</sup>, y no parece que sea aplicable a cualquier otra situación. Desde luego, no cabe discutir la legitimidad del criterio de valoración en el caso del trabajador sancionado, puesto que se había delegado justamente en él el ejercicio de la responsabilidad de control de la transparencia en la empresa, pero el problema es indudablemente más complejo en relación con los empleados comunes que no tienen asignada esa responsabilidad de control sobre el programa de ética<sup>473</sup>.

No obstante, se puede explorar si tal obligación constituye una manifestación del deber de buena fe contractual. Es una duda razonable que se puede plantear, a la vista de que, según los arts. 5. a) y 20.2 del TRLET, el deber de buena fe actúa como estándar de conducta en el cumplimiento de sus obligaciones contractuales para ambas partes.

Tal propuesta no parece, sin embargo, muy plausible. Si bien es posible atribuir a la buena fe la función integradora del contrato y de los derechos y obligaciones, resulta arriesgado recurrir a la buena fe como vía para justificar

---

<sup>471</sup> TSJ de Cataluña de 15 de febrero de 2010, Rec. Nº 6293/2009.

<sup>472</sup> Como señala MORATO GARCÍA, R.M., "Incumplimiento de los códigos...", ob. cit., p. 443.

<sup>473</sup> GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 400.

esta técnica de control, porque una interpretación extensiva podría terminar por exponer a parámetros subjetivos el ámbito del deber de denuncia, requiriendo un comportamiento abusivo y desproporcionado. De la buena fe no deriva un criterio seguro, ni como fórmula para completar la obligación de los trabajadores, ni como freno a la discrecionalidad del empresario.

Se debe partir del dato de que el deber de denuncia constituye una exigencia que limita la libertad de autodeterminación de la persona del trabajador, por lo que los incumplimientos que lo justifican han de interpretarse de manera restrictiva. En este sentido, el empleado sólo estaría obligado a denunciar aquellos hechos que constituyan un claro incumplimiento de las normas, que puedan reconducirse al plan de prevención, por lo que parece claro que esa revelación de informaciones internas ha de ceñirse a los comportamientos irregulares que revisten un interés público o social importante, o a las conductas ilícitas particularmente graves, en términos coherentes con su compromiso contractual.

Es relevante tener en cuenta que la exigencia del deber de denuncia se ha de corresponder con el hecho objetivo de que efectivamente lo sea, pues de lo contrario se incurriría en ejercicio abusivo y antisocial del derecho de la empresa a adoptar las reglas de organización más convenientes para proteger sus intereses. Se piensa, por tanto, que el deber de denuncia del empleado no puede surgir en casos tales como, por ejemplo, irregularidades de fácil fiscalización o poco relevantes desde el punto de vista del perjuicio económico que pueda causarse<sup>474</sup>.

Por otra parte, el riesgo de una eventual amenaza de represalia obliga al empresario también a ser diligente en el cumplimiento de proporcionar el debido grado de protección al empleado. No estaría justificado el deber si el empleador no previese a su vez una protección específica al que utiliza el sistema de denuncia de irregularidades, garantizándole la total indemnidad.

---

<sup>474</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 401-402.

Será por tanto desde el marco de dicha protección desde el cual habrá de definirse, también, la obligación del empleado de denunciar los hechos detectados.

En suma, la regularidad o conformidad del deber de denuncia dependerá de su adecuación a las finalidades propias del sistema, las circunstancias profesionales del autor del incumplimiento, los posibles perjuicios a la compañía y las garantías de protección de los denunciantes. Como sostiene el Grupo de Trabajo del Artículo 29, tiene que haber un equilibrio de intereses entre la proporcionalidad, la subsidiariedad, la gravedad de los presuntos delitos que pueden denunciarse y las consecuencias para los interesados, para entender que el deber de denuncia es exigible<sup>475</sup>.

Por último me parece necesario mencionar la Sentencia de la Sala Social del Tribunal Supremo de 17 de septiembre de 2015 (RJ 2015, 4007), donde el Tribunal Supremo también ha concluido que el poder de dirección del empresario incluye dentro de su esfera de ejercicio la posibilidad de que se pueda imponer a los trabajadores la obligación de tener que denunciar los actos ilícitos penales que se produzcan en la empresa. No resultaría una obligación abusiva o desproporcionada toda vez que la resolución judicial considera dicha instrucción empresarial como ajustada a la legalidad y especialmente al principio de buena fe que debe presidir el desarrollo de las relaciones laborales entre empresario y trabajador<sup>476</sup>. Esta Sentencia se refiere a un caso de unas estaciones de servicio que en forma de protocolo se recogía una instrucción empresarial expresa, por la que se obligaba a los encargados generales de las estaciones de servicio a denunciar las llamadas "fugas", las huidas de clientes que habiendo repostado no pagan el coste del combustible y no reconocen la deuda expresamente. Es perfectamente plausible aplicar los mismos argumentos judiciales para imponer obligaciones

---

<sup>475</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 402.

<sup>476</sup>MIRÓ MORROS, D., " Los trabajadores como 'delatores': la importancia de la Sentencia del Tribunal Supremo de 17 de septiembre de 2015", *Actualidad Jurídica Aranzadi* nº 913, 2015, p.12.

de semejante naturaleza a los trabajadores de otras empresas. Una de las primeras reflexiones es determinar los ámbitos y entornos empresariales a los que se puede extender la obligación de los trabajadores de denunciar cualquier conducta ilícita penal que se produzca en la empresa. A título de ejemplo, los dependientes de las tiendas de grandes marcas de ropa deberán denunciar a los clientes que sustraigan prendas, por lo que no cabe duda que pueden fijarse en los protocolos de actuación empresarial las reglas que dispongan los procedimientos a seguir por los trabajadores.

Esta Sentencia resuelve un caso en que es un trabajador el que denuncia un acto ilícito penal cometido por un cliente. Cabe plantearse si es lícito obligar a los trabajadores a denunciar cualquier conducta penalmente ilícita que se produzca en la empresa, y especialmente si el incumplidor es un trabajador de la propia empresa. Es decir, ¿sería lícito que una empresa obligue a sus ayudantes de conductor a que denuncien a los chóferes que conducen bajo los efectos del alcohol o de sustancias estupefacientes? Otra cuestión que se suscita es si el deber de delación o denuncia de un trabajador puede afectar o no sólo a comportamientos que tengan la consideración de penalmente ilícitos o si puede extenderse a otros comportamientos que puedan considerarse infracciones laborales, por lo que habría que plantearse si el trabajador que incumple el deber de denuncia en relación a otro trabajador puede ser sancionado por no delatar<sup>477</sup>.

Otro interrogante que al respecto se suscita es si las empresas pueden premiar o recompensar a los trabajadores que denuncien a más incumplidores. El planteamiento sería distinto al exponerlo desde el punto de vista del premio o la recompensa, pero las reflexiones son parecidas. Se plantea si se puede premiar al trabajador que más ilícitos penales denuncie de los clientes. Atendiendo a la Sentencia analizada podría establecerse ese premio, pues se estaría gratificando a quien cumple con las órdenes

---

<sup>477</sup>MIRÓ MORROS, D., "Los trabajadores...", ob. cit., p.12.



empresariales lícitas y no habría inconvenientes en retribuir el cumplimiento con una compensación adicional. Pero ¿Se puede premiar al trabajador que denuncie incumplimientos ilícitos penales de otros trabajadores? Otra cuestión es si dicho premio puede aplicarse en caso de que se produzca la denuncia sobre infracciones de carácter laboral y no de tipo penal.

Resulta evidente que habrá que poner ciertos límites, desde la perspectiva del derecho laboral y desde la esfera de la prevención de riesgos laborales. Factores como el clima laboral o el ambiente de trabajo y, especialmente, los niveles de stress que se pueden crear en la empresa o la manera en que estos elementos pueden perjudicar a la salud del trabajador y a las relaciones laborales (individuales y colectivas) si obligamos a los trabajadores a hacer de delatores, son esenciales a la hora de determinar los parámetros y los límites que deben tenerse en cuenta. Cabe por ello preguntarse ¿Qué niveles de denuncia podremos exigir? y si puede resultar exigible la denuncia de todo acto ilícito entre trabajadores o hay aspectos sobre los que podemos o debemos exonerar a los trabajadores de controlar al amparo del derecho a la integridad física y salud personal<sup>478</sup>.

### **3. El alcance de los procedimientos de denuncia de irregularidades**

Estos mecanismos se han concebido tradicionalmente como un sistema de protección a los fraudes en los ámbitos de la contabilidad financiera o de auditoría o hechos vinculados a la corrupción y a los delitos de carácter económico. Pero el nuevo escenario de responsabilidad penal de las personas jurídicas tras la reforma operada en el año 2015 en el art. 31. bis CP, al obligar a éstas a adoptar e implementar programas de prevención de delitos sin especificar cuáles, añade un elemento de incertidumbre sobre el alcance de dicho procedimiento de denuncia.

---

<sup>478</sup>MIRÓ MORROS, D., "Los trabajadores...", ob. cit., p.12.

El riesgo evidente, como la realidad se encarga de demostrar, es que al ser el empleado o el denunciante al que se le atribuye la facultad de calificar y subsumir la conducta supuestamente irregular o delictiva en el tipo penal o en el precepto del código interno que él considere, se termine concediendo relevancia a cualquier sospecha e irregularidad sin que sea posible de antemano discriminar por su adecuación a la finalidad. Y resulta inevitable que por mucho que se informe sobre la naturaleza de las conductas susceptibles de denuncia, cada cual haga su particular valoración de los hechos y llegue a juzgar como trascendente lo que en realidad carece de cualquier papel significativo desde el punto de vista penal.

Tal y como ya hemos mencionado en el apartado anterior, la AEPD en su Informe 128/2007, recoge que el tratamiento de datos de carácter personal derivado de la existencia del sistema de denuncia debe circunscribirse a *“materias o normas internas o externas cuyo incumplimiento tiene una consecuencia efectiva sobre el mantenimiento de la relación contractual entre la empresa y el denunciado, sin que sea suficiente su establecimiento en relación con cualesquiera comportamientos, acciones o hechos que puedan constituir violaciones tanto de las normas internas de la compañía como de las leyes, normativas o códigos éticos aplicables... limitando el sistema a las denuncias relacionadas con hechos o actuaciones que tengan una efectiva implicación en la relación laboral”*<sup>479</sup>.

Sin embargo, no parece que éste sea el criterio más adecuado, dado que la existencia de relevancia laboral no implica necesariamente concurrencia de gravedad para el hecho denunciado. Las repercusiones disciplinarias de un supuesto hecho irregular no pueden utilizarse para justificar una denuncia penal específica y autónoma, porque el ilícito laboral puede no integrar un supuesto de hecho delictivo, que asegure al empleado la posibilidad de denunciar el hecho.

---

<sup>479</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 397-398.

El sistema se crea para la persecución de las conductas ilícitas que puedan reportar consecuencias graves (penales, sobre todo) para la empresa o negocio y, en consecuencia, a lo que debe atenerse el hipotético denunciante, es al sistema de prevención diseñado en función de los riesgos a los que está expuesta la empresa. Hay que tener claro que lo que se trata de proteger son los intereses de la empresa frente a eventuales responsabilidades penales, por lo que no cabe llevar el asunto a cualquier irregularidad por mucha relevancia laboral que posea, porque el interés del sistema reside en la persecución de conductas gravemente irregulares que pueden afectar a la compañía.

De todas formas, no ha de pasarse por alto que el acto de imputación del ilícito puede expresarse también en ataques a la integridad física o moral de las personas o compañeros, cuando comportan repercusiones para la empresa. Es el caso, por ejemplo, de las ofensas de naturaleza sexual. Los ilícitos penales -delitos o faltas (STSJ de Cataluña de 2 de junio de 2003) cometidos por los empleados- pueden constituir una responsabilidad administrativa o civil para la empresa. Resulta destacable que la jurisprudencia hace responsable a la empresa de las ofensas infringidas por sus trabajadores, cuando la empresa, con su asentimiento o actitud tácita o pasiva de aquiescencia, ha podido tolerar dichas actitudes reprobables, de manera que el ámbito objetivo del sistema de denuncia podría alcanzar también a este tipo de ataques personales<sup>480</sup>.

Debe observarse, por último, que, quizá la forma más razonable de proceder sea acoger todas las denuncias presentadas, valorando en una fase subsiguiente por el *Compliance Officer* la legitimidad y corrección de estas, de modo que aquellas que no responden al legítimo fin sean simplemente archivadas, porque no parece que deban ser tramitadas internamente si carecen de la relevancia necesaria para su consideración, so pena de

---

<sup>480</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 398-399.

convertir el sistema de denuncia en una “*suerte de sistema inquisitorial interno frontalmente opuesto a la protección de datos y sin amparo legal alguno*”<sup>481</sup>.

#### **4. Condiciones de eficacia del sistema interno de denuncia**

El análisis de la experiencia en las empresas en que ya existe cierta cultura de los sistemas internos de denuncia deja entrever que la operatividad o la eficacia de estos viene condicionada o subordinada a la observancia de algunos principios. Hay al menos cuatro indicadores de los que depende la decisión del empleado de denunciar la irregularidad detectada.

En primer lugar la necesidad de garantizar la imparcialidad y la independencia en el tratamiento de las denuncias bajo los principios de objetividad y autonomía funcional y orgánica. Para el ejercicio de esta responsabilidad por parte de los empleados, es necesario que la entidad provea un órgano de gestión de denuncias autónomo, que sea especialmente cuidadoso y diligente en la investigación de las comunicaciones que se reciben, y que sobre todo sea capaz de asegurar la confidencialidad en la información manejada. Como ya hemos hecho referencia, la ausencia de la objetividad, imparcialidad e independencia en el funcionamiento del órgano desincentivará a los empleados a presentar las denuncias<sup>482</sup>.

Por ello, la gestión de denuncias se debe encomendar a un departamento específico en el seno de la propia empresa o grupo, dedicado a la gestión de aquéllas y a la organización de la investigación, si bien a condición de que reúna los mencionados requisitos de confidencialidad y “autonomía funcional y orgánica” respecto de la jerarquía interna de la estructura de la empresa<sup>483</sup>. El Grupo de Trabajo del Artículo 29 establece que tres son las condiciones

---

<sup>481</sup>RALLO LOMBARTE, A., “Whistleblowing (Sistemas internos de denuncia y protección de datos)”, cit., p. 106 y GOÑI SEIN, J. L., “Programas de cumplimiento empresarial...”, ob. cit., p. 399.

<sup>482</sup>GOÑI SEIN, J. L., “Programas de cumplimiento empresarial...”, ob. cit., pp. 405-406.

<sup>483</sup>RALLO LOMBARTE, A., “Whistleblowing (Sistemas internos de denuncia y protección de datos)”, cit., p.112.

necesarias para ello: 1) que el departamento en cuestión esté compuesto por personas con formación específica, en número limitado y con un vínculo contractual por lo que respecta a las obligaciones específicas de confidencialidad que deben asumir; 2) que el sistema de denuncia de irregularidades esté estrictamente separado de otros departamentos de la empresa, como el de recursos humanos, y 3) que garantice que la información recogida y tratada se transmita exclusivamente a las personas que sean específicamente responsables dentro de la empresa o grupo al que pertenezca, de adoptar las medidas necesarias<sup>484</sup>.

No obstante, es muy frecuente y, tal vez lo más recomendable, que la empresa decida su externalización a través de proveedores externos. Es más, es frecuente que la responsabilidad de la gestión del sistema de denuncias internas se delegue en empresas que gestionan centros de atención telefónica o bufetes especializados en la recogida e investigación de denuncias, de cara a garantizar mejor la independencia, la exactitud e integridad de la información contenida en dichos sistemas. De los arts. 16 (“Confidencialidad del tratamiento”) y 17 (“Seguridad del tratamiento”) de la Directiva 95/46/CE, se infiere que los proveedores de servicios externos estarán igualmente vinculados por obligaciones estrictas de confidencialidad y que deberán tratar la información sólo para los fines específicos para los que se haya recabado, así como comunicar la información tratada solamente a personas específicas en la empresa u organización responsables de la investigación de la adopción de medidas necesarias. Además, la empresa prestadora de servicios deberá suscribir el correspondiente contrato con la gran organización empresarial, quedando sometida a las exigencias de los arts. 12 LOPD y 20 del RLOPD que regulan el tratamiento de datos por cuenta de terceros, lo que en modo alguno limita la responsabilidad de la empresa que encarga dicho cometido.

---

<sup>484</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., p. 406.

La información que se maneja resulta merecedora de una especial protección y, por tanto, las garantías de seguridad se configuran como un elemento básico que va a influir a los empleados a la hora de decidirse si denunciar o no.

La obligación de aplicar las medidas de seguridad materiales para la protección de los datos personales, tanto del denunciante como del denunciado, con el fin de garantizar la confidencialidad en la recogida, transmisión o conservación de las denuncias, y de impedir cualquier acceso indebido de terceros a su contenido se impone tanto a la empresa como a los proveedores externos. Y en este sentido, del art. 9 LOPD deriva la necesidad de que el responsable del sistema interno de denuncias y, en su caso, el proveedor de servicios externo que preste dicho servicio por cuenta y orden del primero, adopten las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos y evitar la destrucción, la pérdida y el acceso o la difusión no autorizados<sup>485</sup>.

Para aplicar las medidas adecuadas es necesario hacer un análisis de la naturaleza de los datos para el cumplimiento de la finalidad en las denuncias, puesto que deberán ser proporcionadas a fin de investigar las cuestiones que se planteen. Por ello, no es posible extraer una guía única de medidas de seguridad válida para cualquier sistema interno de denuncias. En todo caso, a la vista de que se está tratando de imputaciones penales y de las repercusiones negativas que tal tipo de denuncias tiene para las personas inculpas, parece aconsejable extremar las medidas de seguridad. En tal sentido, la AEPD recomienda la aplicación de las medidas de nivel alto, y ello en atención a que los datos proporcionados en las denuncias pueden resultar singularmente sensibles como las contempladas en el art. 7 de la LOPD al hacer referencia a materias como ideología, religión, afiliación sindical, origen racial, salud o vida sexual, y pueden comportar un riesgo de estigma social

---

<sup>485</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 406-408.

del denunciado, y dado que, eventualmente, puede ser necesario incorporar el dato de la afiliación sindical, en la medida en que la empresa puede verse obligada a comunicar a los sindicatos los procedimientos abiertos a los empleados afiliados a éstos.

A los efectos de garantizar esa máxima seguridad, se considera necesario observar, de acuerdo con lo previsto en el Título VIII RLOPD, las siguientes obligaciones adicionales: 1) identificación de los soportes específicos para los usuarios con acceso autorizado; 2) cifrado de los soportes de distribución de los datos; 3) realización de copias de respaldo y existencia de procedimientos de recuperación; 4) registro de los accesos al sistema de denuncias; 5) existencia de mecanismos que obstaculicen la apertura de los dispositivos de almacenamiento; 6) debida custodia de los soportes; 7) auditorias bianuales preceptivas<sup>486</sup>.

En tercer lugar, el efecto de los sistemas de denuncia interna depende de las garantías de indemnidad que el empleado encuentre en la respuesta de la organización empresarial a las denuncias. Nadie se atreverá a hacer comunicaciones si el tipo de respaldo recibido por la empresa es inconsistente o carece de auténticas medidas de protección de las personas informantes. Éste es otro aspecto clave, porque al menor riesgo de seguridad para el mantenimiento de las condiciones de trabajo o del empleo, o la conservación del mismo, los empleados dejará de colaborar en la denuncia de las irregularidades.

Debe tenerse en cuenta que no existe en el ordenamiento jurídico laboral precepto legal que garantice al trabajador el derecho a no sufrir perjuicio alguno por el hecho de formular denuncias o quejas de anomalías o irregularidades internas en la empresa. Es cierto, que el ordenamiento laboral reconoce a los representantes legales de los trabajadores una serie de

---

<sup>486</sup>RALLO LOMBARTE, A., "Whistleblowing (Sistemas internos de denuncia y protección de datos)", cit., p. 112 y GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 408-409.

derechos, entre otros, el derecho de no ser despedidos o sancionados durante el ejercicio de sus funciones ni dentro del año siguiente a la expiración de su mandato, así como el derecho a no ser discriminados en su promoción económica o profesional en razón, precisamente, del desempeño de su representación, que podrían servir de cobertura para dispensar protección en los casos de denuncia de irregularidades. Pero esa protección sólo alcanza a los representantes legales quedando el resto de los trabajadores privados de esta protección.

Ahora bien, ello no significa que estén desprovistos de protección frente a represalias cuando denuncian irregularidades en su propia empresa, puesto que la conducta delatora podría encontrar cobertura dentro del campo protegido por el genérico derecho de indemnidad, tal y como ha sido configurado por el Tribunal Constitucional<sup>487</sup>.

De esta forma, el Tribunal Constitucional no descarta la posible aplicación del principio de garantía de indemnidad en caso de represalia del trabajador por la denuncia formulada. Así lo ha entendido en la STC 198/2000 al juzgar el despido de un trabajador de un Casino por haber denunciado ante el Servicio de Control de Juegos de Azar determinadas irregularidades cometidas por la empresa, no en defensa de los propios derechos, sino de los de carácter "cívico o altruista", aunque desestima el amparo al no haberse probado el móvil de represalia denunciado<sup>488</sup>.

Con todo, no es muy claro que la garantía de indemnidad no sufra una excepción con relación al supuesto de hecho de la denuncia interna formulada ante el órgano interno instituido por la propia empresa, bien que éste sea autónomo e independiente en su funcionamiento.

---

<sup>487</sup>Inicialmente en la STC 14/1993 y posteriormente en las SSTC 197/1998; 140/1999; 196/2000; 198/2001; 5/2003; 55/2004; 87/2004.

<sup>488</sup>ALVAREZ ALONSO, D., *La garantía de indemnidad del trabajador frente a represalias empresariales*, edit. Bomarzo, Alicante, 2005, p. 81 y GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 409-410



Resulta indispensable que la entidad asegure de forma clara y rotunda una suerte de indemnidad a todos los empleados, agentes y representantes, que hagan uso del derecho a comunicar o denunciar una potencial o actual conducta criminal, garantizándoles que no sufrirán por ello perjuicio alguno en su estatus jurídico laboral, puesto que, de lo contrario, se apoderará de ellos un temor que los llevará a mantener oculta tal información y a no denunciar.

Por último en relación con las obligaciones de notificaciones que asumen las empresas en materia de protección de datos, debe prestarse atención a la notificación del fichero al Registro General de la AEPD. En aplicación de los arts. 18 ("Obligación de notificación a la autoridad de control") a 20 ("Controles previos") de la Directiva 95/46/CE Directiva, las empresas que establezcan sistemas de denuncia deben cumplir con los requisitos de notificación a las autoridades nacionales de protección de datos. Es el mecanismo de garantía de la efectividad de los derechos de acceso, rectificación y cancelación de los afectados por el tratamiento.

De esta forma, todas las empresas que prevean tales procedimientos de denuncia de irregularidades en su programa de cumplimiento deberán ajustarse a los referidos criterios y ello no ya sólo porque constituyen los límites que la AEPD considera obligados en virtud de la normativa de protección de datos, sino porque son condición de eficacia<sup>489</sup>.

---

<sup>489</sup>GOÑI SEIN, J. L., "Programas de cumplimiento empresarial...", ob. cit., pp. 410-411.

## VI. EL CANAL INTERNO DE DENUNCIAS

### 1. Consideraciones generales

Al analizar distintos canales de denuncia existentes en gran número de empresas que cotizan en mercados europeos o norteamericano este trabajo trata de recoger los principios básicos que deben regir en la configuración e implantación de un canal de denuncias efectivo a todos sus efectos.

El principio nuclear y prioritario es el que las personas que presenten una denuncia interna deben hacerlo de buena fe, con respeto a la verdad, con el convencimiento de actuar correctamente y solamente en beneficio de la empresa, del Estado y de la sociedad en general. Queda prohibida la formulación de denuncias falsas, por resultar contrarias a la ley y a los principios y valores éticos de la empresa<sup>490</sup>. El canal de denuncias no deja de ser una expresión más del *Compliance*, tal y como hemos resaltado a lo largo de todo el trabajo, por lo que una denuncia que no parta de la buena fe y la ética estaría vulnerando el principio fundamental del origen del cumplimiento normativo.

Como consecuencia de todo lo acontecido en los último tiempos, cada vez más organizaciones son conscientes de la necesidad de implantar sistemas y programas de cumplimiento normativo que permitan prevenir o, al menos, reducir la comisión de actos ilícitos o indebidos en las mismas, y un componente esencial del *Corporate Compliance Program* es la implantación efectiva de un canal de denuncias internas<sup>491</sup>.

Tal y como hemos analizado a lo largo del trabajo la transparencia y el diálogo deben ser los pilares sobre los que se asiente un programa de cumplimiento efectivo y, para ello, los whistleblowers juegan un importante

---

<sup>490</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1242.

<sup>491</sup>ARMENTIA MORILLAS, P."Plan de acción e implantación del Compliance Program. Plan de prevención, detección y reacción. Canal de Denuncias", en AA.VV., *Compliance. Cómo gestionar los riesgos normativos en la empresa*, obra colectiva coordinada por C.A. Sáiz Peña, Pamplona, 2015, pp. 610 y ss.

papel. El tradicional deber de silencio impuesto, - tácita o expresamente- a los empleados en señal de lealtad a la compañía y el hermetismo respecto a los “trapos sucios” (especialmente en países con poca tradición de denuncias, como es el nuestro) debe dar paso a dinámicas completamente diferentes basadas en la transparencia informativa y en el fomento de la delación.

En términos generales, el whistleblower puede definirse como la persona que revela información negativa sobre una organización (pública o privada) con la que, generalmente, tiene alguna vinculación, lo que le permite tener un mayor conocimiento sobre sus prácticas y su personal. La información puede estar referida a una conducta ilícita —negligente o intencionada— o simplemente poco ética realizada por un empleado o directivo de la entidad y el medio para revelarla, en principio, puede ser cualquiera. Las vías preferidas por los whistleblowers hasta ahora han sido las autoridades competentes y los medios de comunicación, pero la proliferación de canales de denuncia en las empresas, como parte de sus políticas de cumplimiento, están sin duda aportando una nueva perspectiva al fenómeno<sup>492</sup>.

Por otra parte, hay voces que apoyan que la falta de actividad o el mal uso del canal de denuncia es síntoma de la escasa vigencia del programa de cumplimiento, de un *compliance program* mal diseñado o de un programa que se limita a cumplir únicamente funciones formales o de publicidad.

Tal y como hemos analizado anteriormente, la protección del whistleblower frente a las represalias de la organización o de sus compañeros constituye una de las principales preocupaciones en esta materia, ya que un empleado sólo se decidirá a denunciar una irregularidad de un superior o de un compañero si tiene la certeza de que ello no le reportará consecuencias negativas. En el marco de un programa de cumplimiento, esta certeza sólo se consigue si el compromiso de la entidad con el programa, con la prevención y el castigo de ilícitos es auténtico, y es que la falta de una cultura corporativa

---

<sup>492</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., pp. 206-207.

adecuada, merma la efectividad del canal y de toda la política de cumplimiento. Si el empleado sospecha que su denuncia no va a ser tomada en serio, no se expondrá a los riesgos que implica utilizar el canal.

En el marco de un programa de cumplimiento sólido, un canal de denuncia es un instrumento tremendamente valioso, pues pone a disposición de la compañía una fuente de información de primera mano que puede serle muy útil a efectos de eludir una posible responsabilidad penal. Es una de las herramientas para el ejercicio del debido control y además dará las claves para mejorar o reconfigurar otras. El canal puede proporcionar evidencias claras de la eficacia (o ineficacia) del programa pues, si funciona adecuadamente, registrará los incumplimientos y facilitará su sanción. La información recopilada a través de él será por ello un elemento fundamental en las evaluaciones y actualizaciones periódicas a las que se debe someter al programa de cumplimiento, ya que permite comprobar si el análisis de riesgos se realizó adecuadamente y si las estrategias y protocolos están funcionando según lo previsto. Asimismo la información recibida a través del canal puede llegar a ser fundamental para la defensa de la organización si se incoa un proceso penal contra ella. Contar con información de los hechos antes de que ésta llegue a manos del Fiscal o del Juez y poder gestionarla a su conveniencia coloca a la entidad en una posición ventajosa<sup>493</sup>.

En el diseño de un canal de denuncia eficaz hay muchas variables que deben tenerse en cuenta. Son factores determinantes en la configuración del canal: la actividad social, el perfil de los empleados y el grado de compromiso ético alcanzado en la compañía. Lo que es imprescindible es lograr la confianza en el sistema por parte de sus potenciales usuarios<sup>494</sup>. Dicha confianza en el mismo se logra demostrando seriedad y rigor en la política de cumplimiento de la entidad y específicamente en la implementación del canal, tal y como hemos mencionado, los empleados y directivos deben percibir un

---

<sup>493</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., pp. 207-208.

<sup>494</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 214.

compromiso *auténtico* de la empresa. Frente a la denuncia la reacción de la empresa será fundamental, por ello una respuesta inadecuada o la negación del problema pueden hacer surgir en el denunciante la impresión de que sus preocupaciones no han sido apreciadas y que la entidad está dispuesta a consentir esos comportamientos ilícitos o poco éticos. Si no se le escucha dentro de la empresa puede que abandone su actitud pero también que muestre fuera de ella sus preocupaciones. También debe apuntarse que la ausencia de un reglamento interno claro y completo genera incertidumbre en quien ha de manejar las denuncias, la investigación y la toma de medidas al respecto, lo que puede inducir a la inactividad de la entidad frente a los hechos, no por tolerancia de la mala conducta sino por su desconocimiento. Es necesario que el procedimiento de denuncia y su tramitación estén previamente definidos y detallados, con indicación de quién se ocupará en la recepción, investigación y toma de decisiones y, quien tendrá acceso al procedimiento y a la información en él recogida porque la incertidumbre sobre qué ocurrirá después de la denuncia desincentiva al posible denunciante<sup>495</sup>. Por el contrario, la existencia de un procedimiento de denuncia reglado resulta una herramienta muy útil para conseguir la confianza de los trabajadores.

Es necesario destacar que las ventajas de un canal propio de denuncia frente al descubrimiento público de la información son esenciales para la empresa, aunque son menos claras para el interés público. Por una parte, la delación interna da a la entidad la oportunidad de solucionar el problema evitando así una publicidad negativa. Incluso si la conducta irregular se hiciera pública, la posición de la organización seguirá siendo ventajosa, pues podrá mostrarse como una entidad responsable y diligente. Por otro lado, comodesventaja, denunciar internamente puede facilitar el que la información sea ignorada o que las medidas que se tomen sean exclusivamente cosméticas. Se ha propuesto como una solución intermedia la creación de agencias públicas

---

<sup>495</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., pp. 214-215.

encargadas de la recepción e investigación de las denuncias, asegurándose de la toma de medidas eficaces sin comprometer la imagen de la empresa.

Existen muy diversas opciones en el diseño de los canales de denuncia, ya que muchas decisiones quedan al arbitrio de la empresa: quién puede hacer uso de la hotline, qué se puede denunciar, cómo se gestiona el canal o qué consecuencias puede tener la denuncia de una información falsa. En principio, los únicos límites que deben observarse- tal y como se ha analizado en el presente trabajo- son los derivados por la legislación laboral y de protección de datos, lo que proporciona a la entidad un significativo margen de maniobra para desarrollar un canal que se acomode a su tamaño, estructura, funcionamiento y valores<sup>496</sup>.

## **2. Características**

### **2.1 Consideraciones generales**

Después de un análisis a las experiencias de empresas españolas y sus canales de denuncia puede llegarse a la conclusión de que para que un sistema de denuncias internas sea eficaz y responda a la finalidad para la que fue implantado es necesario que cumpla, como mínimo, con determinadas características:

#### **2.1.1 Sistema respaldado por la dirección.**

El sistema debe estar respaldado por la alta dirección de la entidad, de forma que sea obligatorio su cumplimiento y sea respetado por todas las estructuras de la organización<sup>497</sup>.

Cuando una entidad pretenda implantar por primera vez un canal de denuncias, es necesario que previamente hayan sido informados y consultados los representantes de los trabajadores (artículo 64 del TRLET).

---

<sup>496</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 215.

<sup>497</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 615.

### **2.1.2 Sistema previamente divulgado y que cumpla con la obligación de información.**

Tal y como hemos visto, el canal de denuncias debe ser divulgado previa y efectivamente entre sus destinatarios: empleados y personas que tengan alguna vinculación con la entidad. De acuerdo con los derechos de los empleados analizados con anterioridad, los denunciadores y los denunciados han de ser previamente informados de la existencia del sistema, del tratamiento de los datos que conlleva la formulación de una denuncia y de las consecuencias que para el denunciado puede comportar este hecho.

En todo caso, para garantizar esa divulgación, es recomendable que se incluya información sobre su existencia en los modelos de documentos que maneja la entidad. Así se había de incluir información sobre su existencia y su funcionamiento en el modelo del contrato de trabajo y en la Intranet, en los modelos de contratos con proveedores, clientes y colaboradores externos, así como en la página Web de la entidad<sup>498</sup>.

Debe puntualizarse que hay autores que sostienen que aunque la información previa juega un papel importante, no es necesario para la entidad contar con el consentimiento de los trabajadores para implantar un sistema de denuncias internas. De hecho, la AEPD considera que no es necesario el consentimiento de los titulares para el tratamiento de sus datos personales en los procedimientos de denuncias internas, si concurre pleno conocimiento de la existencia de este mecanismo de denuncia, pues está amparado en la excepción a la obligación de consentimiento al disponerse que "*no será preciso el consentimiento cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento*"<sup>499</sup>. En este sentido, la AEPD considera que la implantación de sistemas de denuncias no requiere

---

<sup>498</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 615-616.

<sup>499</sup> Art. 6.2 LOPD

del consentimiento de los interesados siempre que exista un " *vínculo contractual de derecho laboral, civil o mercantil*" y " *pleno conocimiento de la existencia de los mecanismos descritos por parte de las personas cuyos datos pudieran ser tratados por los mismos, quedando la existencia de dichos procedimientos incorporada a la relación contractual como parte integrante de la misma*"<sup>500</sup>.

Tampoco es necesario el consentimiento para la comunicación de datos a terceras partes que investiguen los hechos de la denuncia si " *el tratamiento responde a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros*", en este caso la comunicación sólo es legítima en cuanto se limite a la finalidad que la justifique<sup>501</sup>.

### **2.1.3 Sistema fácilmente accesible**

El sistema de comunicación de irregularidades debe estar a disposición de cualquier persona que tenga una relación civil, mercantil o laboral con la entidad. Para que esos canales puedan ser utilizados por todas las personas que están vinculadas a la misma, es necesario que se dispongan diversos procedimientos para hacer llegar esas irregularidades, tales como:

- a través de la cumplimentación de un formulario electrónico incluido en la Página Web y en la Intranet de la Empresa;
- mediante el envío de un correo electrónico a un buzón corporativo específico (p.e. denuncias@dominio.es);
- a través del envío de una carta en soporte papel mediante el correo postal a una dirección determinada.

Después de haber estudiado la materia y diversas opiniones en este sentido, puedo concluir uniéndome a la voz mayoritaria, que es recomendable que la

---

<sup>500</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 616-617.

<sup>501</sup> Art. 11.2.c LOPD



entidad descarte la vía telefónica como forma aceptada de recibir denuncias, por los inconvenientes que ello puede suponer (p.e. atención 24 h., el destinatario de la llamada puede no ser la persona que debería ser, la imposibilidad de adjuntar documentación y la dificultad de informar al denunciante de los requisitos que requiere la normativa de protección de datos y poder probar que se ha realizado esa información)<sup>502</sup>.

Para realizar una gestión eficaz y no sujeta a posibles sanciones es necesario:

a) que exista una entrada única, en la que se reciban las comunicaciones que dirijan los denunciantes con independencia de que existan diversos mecanismos por los cuales se interponga la denuncia, todos ellos deberán tener un canal único de entrada que permita gestionar correctamente dicha denuncia;

b) que se encuentre desarrollada a través de diversos mecanismos, de forma tal que el denunciante pueda elegir el que mejor le convenga,

c) que se ajuste, en todo momento, al cumplimiento de las obligaciones establecidas por la normativa de Protección de Datos analizadas anteriormente.

#### **2.1.4 Sistema proporcional**

Esta característica supone que los hechos denunciados tengan una implicación directa en la relación existente entre el denunciante/denunciado y la entidad, no debiendo ser objeto de denuncia cualquier tipo de comportamiento, sino sólo los que estén relacionados con su vinculación con la entidad.

---

<sup>502</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 617.

### **2.1.5 Sistema documentado**

Tal y como hemos puesto de manifiesto al comienzo de este Capítulo el procedimiento del canal de denuncias debe estar previamente aprobado y documentado por escrito, de forma que los denunciadores y los órganos que gestionen las denuncias tengan un conocimiento del proceso (funcionamiento del sistema interno de denuncias, órganos que formarán parte de la instrucción, plazos, etc.).

Es conveniente que se especifiquen los extremos del procedimiento que pueden ser objeto de excepción al sistema formalmente aprobado e implantado, así como los requisitos que se deben cumplir para poder hacer uso de dichas excepciones (p.e. aprobación del Comité, determinación de supuestos en los que se podrá admitir una excepción al procedimiento formalmente aprobado e implantado)<sup>503</sup>.

### **2.1.6 Sistema en el que los comportamientos irregulares estén expresamente detallados, así como las consecuencias de su incumplimiento**

Deben estar expresamente recogidos y tipificados los comportamientos y acciones que se consideran irregulares y, por tanto ser objeto de denuncia. Una parte de la doctrina apunta a que no es suficiente la mera inclusión de un listado de incumplimientos genéricos.

Es preciso señalar que son comportamientos irregulares los que transgredan la buena fe o la legislación vigente, y aquellos que vulneren las políticas corporativas que impliquen un incumplimiento de los deberes laborales o contractuales del denunciado, aquellos que supongan algún tipo de responsabilidad penal para la entidad.

---

<sup>503</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 617-618.

Dichos comportamientos versarán sobre materias relacionadas con cumplimiento normativo, respeto a los valores éticos, respeto a la dignidad de las personas, desarrollo profesional, no discriminación, colaboración y dedicación, manipulación de la información, uso y protección de activos, corrupción y soborno, blanqueo de capitales e irregularidades en los pagos, conflicto de intereses y lealtad a la empresa, neutralidad política, relaciones con clientes, contratistas y proveedores, imagen y reputación corporativa.

En la Guía de Relaciones Laborales publicada por la AEPD se establece expresamente que "Tanto los denunciante como los potenciales denunciados deberán haber sido informados previamente (...) de las consecuencias que para el denunciado puede comportar este hecho"<sup>504</sup>.

En la regulación del procedimiento de denuncias debe indicarse expresamente las consecuencias de los incumplimientos, como son la aplicación del régimen disciplinario de la entidad, además de las responsabilidades de otra índole que le puedan corresponder judicialmente. El incumplimiento de esta regulación debe ser entendido en una doble vertiente: bien derivado del comportamiento irregular del denunciado o bien cuando la denuncia de irregularidad surge de la conciencia de falsedad, habiendo actuado dolosamente y con ánimo de perjudicar al denunciado o bien de un simple error.

### **2.1.7 Sistema que garantice que no habrá represalias para el denunciante**

Tal y como hemos señalado en el Capítulo anterior, es fundamental que el denunciante tenga clara la confidencialidad de sus datos identificativos durante todo el proceso y que no puede ser objeto de represalias de ningún tipo<sup>505</sup>.

---

<sup>504</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 618-619.

<sup>505</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 619.

Se puede detallar expresamente en la propia regulación que, en el caso de que el denunciante esté relacionado con los hechos, existen atenuantes por confesión anterior al descubrimiento del delito y por disminución de los efectos de los que podría beneficiarse si denuncia<sup>506</sup>.

## **2.2 Confidencialidad y la protección de datos**

Si las denuncias se realizan de buena fe y cumpliendo con el código ético de la empresa, la tramitación ha de ser con carácter confidencial, es decir, guardando estricto secreto y reserva sobre la identidad del denunciante. Los datos del denunciante sólo podrán ser revelados, en su caso, a la autoridad pública competente para la investigación de los hechos<sup>507</sup>. Por el contrario, si como consecuencia de la investigación de una denuncia resulta evidente que es falsa, o si el denunciante ha actuado con mala fe o infringiendo de manera flagrante una norma, con independencia de las medidas legales que pudiera adoptar la empresa, los datos del denunciante pueden ser revelados a la persona denunciada para que si lo estima oportuno, pueda iniciar las acciones legales correspondientes<sup>508</sup>.

Tras haber analizado previamente la legislación americana, europea y nacional parece claro que para cumplir con el objetivo principal que motiva la implantación del canal de denuncias en una organización y animar a las personas a que hagan uso de dicho sistema, es fundamental (además de garantizar que no van a tomarse represalias por haber denunciado un hecho o comportamiento) que se asegure la confidencialidad de la información durante todo el proceso.

---

<sup>506</sup>En el propio Código Penal se establece que son circunstancias atenuantes de la responsabilidad criminal "La de haber procedido el culpable, antes de conocer que el procedimiento judicial se dirige contra él, a confesar la infracción a las autoridades" (art. 21.4 CP), "La de haber procedido el culpable a reparar el daño ocasionado a la víctima, o disminuir sus efectos, en cualquier momento del procedimiento y con anterioridad a la celebración del acto del juicio oral" (art. 21.5 CP).

<sup>507</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1246.

<sup>508</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1246.

Con la expresión de confidencialidad se hace referencia a la no divulgación de las características y demás extremos de la denuncia (ni de los denunciantes, ni de los hechos ni de las personas cuya conducta o actuación pudiera ser mencionada en las denuncias) fuera de los órganos autorizados, por las consecuencias negativas que podrían suponer para el denunciante y el denunciado la revelación de su identidad dentro de la organización. La confidencialidad del sistema puede cesar en los supuestos, en los que en función de las materias a las que afecten, su conocimiento de los hechos sea requerido judicialmente por la autoridad competente.

Cabe cuestionarse si las denuncias pueden ser, además de confidenciales, anónimas o siempre han de ser nominales<sup>509</sup>.

Si se analiza la normativa detallada en capítulos anteriores en la que se estudian las regulaciones referentes a los canales de denuncia, prácticamente todas aceptan las denuncias anónimas. La SOX aboga por un sistema de denuncias anónimo al establecer *"procedimientos para la recepción, retención y tratamiento de quejas recibidas por el causante en relación con la contabilidad, controles contables internos o cuestiones de auditoría; y la presentación confidencial y anónima por parte de los empleados de la persona causante de preocupación en relación con cuestiones contables o de auditoría cuestionables"*.

El Código de Buen Gobierno de las Sociedades Cotizadas de 2015 recomienda reforzar las normas legales en relación con la función de la auditoría interna y ampliar las funciones de la comisión de auditoría. Así, en relación con los sistemas de información y control interno se recomienda que a la comisión de auditoría además de las funciones previstas en la Ley, le corresponda entre otras la función de *"establecer y supervisar un mecanismo que permita a los empleados comunicar, de forma confidencial y, si resulta posible y se considera apropiado, anónima, las irregularidades de potencial*

---

<sup>509</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 622-623.

trascendencia, especialmente financieras y contables, que adviertan en el seno de la empresa" (Recomendación 42.1.c).

En cambio, si revisamos los dos citados Informes de referencia en los que se analizan los extremos que deben ser observados por las entidades que pretendan implantar un canal de denuncias para cumplir con la normativa de protección de datos (Dictamen 1/2006 del Grupo de Trabajo del artículo 29 y entre el Informe 0128/2007 de la AEPD), se aprecian diferencias de criterios<sup>510</sup>.

En el Dictamen 1/2006<sup>511</sup> se establece como criterio general que las denuncias sean nominales (de forma que no se fomente la interposición de denuncias anónimas). El organismo europeo es consciente de que la interposición de una denuncia en la que el denunciante no se identifique, es un hecho que se da en la gran mayoría de sociedades, especialmente, en las de países no anglosajones en los que no está tan arraigada la cultura de la denuncia. Por ello, se establece la obligación de informar al denunciante que sus datos identificativos se mantendrán confidenciales (fuera de los órganos autorizados) y si, a pesar de ello, la persona quiere permanecer en el

---

<sup>510</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 623.

<sup>511</sup>Dictamen 1/2006 "(...) *Por lo que respecta a las normas de protección de datos, los informes anónimos plantean un problema específico con respecto al requisito esencial de que los datos personales sólo deberían recopilarse de manera leal. Como norma, el Grupo de Trabajo considera que sólo los informes identificados deberían comunicarse a través de programas de denuncia de irregularidades para satisfacer este requisito. No obstante, el Grupo de Trabajo es consciente de que algunos denunciantes podrían no encontrarse siempre en situación o tener disposición psicológica para presentar informes identificados. También es consciente del hecho de que las quejas anónimas son una realidad dentro de las sociedades, incluso y especialmente en ausencia de sistemas de denuncia de irregularidades confidenciales y organizados, y que esta realidad no puede ignorarse. Por ello, el Grupo de Trabajo considera que los programas de denuncias de irregularidades podrían llevar a la presentación de informes anónimos a través del programa y a la toma de medidas basadas en ellos, pero sólo como excepción a la regla y en las siguientes condiciones. El Grupo de Trabajo considera que los programas de denuncia de irregularidades deberían estar creados de tal manera que no fomenten los informes anónimos como la manera habitual de presentar una queja. En concreto, las sociedades no deberían anunciar el hecho de que se permiten los informes anónimos a través del programa. (...) Las personas que pretendan presentar un informe mediante un sistema de denuncia de irregularidades deberían ser conscientes de que no sufrirán por su acción. Por esa razón, el programa debería informar al denunciante, en el momento de establecer el primer contacto con el programa, de que su identidad se mantendrá confidencial en todas las etapas del proceso y, en concreto, que no se divulgará a terceros, ni a la persona inculpada y a los mandos directivos del empleado. Si, a pesar de esa información, la persona que informa al programa sigue queriendo permanecer en el anonimato, el informe se aceptará en el programa (...)*".

anonimato, su denuncia deberá ser aceptada. En estos casos, las denuncias anónimas deben ser tratadas con una mayor rapidez para evitar riesgos por su mala utilización.

En el ya analizado Informe 0128/2007 de la AEPD<sup>512</sup> no se da lugar a las entidades a aceptar denuncias anónimas en sus sistemas, ya que mantiene que se deben evitar esta clase de denuncias para garantizar la exactitud e integridad de la información que predica la normativa de protección de datos, en defensa del deber de calidad (art. 4<sup>513</sup> LOPD).

No se puede obviar que las entidades pueden querer tener en consideración todas las denuncias recibidas, aunque su denunciante no esté identificado<sup>514</sup>. Así lo entienden un tercio de las entidades que cotizan en el IBEX 35 y, según se predica en sus códigos y procedimientos de gestión de denuncias, aceptan las denuncias anónimas en su sistema (o al menos, no consta su negativa a aceptarlas expresamente)<sup>515</sup>.

---

<sup>512</sup>Informe 0128/2007 de "Creación de sistemas de denuncias internas en las empresas (mecanismos de "whistleblowing")", publicado por la Agencia Española de Protección de Datos se establece que "A nuestro juicio, debería partirse del establecimiento de procedimientos que garanticen el tratamiento confidencial de las denuncias presentadas a través de los sistemas de "whistleblowing", de forma que se evite la existencia de denuncias anónimas, garantizándose así la exactitud e integridad de la información contenida en dichos sistemas. (...) En consecuencia, el establecimiento de mecanismos que garanticen la presentación de denuncias confidenciales, y no anónimas, no perjudicaría la operatividad del sistema, al deber quedar claramente planteada la conclusión de que los datos del denunciante en modo alguno podrían ser transmitidos al denunciado con ocasión del ejercicio del derecho de acceso.

Por ello, a fin de garantizar el cumplimiento del mencionado principio deberá exigirse que el sistema únicamente acepte la inclusión de denuncias en que aparezca identificado el denunciante, sin perjuicio de las salvaguardias que se han señalado para garantizar la confidencialidad de sus datos de carácter personal, no bastando el establecimiento de un primer filtro de confidencialidad y una posible alegación última del anonimato para el funcionamiento del sistema".

<sup>513</sup>El artículo 4 de la LOPD dispone que "1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. 2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos (...). 3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. 4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados (...)".

<sup>514</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 624-625.

<sup>515</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 625.

La confidencialidad debe ser uno de los pilares esenciales sobre el que se debe articular cualquier canal de denuncias. Para garantizar la confidencialidad de la información en todo el proceso de gestión de denuncias, es recomendable que la organización valore la posibilidad de implantar mecanismos técnicos de cifrado:

- Sistemas que permitan cifrar el canal de transmisión por el que va a circular dicha información o;

- a) Canal cifrado por el que se transmite la información desde el formulario electrónico hasta la base de datos en el que se almacena dicha información. La transmisión de la información que viaja desde la página Web de la entidad en la que se cumplimenta el formulario electrónico, por el que se interpone la denuncia, hasta la base de datos en la que se almacena dicha información, se realice a través de un canal que utilice el protocolo "https", de forma que se garantice que la información que viaja desde dicha página hasta la base de datos no podrá ser interceptada ni utilizada por terceros.

- b) Correos electrónicos cifrados con certificados digitales. El uso del correo electrónico por canales inseguros (como la red Internet), no garantiza la confidencialidad en los mensajes intercambiados entre los destinatarios. Por ello, para asegurar dicha confidencialidad es posible codificar la información intercambiada mediante el uso de la criptografía de mensajes. Los mensajes son cifrados por el remitente y descifrados por el destinatario, utilizando claves que solamente ellos conocen. De forma que los datos de los correos electrónicos que circulan por las redes y servidores de Internet están codificados, y son totalmente ininteligibles para terceras personas.

- Herramientas que permiten cifrar la información que se almacena en un determinado sistema o aplicación (como es el caso de cifrar los servidores y/o bases de datos) o;



- Soluciones técnicas que permitan cifrar el archivo que contiene la información (Solución IRM – Information Risk Management). Lo que queda cifrado es el archivo en sí mismo y no el canal de distribución<sup>516</sup>.

Mediante el uso de esta tecnología se puede evitar que personas no autorizadas puedan leer, imprimir, reenviar o copiar información confidencial (ya sea debido a errores humanos que hacen que se envíe la información a quién no se debe realizar o a usuarios avanzados o hackers cuyo propósito es vulnerar los sistemas y hacerse con dicha información)<sup>517</sup>.

Una de las cuestiones más controvertidas y de mayor trascendencia es el tratamiento de la identidad del whistleblower. Caben dos posibilidades respecto de la identidad del denunciante: el anonimato y la confidencialidad<sup>518</sup>.

Optar por un sistema de denuncias anónimas otorga mayores garantías para el denunciante, lo que favorece la eficacia del canal. Los empleados se mostrarán menos reticentes a utilizar la hotline si para ello no tienen que proporcionar sus datos, pues así se aseguran auténtica protección frente a represalias u otro tipo de consecuencias negativas derivadas de su delación. El anonimato plantea algunos problemas. La facilidad para realizar las denuncias podría fomentar los chivatazos por venganza o con ánimo de perjudicar a un compañero o a un superior, con la consiguiente dificultad para emprender acciones respecto del denunciante de mala fe, cuya identidad se desconoce. Por todo ello, la configuración preferida tanto por la doctrina como por las autoridades de protección de datos es la de confidencialidad. Por este modelo se han decantado la mayoría de las compañías.

---

<sup>516</sup>El IRM es la tecnología que se basa en el cifrado de los archivos (ya sea un documento Word, una presentación o un correo electrónico) de manera individualizada y que permite gestionar los derechos de acceso de los usuarios a la información en soporte electrónico.

<sup>517</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 625-626.

<sup>518</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 224.

El sistema de denuncias confidenciales presenta menos problemas. Se evita el mal uso de la hotline y se sigue protegiendo la identidad del denunciante, pues cuando se opta por la confidencialidad, si se externaliza el canal de denuncia, todo el procedimiento puede ser gestionado a través de un proveedor externo y, si se gestiona desde la propia empresa, el acceso a los datos debe limitarse a las personas responsables de la recepción y tramitación de las denuncias. La limitación puede ir más allá, pues la identidad del denunciante no tiene que ser conocida por todas las personas con participación en el canal.

Los problemas en los canales que optan por la confidencialidad aparecen cuando la investigación y el procedimiento para sancionar al responsable trascienden el ámbito de la entidad, y se desarrollan en los ámbitos administrativos, policiales y judiciales. La protección de la identidad del whistleblower decae ante un requerimiento judicial y, aun recibiendo tratamiento de testigo protegido. Esto merma la efectividad del sistema de denuncia y, en general, del programa de cumplimiento, pues no favorece la denuncia y desvela las irregularidades. Éste no es un problema que se plantee únicamente respecto de la información obtenida a través de la hotline, sino que se presenta en general con toda la información generada a partir de programa de cumplimiento<sup>519</sup>.

Existen modelos mixtos que pueden atenuar los aspectos negativos y aprovechar los positivos de unos y otros. Quienes defienden esta posición intermedia sostienen que desde la empresa y, especialmente, desde los órganos encargados del sistema de cumplimiento, se favorezca el uso de la denuncia confidencial, pero aceptando la recepción de las anónimas en determinadas circunstancias. Así se ha propuesto aceptar el uso anónimo del canal cuando la situación personal del whistleblower lo aconseje, cuando la denuncia, aun siendo anónima, está suficientemente fundamentada, o cuando

---

<sup>519</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 225.

el interés jurídico amenazado merece especial protección (la vida, la integridad física y moral, y la libertad sexual)<sup>520</sup>.

### **2.2.1 Deberes y derechos de las partes**

#### *A) Deber de información*

##### *a) Al denunciante*

Tal y como se ha destacado, las personas sobre las que se va a recabar datos personales, con independencia del mecanismo utilizado para recabarlos, deben ser informadas de manera previa y precisa, del conjunto de extremos recogidos por la normativa de protección de datos<sup>521</sup>.

Para cumplir con este deber de información al denunciante que la normativa impone al sujeto que va a tratar los datos es necesario que en los mecanismos o procedimientos habilitados por la entidad para comunicar posibles comportamientos irregulares, se deba incluir una cláusula de información con el contenido que exige la normativa vigente, con la siguiente información<sup>522</sup>:

- a) razón social y dirección del responsable del fichero que realice el tratamiento de la información;
- b) finalidad del tratamiento de los datos;
- c) posibles comunicaciones de datos amparadas por la normativa, tanto a los Jueces y Tribunales como a las personas que se considere pertinentes implicadas en cualquier fase de la investigación y en el caso de grupo de empresas, se ha de especificar si se van a comunicar sus datos a otras entidades del grupo especificando siempre la razón social de la organización e información sobre sus actividades, direcciones y la concreta finalidad que motiva la comunicación (p.e. supuesto en el que los datos son gestionados por la matriz del grupo);

---

<sup>520</sup> GARCIA MORENO, B., "Whistleblowing...", ob. cit., pp. 225-226.

<sup>521</sup> Artículo 5.1<sup>521</sup> LOPD.

<sup>522</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 628-629.

- d) forma y dirección en el que ejercer los derechos de acceso, rectificación, cancelación y oposición;
- e) confidencialidad del sistema de denuncias;
- f) consecuencias que conlleva realizar una denuncia falsa con mala fe;
- g) no represalias por parte de la organización.

Consideramos que debe señalarse que es importante que la organización implante mecanismos que le permitan poder demostrar a posteriori haber cumplido con el deber de información al denunciado que le exige la normativa vigente. Dependiendo de la forma utilizada por el denunciante para comunicar la irregularidad esta información puede establecer las siguientes propuestas<sup>523</sup>:

- Si se cumplimenta un formulario electrónico incluido en la página Web o en la Intranet de la entidad, cabe incluir una cláusula de información en materia de protección de datos en un lugar visible del propio formulario.
- Si se envía un correo electrónico a un buzón específico de recepción de denuncias, se puede establecer un mecanismo automático para recibir un correo, el remitente reciba un correo de respuesta con la cláusula de información en materia de protección de datos.
- Si se envía una carta en soporte papel mediante correo postal a una determinada dirección, se debe remitir a la dirección postal del remitente o a la dirección electrónica si se hubiese facilitado, un correo con la cláusula de información en materia de protección de datos.

*b) Al denunciado y a terceras partes implicadas (afectados, testigos, etc.)*

Para el cumplimiento de la normativa de protección de datos (art. 5.4<sup>524</sup> LOPD), es preciso informar al titular de los datos sobre los extremos

---

<sup>523</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 629-630.

<sup>524</sup>El art. 5.4 de la LOPD dispone que "Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del

detallados en la misma, cuando éstos no hayan sido recabados directamente del propio titular, como puede ser el denunciado y terceras personas que puedan ser mencionadas o estar implicadas en los hechos de la denuncia.

La normativa exige que esa obligación de información a denunciados y terceras partes implicadas, sea cumplida por la entidad dentro de los tres meses siguientes al momento en que se recabaron los datos de su titular, que suele coincidir con la fecha de interposición de la denuncia.

Ese deber de información no implica revelar al denunciado y a terceras personas, la identidad del denunciante (o datos que permitan conocer o deducir su identidad), sino únicamente de lo siguiente<sup>525</sup>:

a) que ha sido denunciado a través del sistema de canal de denuncias que está implantado en la compañía;

b) de los hechos denunciados;

c) razón social y dirección del responsable del fichero que realice el tratamiento de la información;

d) Finalidad del tratamiento de los datos;

e) posibles comunicaciones de datos amparadas por la normativa a los Jueces y Tribunales y a las personas que se considere pertinentes implicadas en cualquier fase de la investigación, en el caso de grupo de empresas, especificar si se van a comunicar sus datos a otras entidades del grupo especificando siempre la razón social de la organización e información sobre sus actividades, direcciones y la concreta finalidad que motiva la comunicación;

---

*registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo".*

<sup>525</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 630-631.

- f) forma y dirección en el que ejercer los derechos de acceso, rectificación, cancelación y oposición;
- g) confidencialidad del sistema de denuncias;
- h) consecuencias que conlleva realizar una denuncia falsa con mala fe;
- i) no represalias por parte de la organización.

Para cumplir con este deber parece oportuno, lo antes posible y siempre en el plazo máximo de tres meses desde la recogida inicial de datos, celebrar una reunión individual con cada interesado (denunciado, afectados y testigos) en la que se pregunten por los hechos denunciados, redactando un acta en la que se incluya la cláusula de información de forma que, en un futuro, permita probar su cumplimiento por parte de la Organización ante cualquier requerimiento de información que pudiera hacer la AEPD.

*c) Excepción a la obligación de informar en el plazo máximo de tres meses*

Como regla general cualquier sociedad que tenga implantado un sistema interno de denuncias, el deber de información al denunciado y terceros interesados debe realizarse dentro de los tres meses siguientes al registro de sus datos. Con su cumplimiento se da la posibilidad al denunciado y a terceros interesados de poder defender debidamente sus intereses<sup>526</sup>.

Muchas entidades aprecian que existe cierto peligro al informar al denunciado que ha sido denunciado y los hechos sobre los que versa la denuncia, ya que éste podría eliminar indicios o pruebas comprometedoras. Por ello cabe plantearse si es posible retrasar el cumplimiento de este deber de información, durante el tiempo necesario para recabar evidencias sobre los hechos denunciados y extender su plazo más allá de los tres meses exigidos por la normativa. En el Dictamen 1/2006 del Grupo del Artículo 29 se

---

<sup>526</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 631.

contempla como excepción a la regla general, establecer la posibilidad de retrasar este deber de información, por el tiempo mínimo e imprescindible<sup>527</sup> cuando exista un riesgo importante de que dicha notificación pueda poner en peligro la capacidad de la entidad para investigar de manera eficaz la alegación o recopilar las pruebas necesarias. Sólo debe suponer retraso pero no una supresión de ese deber. Es preciso señalar que, en cambio, el Informe 128/2007 de la AEPD no menciona la posibilidad de que la entidad pueda retrasar el cumplimiento de este deber en situaciones excepcionales<sup>528</sup>.

Por tanto, puede concluirse que en los supuestos en los que exista un riesgo importante de que la notificación pondría en peligro la capacidad de la entidad para investigar o recopilar las pruebas necesarias, será la entidad la que deba valorar los riesgos de retrasar excepcionalmente la información al denunciado o si esa notificación ha de realizarse en el plazo de tres meses dispuesto en la normativa. Así, si la entidad se inclina por la posición expuesta en el Dictamen 1/2006 del Grupo del Artículo 29, al tratarse de una excepción a la regla general se ha de utilizar de forma puntual y los requisitos para su utilización deberían encuadrarse previamente aprobados y documentados por la entidad. En concreto debe tenerse en cuenta lo siguiente:

a) la excepción al deber de información debe ser acordada de manera restrictiva, caso por caso y aprobada por el Comité de Denuncias Internas;

---

<sup>527</sup> En relación con el deber de información al denunciado, el documento WP117 (Grupo de Trabajo del Artículo 29 creado por el artículo 29 de la Directiva 95/46/CE como Documento WP 117, la Opinión 1/2006) señala lo siguiente (...) La persona acusada en el informe de un denunciante, deberá ser informada por la persona a cargo del programa tan pronto como sea posible después de que los datos relativos a ella hayan sido registrados (...). En concreto, el empleado en cuestión deberá ser informado de: [1] la entidad responsable del programa de denuncia de irregularidades, [2] los hechos de los que se le acusa, [3] los departamentos y servicios que podrían recibir el informe dentro de su propia sociedad o en otras entidades o sociedades del grupo del que forma parte su sociedad, y [4] cómo ejercer sus derechos de acceso y rectificación.

No obstante, cuando exista un riesgo importante de que dicha notificación pondría en peligro la capacidad de la sociedad para investigar de manera eficaz la alegación o recopilar las pruebas necesarias, la notificación a la persona inculpada podría retrasarse mientras exista dicho riesgo. El objetivo de esta excepción a la norma dispuesta en el artículo 11 consiste en preservar las pruebas evitando su destrucción o alteración por la persona inculpada. Deberá aplicarse de manera restrictiva, caso por caso, y deberá tener en cuenta los intereses más amplios en juego."

<sup>528</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 631-632.

b) deben existir sospechas fundadas en criterios objetivos, que permitan considerar que si se cumpliera ese deber se pondría en peligro la investigación de la denuncia;

c) únicamente se puede retrasar la notificación por el tiempo mínimo e imprescindible durante el que existiera dicho riesgo.

Como la normativa española no contempla la posibilidad de excepción, puede ser recomendable que la entidad "retrase" este deber de información al límite del tiempo máximo dentro del plazo de tres meses que le otorga la normativa de protección de datos.

Para poder conocer la información electrónica que haya podido ser eliminada, la entidad puede utilizar herramientas de e-Discovery que le permitan examinar importantes cantidades de datos en formato electrónico que hayan sido obtenidas mediante procedimientos de Análisis Forense. De esta forma, la Entidad podrá realizar procedimientos de identificación, recopilación, custodia y localización de información en soporte electrónico, que posteriormente pueda ser utilizada como prueba para Jueces y Tribunales<sup>529</sup>.

### **2.2.2 Deber de calidad de los datos. Plazos de conservación de la información relacionada con la denuncia**

Para el cumplimiento del deber de calidad exigido por la normativa de protección de datos, los datos personales se han de conservar durante el tiempo estrictamente necesario para servir a la finalidad para la que fueron recabados. Al ser las denuncias una información que debido a su sensibilidad puede afectar negativamente a las personas implicadas en las mismas, es imprescindible que en la entidad (organización) se detallen unos plazos máximos durante los que se puede almacenar la denuncia e información surgida y elaborada como consecuencia de las mismas.

---

<sup>529</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 632-633.



Respecto a los plazos de conservación de la información sobre denuncias internas, el Dictamen 1/2006 del Grupo de Trabajo del Artículo 29 y el Informe AEPD sí son coincidentes. Así, establecen que *"Los datos personales tratados por un programa de denuncias de irregularidades deberían eliminarse inmediatamente, y normalmente en un plazo de dos meses desde la finalización de la investigación de los hechos alegados en el informe (...). Este plazo debería limitarse a la tramitación de las medidas de auditoría interna que resultasen necesarias y, como máximo, a la tramitación de los procedimientos judiciales que se derivasen de la investigación realizada (como los que se deriven de las medidas disciplinarias adoptadas o de la exigencia de responsabilidad contractual de los auditores)"*<sup>530</sup>.

Por tanto, podemos concluir que los plazos pueden ser los siguientes:

a) Durante la fase de investigación/instrucción de la denuncia interna<sup>531</sup>

Con carácter general, las denuncias e información surgida o elaborada como consecuencia de las mismas, puede ser almacenada durante el tiempo que dure la investigación, siempre que los plazos no sean excesivamente dilatados y puede conllevar un perjuicio para el denunciado<sup>532</sup>.

b) Finalizada la investigación/instrucción de la denuncia interna

b.1) Denuncias sobre hechos no probados. Deben ser eliminadas en un plazo de dos meses desde la finalización de la investigación de los hechos alegados. La AEPD, en relación con el plazo de conservación de los datos de las denuncias cuyos hechos no han sido probados, señala que deben ser eliminadas "en un plazo de dos meses desde la finalización de la investigación", si no derivan de la denuncia una investigación posterior.

---

<sup>530</sup> Informe 128/2007 AEPD, p. 9. ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 633-634.

<sup>531</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 634.

<sup>532</sup> Esto es, se almacenarán durante el plazo que dure la investigación y que, con carácter general, no podrá superar los 6 meses desde el inicio de la misma. (\*) Será el Comité de Denuncias Internas el que decida sobre la necesidad de ampliar el plazo para un supuesto concreto. Dicha decisión deberá ser motivada.

b.2) Denuncias sobre hechos probados. Los datos deben conservarse durante la tramitación del procedimiento. Si como consecuencia de la investigación los hechos de la denuncia son probados y de ello se deduce la adopción de determinadas medidas contra el denunciado, será posible conservar los datos por un plazo superior. Una vez finalizado el procedimiento (penal, laboral, etc.) se deben eliminar en el plazo de 2 meses desde su finalización.

### **2.2.3 Derechos de acceso, rectificación, cancelación y oposición (ARCO)**

Todo titular de datos está legitimado para ejercitar, respecto a sus propios datos, los derechos de acceso, rectificación, cancelación y oposición<sup>533</sup>. En este sentido, se considera necesario señalar determinadas cuestiones en relación a estos derechos en los supuestos de información relativa a denuncias internas<sup>534</sup>:

- El derecho de acceso que puede ejercitar el denunciado, exclusivamente le debe permitir obtener información de la denuncia pero siempre relacionada con sus datos personales, sin que se le comuniquen los datos identificativos del denunciante pues no hallaríamos ante un supuesto de cesión de datos no consentida. Habrá que tener en cuenta cuando se esté ejecutando este derecho de acceso, que no haya posibilidad de conocer los datos de otras personas y, específicamente, del denunciante.
- Durante la tramitación del expediente de la denuncia, no podrá ser ejecutado el derecho de cancelación que las partes hayan podido solicitar. No obstante lo anterior, una vez terminado el expediente e independientemente de que el denunciado solicite el derecho de

---

<sup>533</sup>Regulados en el Título III del RLOPD.

<sup>534</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 634-635.

cancelación de sus datos, es necesario tener en cuenta los plazos señalados de conservación de la información.

- Respecto al derecho de oposición los denunciados o terceros partes no puede oponerse a que sus datos sean tratados en el sistema de denuncias internas.

La entidad con independencia de que puedan o no ejecutarse estos derechos sobre la información del sistema de denuncias, en todo caso, debe contestar al interesado que ha realizado la petición en tiempo y forma<sup>535</sup>.

#### **2.2.4 Sanciones por incumplimiento**

En la siguiente tabla, se detallan los principales incumplimientos de la normativa de Protección de Datos que pueden ser cometidos por la Organización en la que se implante un sistema de denuncias sin cumplir con los requisitos exigidos por la misma, así como las sanciones económicas que dicho incumplimiento puede conllevar a la compañía (además del correspondiente daño reputacional)<sup>536</sup>:

---

<sup>535</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 635-636.

<sup>536</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 641.

INCUMPLIMIENTO	SANCIÓN <sup>537</sup>
Admitir en el sistema denuncias anónimas (artículo 4 LOPD)	Infracción Grave (40.001€ a 300.000€)
No eliminar la denuncia en plazo (artículo 4 LOPD)	Infracción Grave (40.001€ a 300.000€)
No informar al denunciante (artículo 5.1 LOPD)	Infracción Leve (900€ a 40.000€)
No informar al denunciado y/o terceros (artículo 5.4 LOPD)	Infracción Grave (40.001€ a 300.000€)
No implantar medidas de seguridad (Título VIII RLOPD)	Infracción Grave (40.001€ a 300.000€)
	Infracción Muy Grave (300.001€ a 600.000€)
No haber obtenido autorización para la TID –en caso de ser necesario (artículos 33 y 34 LOPD, Título VI)–	Infracción Muy Grave (300.001€ a 600.000€)

### 2.2.5 Medidas de seguridad a implantar en el canal de denuncia interna

Todas las denuncias e información surgida o elaborada como consecuencia de las mismas, pueden gestionarse en soporte papel y en soporte electrónico<sup>538</sup>.

Al tratarse de datos personales es necesario que los soportes en los que se gestionen y almacenen (sean en soporte informático o en soporte papel), tengan dispuestas las medidas de seguridad que permitan garantizar su confidencialidad, impidan el acceso a personal no autorizado, y posibles pérdidas de dicha información<sup>539</sup>.

<sup>537</sup> Dichas sanciones económicas son las establecidas por la LOPD (artículos 44 y 45), sin perjuicio de que la Agencia, en virtud del artículo 45.4 LOPD pueda establecer distinta graduación en la cuantía en función de diversos criterios (p.e. carácter continuado de la infracción, reincidencia, volumen de los tratamientos efectuados, volumen de negocio o actividad del infractor, grado de intencionalidad, etc.).

<sup>538</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 636.

<sup>539</sup> La descripción de las medidas de seguridad está recogida en el Título VIII del RLOPD

En relación con esas medidas de seguridad, hay que señalar que debido a la tipología de información de las denuncias internas, como mínimo, es conveniente que la organización implante en los sistemas de gestión de denuncias las medidas de seguridad de nivel medio, excepto en el caso de que se traten datos personales de nivel alto<sup>540</sup>, en cuyo caso se deberán implantar las medidas de seguridad de dicho nivel.

Tanto para las denuncias e información relacionada, en soporte electrónico o en soporte papel, se debe tener en cuenta lo siguiente<sup>541</sup>:

- a) únicamente se debe permitir el acceso a las denuncias (e información relacionada) a un grupo reducido de personas que lo necesiten por razón de sus funciones (así sólo podría acceder las personas concretas del Departamento de auditoría que lo gestiona);
- b) elaborar una relación actualizada de usuarios con acceso a los sistemas y los perfiles de los usuarios con acceso autorizado para uno de ellos;
- c) hacer firmar compromisos de confidencialidad específicos a las personas encargadas de la gestión de estos sistemas;
- d) comunicar inmediatamente cualquier incidencia de seguridad; trasladar inmediatamente al Comité de Denuncias cualquier anomalía, problema, accesos no autorizados, etc., relacionado con dicha información;

---

<sup>540</sup>El art. 81.3 de la RLOPD. "Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas c) Aquéllos que contengan datos derivados de actos de violencia de género" y en su apartado 4 se dispone que "A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento".

<sup>541</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 636-637.

e) llevar un registro de entrada y salida de la información, ya sea en papel o por correo electrónico (p.e. registro de salida con la información enviada a Jueces y Tribunales);

f) realizar la auditoría que exige el RLOPD sobre el fichero de denuncias internas, al menos, cada 2 años.

Respecto a las denuncias e información surgida o elaborada como consecuencia de las mismas en soporte electrónico, además de lo anterior, se deben implantar las siguientes medidas de seguridad<sup>542</sup>:

a) Establecer usuario y contraseña que caduquen por lo menos, una vez al año, para la autenticación del sistema. Además, las contraseñas han de ser almacenadas, mientras estén vigentes, de forma ininteligible.

b) Almacenar toda la información relativa a denuncias internas en el sistema de información, incluidos los correos con información sobre denuncias internas (no en el buzón de correo ni en el equipo informático).

c) Realizar copias de seguridad, por lo menos una vez a la semana (a no ser que la información haya sido modificada).

d) Prohibir expresamente almacenar este tipo de información en USB, pendrives o cualquier tipo de dispositivos portátiles.

e) De cada intento de acceso al sistema de información (en caso de que se almacenen datos de nivel alto) se guardarán durante 2 años, como mínimo:

\* la identificación del usuario,

\* la fecha y hora en que se realizó,

---

<sup>542</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 637-638.

\* el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado,

\* en el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro de nivel alto accedido.

En este caso, el responsable de seguridad, o la persona delegada por éste, se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

Respecto a las denuncias e información surgida o elaborada como consecuencia de las mismas en soporte papel, se deberán cumplir lo siguiente<sup>543</sup>:

a) Archivarla según el criterio que permita garantizar la correcta conservación de los documentos, la localización y consulta de la información.

b) Almacenarla en armarios o cajones que estarán cerrados con llave.

c) No almacenarla sobre las mesas de trabajo, excepto cuando se esté trabajando sobre el mismo, siendo su usuario responsable de su custodia.

d) Registrar la salida y/o la entrada de documentos.

e) Eliminar la información cuando sea necesario, de forma que no se pueda recuperar su información (p.e. destructoras).

f) Archivar (en caso de que existan documentos con datos de nivel alto) en salas cerradas en las que el acceso esté protegido con puertas de

---

<sup>543</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 638.

acceso con llave, que deben permanecer cerradas cuando no sea preciso el acceso a dichos documentos o soportes.

g) Custodiar los documentos durante su transporte por una persona hasta su destino.

Si la entidad ha notificado el fichero ante la AEPD como de nivel alto (o que, sin tener datos de nivel alto, se encuentre notificado como parte de otro fichero que tuviera un nivel alto como puede ser el de Gestión de Personal), pueden existir ficheros que sean de un nivel inferior por no contener información de esa tipología, se podrán aplicar otras medidas de seguridad.

En virtud de lo dispuesto en el artículo 81.8<sup>544</sup> RLOPD y siempre que se puedan delimitar los datos y los usuarios con acceso autorizado (además de hacer referencia a esta circunstancia en el Documento de Seguridad de la Organización), pueden establecerse medidas de seguridad diferentes a las declaradas para el fichero principal, siendo de aplicación en cada sistema en el nivel de aplicación que corresponda con la tipología de datos tratada. En el sistema que contenga datos de nivel alto se han de aplicar esas medidas pero sobre aquel que no contenga esta tipología de datos y se cumplan los requisitos especificados en el mencionado artículo, la compañía podrá aplicar las medidas de seguridad de nivel medio<sup>545</sup>.

Estos sistemas comportan el almacenamiento de datos personales, por lo que las condiciones de su implantación están sometidas a la legislación española sobre la materia. La interpretación de esta legislación defendida por el Gabinete Jurídico de la AEPD en la respuesta a una consulta de 2007 fijó una serie de pautas en cuestiones tales como el tiempo máximo de

---

<sup>544</sup>Art. 81.8 RLOPD. "A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad".

<sup>545</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 639.



almacenamiento de la información, las medidas de seguridad aplicables, el derecho de acceso o los requisitos para la transferencia de datos al extranjero etc... El seguimiento por una empresa no debería ser valorada negativamente por un juez penal aun cuando la voluntad de respetar esas limitaciones suponga una menor efectividad en el empleo de esos procedimientos<sup>546</sup>.

### **2.3 Aceptación de las normas y política de privacidad**

La formulación de una denuncia interna supone la aceptación íntegra y sin reservas de la norma de funcionamiento del canal de denuncia y la Política de Privacidad.

De acuerdo con lo dispuesto en la LOPD, la empresa ha de informar a los usuarios del canal de denuncia de la existencia de un fichero de datos de carácter personal debidamente inscrito en el Registro General de Protección de Datos, creado con los datos que le sean facilitados a través de dicho Canal de Denuncia, por y para la empresa, y bajo su responsabilidad, con la finalidad de gestionar las denuncias que se formulen internamente por la presunta comisión de actos contrarios a la Ley en el seno de la empresa o en perjuicio de ésta y las infracciones del Código Ético de Conducta de la entidad.

Los usuarios que formulen una denuncia interna aceptan expresamente la inclusión de los datos que faciliten a través del canal de denuncia en ese fichero automatizado de datos de carácter personal. A su vez, los usuarios prestan su consentimiento para que sus datos de carácter personal puedan ser cedidos o comunicados a las Fuerzas y Cuerpos de Seguridad del Estado, a otros órganos de la Administración Pública con competencias en la investigación de los hechos denunciados y a los Tribunales de Justicia y demás órganos jurisdiccionales<sup>547</sup>.

---

<sup>546</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. p. 188.

<sup>547</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., pp. 1246-1247.

La entidad se compromete a respetar la confidencialidad de los datos incluidos en el fichero y a utilizarlos de acuerdo con su finalidad, así como a dar cumplimiento a su obligación de guardarlos y adoptar todas las medidas para evitar la alteración, pérdida, tratamiento o acceso no autorizado. La empresa mantendrá la confidencialidad de los datos de los usuarios que formulen denuncias internas, impidiendo el acceso a los mismos por parte de las personas denunciadas<sup>548</sup>.

Como ya hemos analizado, los titulares de datos de carácter personal incluidos en ese fichero pueden ejercitar, con respecto a los mismos, los derechos reconocidos en LOPD y, en particular, los derechos de acceso, rectificación y cancelación; así como el derecho de oposición, cuando resulte pertinente<sup>549</sup>.

Se ha de informar a los titulares de datos de carácter personal incluidos en el fichero de que para el ejercicio de los derechos referidos deben indicar una serie de datos básicos<sup>550</sup>.

## **2.4 Ausencia de represalias**

Es una conclusión fundamental la de que para procurar el correcto funcionamiento de un canal de denuncias se han de prohibir las represalias, las amenazas y las coacciones contra las personas que formulen denuncias internas de buena fe. Con el fin de garantizarlo, el denunciante debería tener derecho a acudir al Oficial de Cumplimiento Normativo o al Director de la Asesoría Jurídica con el fin de obtener orientación y protección frente a las

---

<sup>548</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., pp. 1247-1248.

<sup>549</sup>Los derechos referidos en el párrafo precedente podrán ejercitarse por cada titular mediante solicitud por correo electrónico dirigido a [privacidad@xxxxxx.com](mailto:privacidad@xxxxxx.com) o por correo postal ordinario dirigido a<sup>549</sup>: consultora o despacho jurídico. Se ha de informar a los usuarios y al resto de titulares de datos de carácter personal incluidos en el fichero "Canal de Denuncia", que xxxxx es una consultoría legal externa de la empresa que ostenta la condición de encargada del tratamiento de los datos del citado fichero y que tiene encomendado atender, por cuenta de la empresa, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición.

<sup>550</sup>Cfr. Art. 25 RLOPD.

posibles represalias que pudiera estar padeciendo por el mero hecho de haber formulado una denuncia interna<sup>551</sup>.

#### **2.4.1 Protección por el Derecho constitucional y laboral**

Las situaciones o comportamientos denunciados por el whistleblower tienen lugar en el entorno laboral y la información revelada puede perjudicar o poner en peligro intereses de compañeros o superiores. La protección que brinda el derecho laboral al denunciante es distinta dependiendo de si el perjuicio proviene del empleador (despido principalmente, pero caben otras: dificultades a la promoción, cambios en los turnos...) o, por el contrario, de algún compañero (agresiones físicas o verbales).

Ya han sido analizadas en este trabajo las medidas disciplinarias que el empresario puede adoptar respecto de los empleados agresores, que son quizás las herramientas más inmediatas de protección del delator frente a sus compañeros y son las que tienen consecuencias directamente para ellos. Sin embargo no es ésta la única vía disponible<sup>552</sup>.

En este sentido, se debe tener en cuenta que entre los derechos de los trabajadores también se encuentra "*el respeto de su intimidad y la consideración debida a su dignidad*"<sup>553</sup> y su "*integridad física*"<sup>554</sup>. Por su parte, la LPRL reconoce a los trabajadores el "*derecho a una protección eficaz en materia de seguridad y salud en el trabajo*"<sup>555</sup> y el correlativo deber del empresario de proporcionar esta protección. La existencia de acoso o violencia en la entidad, desde el momento en que genera un daño —físico o psicológico—, supone que la prevención de riesgos laborales no ha sido lo efectiva que debiera y, que por tanto el empresario no ha cumplido con la obligación que le impone la LPRL. El trabajador objeto de represalias está habilitado a solicitar la extinción del contrato laboral, conservando su derecho

---

<sup>551</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1246.

<sup>552</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 227.

<sup>553</sup>Art. 4.2 e TRLET.

<sup>554</sup>Art. 4.2 d TRLET.

<sup>555</sup>Art. 14 LPRL.

a indemnización por despido improcedente e incluso añadiendo a dicha indemnización la que pudiera derivar de la responsabilidad civil por los daños y perjuicios causados por parte del empresario, adicionales a la propia extinción (art. 50.1 c del TRLET)<sup>556</sup>.

La posibilidad de rescindir el contrato por incumplimiento del empresario opera cuando quien ha actuado contra el delator es el propio empresario, en el marco de la relación empresario-empleado. La protección del denunciante dispone además de otras alternativas que, sin embargo, presentan alguna dificultad añadida<sup>557</sup>.

Es necesario resaltar que las represalias ejercidas por el empleador ponen en riesgo las libertades de expresión e información frente a la buena fe contractual. El trabajador es titular de los derechos fundamentales que recoge nuestra Constitución, éstos pueden verse modulados para equilibrarse con los intereses del empresario. Además de los cánones propios de las libertades de información y expresión (los requerimientos de información veraz y de que la expresión de opiniones no se haya realizado a través de apelativos formalmente injuriosos e innecesarios), en el ámbito laboral pueden verse moduladas por la buena fe y el deber de secreto y sigilo. Cabe plantearse si dicha modulación limita hasta el punto de impedir la denuncia por parte del trabajador, amparando las acciones tomadas por el empleador contra aquél en respuesta a su delación, es decir si el empresario puede despedir disciplinariamente (o imponer otro tipo sanción) al trabajador que denuncia, basándose en un incumplimiento de la buena fe.

El TC ha señalado que *“el deber de buena fe que pesa sobre el trabajador no se puede interpretar en términos tales que vengan a resultar amparadas por esta exigencia de honestidad y lealtad en el cumplimiento de las obligaciones, situaciones o circunstancias que, lejos de corresponderse con el ámbito*

---

<sup>556</sup>“Cualquier otro incumplimiento grave de sus obligaciones por parte del empresario, salvo los supuestos de fuerza mayor, así como la negativa del mismo a reintegrar al trabajador en sus anteriores condiciones de trabajo en los supuestos previstos en los artículos 40 y 41, cuando una sentencia judicial haya declarado los mismos injustificados” (art. 50.1.c TRLET de 2015).

<sup>557</sup>GARCIA MORENO, B., “Whistleblowing...”, ob. cit., pp. 227-228.

normal y regular de la prestación de trabajo, supondrían desviaciones de tal normalidad”<sup>558</sup>. Dado que los ilícitos y la falta de ética no encajan dentro del “ámbito normal y regular de la prestación de trabajo”, se ha de concluir que la buena fe no es un argumento válido para castigar la delación en la empresa. Es importante señalar que la buena fe vincula al trabajador y al empresario, pues ambos tienen derecho a esperar de la otra parte una actuación leal, social y contractualmente correcta. El empresario sólo podrá exigir una actuación de buena fe por parte del empleado cuando su actuación sea igualmente correcta y leal<sup>559</sup>.

#### 2.4.2 Protección por el Derecho penal

El Derecho penal no es ajeno a la delación, aunque su aproximación ha sido hasta la fecha limitada. El tratamiento penal del delator en España se ha circunscrito a la protección del criminal arrepentido que decide revelar delitos en los que ha intervenido como autor o partícipe (bien a través de la atenuante genérica de confesión, bien mediante la rebaja de la pena<sup>560</sup> para

---

<sup>558</sup>FJ 9 STC (Sala Primera) núm. 6/1988, de 21 enero (RTC 1988\6).

<sup>559</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 228.

<sup>560</sup>El artículo 376 del CP cuyo epígrafe es Atenuación de la pena dispone lo siguiente:

*"En los casos previstos en los artículos 361 a 372, los jueces o tribunales, razonándolo en la sentencia, podrán imponer la pena inferior en uno o dos grados a la señalada por la ley para el delito de que se trate, siempre que el sujeto haya abandonado voluntariamente sus actividades delictivas y haya colaborado activamente con las autoridades o sus agentes bien para impedir la producción del delito, bien para obtener pruebas decisivas para la identificación o captura de otros responsables o para impedir la actuación o el desarrollo de las organizaciones o asociaciones a las que haya pertenecido o con las que haya colaborado.*

*Igualmente, en los casos previstos en los artículos 368 a 372, los jueces o tribunales podrán imponer la pena inferior en uno o dos grados al reo que, siendo drogodependiente en el momento de comisión de los hechos, acredite suficientemente que ha finalizado con éxito un tratamiento de deshabituación, siempre que la cantidad de drogas tóxicas, estupefacientes o sustancias psicotrópicas no fuese de notoria importancia o de extrema gravedad".*

El artículo 579 CP cuyo epígrafe es Provocación, conspiración y proposición para cometer delitos de terrorismo establece lo siguiente:

*"1. Será castigado con la pena inferior en uno o dos grados a la prevista para el delito de que se trate el que, por cualquier medio, difunda públicamente mensajes o consignas que tengan como finalidad o que, por su contenido, sean idóneos para incitar a otros a la comisión de alguno de los delitos de este Capítulo.*

*2. La misma pena se impondrá al que, públicamente o ante una concurrencia de personas, incite a otros a la comisión de alguno de los delitos de este Capítulo, así como a quien solicite a otra persona que los cometa.*

*3. Los demás actos de provocación, conspiración y proposición para cometer alguno de los delitos regulados en este Capítulo se castigarán también con la pena inferior en uno o dos grados a la que corresponda respectivamente a los hechos previstos en este Capítulo.*

los delitos relacionados con el terrorismo y el tráfico de drogas). La delación de quien no ha tenido participación en los hechos es una institución desconocida para el Derecho penal. En el CP se encuentran algunos preceptos que pueden resultar útiles en la protección del denunciante-testigo<sup>561</sup>. Así, por ejemplo, frente a las represalias, se castiga como autor de un delito de obstrucción a la justicia, al que *“con violencia o intimidación intentare influir directa o indirectamente en quien sea denunciante, parte o imputado, abogado, procurador, perito, intérprete o testigo en un procedimiento para que modifique su actuación procesal”* y a quien *“realizare cualquier acto atentatorio contra la vida, integridad, libertad, libertad sexual o bienes, como represalia contra las personas citadas en el apartado anterior, por su actuación en procedimiento judicial”* (art. 464 CP). Estas disposiciones no contemplan el caso de quien es objeto de represalias meramente laborales con posterioridad a su denuncia o testimonio en el proceso, y no resultan aplicables a los casos en los que las represalias sucedan cuando la información aún no ha salido de la empresa y no se ha iniciado ni se tiene conocimiento de que se vaya a iniciar un proceso judicial. El castigo de estos comportamientos debe buscarse en otros tipos penales como, por ejemplo, el de coacciones o en los delitos contra la integridad moral.

El Derecho penal proporciona al delator una herramienta fundamental para la protección de su identidad: el delito de revelación de secretos. El CP prevé un tipo agravado de revelación de secretos en razón de la esfera de dominio profesional del sujeto activo, que castiga con penas de prisión de hasta 5 años al responsable de los archivos o registros que desvele su contenido. Se trata de un arma de doble filo pues, en el tráfico de informaciones que implica un mecanismo de este tipo, la conducta del whistleblower podría considerarse

---

4. En los casos previstos en este precepto, los jueces o tribunales podrán adoptar las medidas establecidas en los apartados 4 y 5 del artículo anterior”.

<sup>561</sup> Para comentarios sobre el CP, y al objeto de abordar los principios generales aplicables en materia común y de tipos penales, ver la magnífica obra de LÓPEZ BARJA DE QUIROGA, J: *“Tratado de Derecho Penal”*. Civitas Ediciones. 2010.

en algunos casos típica en cuanto “utilice en perjuicio del titular de los datos o de un tercero” información obtenida sin autorización (art. 197.2 CP).

### **2.4.3 Programas de amnistía y otros incentivos**

El reforzamiento del blindaje del whistleblower frente a las represalias, (frecuentemente el ofrecimiento de protección) no es suficiente para que aquél que conoce alguna irregularidad se decida a desvelarla. La experiencia avala que los sistemas de denuncia que mejores resultados alcanzan son los que ofrecen a cambio de la información otro tipo de incentivos, como las recompensas económicas<sup>562</sup>.

Es complicado fomentar la delación en aquél que tiene alguna implicación en la infracción a denunciar, pues además de los riesgos habituales que enfrenta el whistleblower, debe asumir las responsabilidades derivadas de su infracción; por lo que las consecuencias negativas que para él tenga su propia denuncia son mucho mayores que en los casos de whistleblower-testigo. Cuando la empresa está realmente interesada en conseguir la información, debe poner a su disposición otros incentivos. Uno de los instrumentos utilizados en estos casos es la amnistía interna. La empresa no puede prometer al denunciante que no será sancionado penalmente, pero puede ofrecer no imponer sanción disciplinaria, ni iniciar acciones para la reclamación de los daños que la infracción hubiera podido causar a la compañía e, incluso, puede comprometerse a sufragar los costes de su defensa. Este tipo de incentivos debe usarse con prudencia. En primer lugar, porque la decisión de no perseguir infracciones que perjudican a la entidad, lesionando su patrimonio o su reputación, podría llegar a ser incluso constitutiva de un delito de administración desleal. El recurso a la amnistía debe estar siempre basado en una ventaja o beneficio para la empresa, así el poder usar la información para beneficiarse de la atenuante por colaboración. Y, en segundo lugar, porque la credibilidad de la política de cumplimiento de

---

<sup>562</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., pp. 229-230.

la entidad y la confianza de los empleados en el canal de denuncia pueden resultar seriamente dañadas si se utilizan de forma indebida como, por ejemplo, para favorecer a determinados infractores; así como cuando se conceden cuando no eran necesarias porque la empresa ya tenía conocimiento de la infracción por otros medios o se concentran, de forma injustificada, en los empleados que ocupan puestos más altos en la jerarquía.

Para que un canal de denuncia sea eficaz, para que los denunciante acudan a él cuando tengan conocimiento o sospecha de una irregularidad es necesario que confíen en el sistema. Una de las claves de esa confianza es garantizar al denunciante una protección real y efectiva frente a las posibles consecuencias negativas derivadas de su delación, pues difícilmente un trabajador accederá a informar si no se le garantiza de posibles acciones (del empresario o de otros trabajadores) tendentes a perjudicar su carrera profesional o sus derechos laborales. La configuración del sistema de protección del whistleblower es decisiva para el éxito del programa de cumplimiento<sup>563</sup>. Las empresas estadounidenses, bien por propia iniciativa o por exigencias derivadas de la sección 806 de la Sarbanes-Oxley Act, han incorporado en sus *compliance programs* disposiciones con esta propuesta, pero el débil valor jurídico de estos programas convierte la protección en ellos contenida y merma su eficacia. A lo sumo, las disposiciones del código pueden considerarse que operan como cláusulas contractuales dentro de la relación laboral, lo que habilita al empleado a reclamar ante los tribunales los perjuicios causados por las represalias tomadas por otro trabajador o por el empresario en respuesta a su denuncia.

Ahora bien, la práctica evidencia que esta protección es limitada y que si el denunciante es despedido, las posibilidades de reincorporarse al puesto son escasas; ya que en el ordenamiento español se hace depender de una vulneración de derechos fundamentales y, si se considera el despido como

---

<sup>563</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 226.



improcedente, el empresario puede optar por la indemnización<sup>564</sup>, la declaración del despido como nulo es difícil.

## 2.5 Voluntariedad vs. Obligatoriedad

Las políticas en materia de whistleblowing han girado en torno a dos elementos: la eficaz protección del denunciante frente a represalias y los mecanismos de fomento de la delación. Tal y como hemos analizado en el Capítulo anterior, estos fundamentos responden a la concepción de los canales de denuncia como herramientas de uso voluntario.

Aunque es poco respaldada, la idea del uso obligatorio del canal de denuncia ha comenzado a introducirse en los debates académicos e, incluso, legislativos. La SOX incluyó entre sus disposiciones la obligación de los abogados de las compañías cotizadas de comunicar al director ejecutivo o al responsable del departamento jurídico las violaciones de la legislación del mercado de valores u otro tipo de irregularidades de las que tuviera conocimiento. La reforma del Código Penal español establece una nueva redacción del artículo 31 bis, que en su apartado 5 se refiere los elementos que debe tener un modelo de prevención para que las empresas puedan evitar la responsabilidad penal, y que de acuerdo a su literal redacción parece exigir que el uso del canal de denuncia corporativo tenga carácter obligatorio<sup>565</sup>. A diferencia de la SOX, que limita la obligación de denuncia a un sector profesional y en el que podría estar justificado el nuevo artículo 31 bis extiende esta obligación a todos los trabajadores de la entidad, lo que generará previsiblemente importantes problemas prácticos<sup>566</sup>.

No parece que la imposición del uso del canal encaje con un modelo de *Compliance* basado en la ética, el diálogo y la transparencia. La obligación de

---

<sup>564</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 226.

<sup>565</sup>"Los modelos de organización y gestión a que se refieren la condición 1.ª del apartado 2 y el apartado anterior deberán cumplir los siguientes requisitos: [...]4.º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención".

<sup>566</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 220.

denunciar responde en realidad a una dinámica completamente diferente y su implantación en la empresa la alejaría de los objetivos de su programa de cumplimiento. Lejos de crear un clima de confianza, donde empleados y directivos se sientan libres de plantear dudas e inquietudes sobre la licitud o la ética de sus comportamientos, la denuncia obligatoria generaría recelos entre compañeros y rechazo al sistema de cumplimiento.

En cambio, algunos autores comienzan a apuntar que configurar la denuncia de irregularidades como una obligación y no como un derecho podría contribuir decisivamente a paliar algunos de los defectos que aquejan no sólo los sistemas de denuncia sino, en general, la política de cumplimiento de la empresa. Y es que no hay duda de que los trabajadores son los mejores posicionados para identificar los riesgos y conocer las prácticas irregulares dentro de la organización (participan en el diario funcionamiento de la empresa, están en contacto con compañeros y superiores y conocen su actitud en el trabajo, y conocen con detalle los procedimientos). Los directivos de una entidad pueden no tener un conocimiento tan profundo de las cuestiones, por lo que la información que aportan los trabajadores a través del canal de denuncias es especialmente valiosa. Para una eficaz política de cumplimiento, es necesario contar con información fiable y suministrada puntualmente. La configuración de la denuncia como derecho en lugar de como obligación supondría “desaprovechar” una de las herramientas más potentes en materia de prevención y detección de irregularidades<sup>567</sup>.

La cuestión que se plantea entonces es en qué medida y bajo qué circunstancias puede una empresa imponer tal obligación a sus empleados. Algunos autores han apuntado que la implementación de mecanismos que aseguren el derecho de los trabajadores a denunciar impone implícitamente un deber de hacerlo. Disponer de canales y de fácil acceso y no utilizarlos hace- en cierta forma -al trabajador que no denuncia responsable en parte de los hechos. TSAHURIDU y VANDEKERCKHOVE expresaban esta idea en

---

<sup>567</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., pp. 220-221.

los siguientes términos: “*Knowing leads to responsibility just as doing does*”<sup>568</sup>. La cuestión es si éste es un deber moral o puede ser legalmente exigido.

En el marco del ordenamiento jurídico español vigente, tal y como se ha delimitado anteriormente esta cuestión también puede abordarse desde la perspectiva del Derecho penal o del Derecho laboral.

Desde la perspectiva laboral, la incorporación del deber de denunciar no plantea problemas en los casos en los que el puesto de trabajo o la concreta actividad encomendada implican una especial responsabilidad sobre el correcto desarrollo de la misma. Así no habría duda sobre la obligación del auditor de denunciar las irregularidades contables de las que tuviera conocimiento, y lo mismo ocurre con los responsables de departamento respecto de las conductas de sus subordinados o con los abogados de la compañía que sepan de la realización de prácticas ilícitas en ella. En todos estos casos, la obligación de denunciar cabe considerarla implícita al puesto e incluida en el contenido del contrato laboral.

Es unánime que plantea problemas mayores la incorporación de un deber genérico de denuncia que alcance a todos los empleados de la entidad independientemente de cuál sea su estatus en la empresa y el contenido de su contrato laboral. En estos casos, la buena fe y la fuerza vinculante de los códigos de conducta han sido los argumentos utilizados para fundamentar su admisibilidad, pero no están libres de controversia<sup>569</sup>.

La buena fe, por sí sola, difícilmente puede justificar una obligación no incluida entre los deberes del trabajador previstos en el TRLET, ni en su contrato de trabajo, como se desprende del artículo 5 del TRLET<sup>570</sup>. Este

---

<sup>568</sup> TSAHURIDU, E.E. / VANDEKERCKHOVE, W., “Organisational Whistleblowing Policies: Making Employees Responsible or Liable?”, *Journal of Business Ethics*, vol. 82, Issue 1, 2008, pp 107–118

<sup>569</sup> GARCIA MORENO, B., “Whistleblowing...”, ob. cit., pp. 221-222.

<sup>570</sup> El artículo 5 del TRLET cuyo epígrafe es Deberes laborales establece que “*Los trabajadores tienen como deberes básicos:*

a) *Cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad con las reglas de la buena fe y diligencia.*  
b) *Observar las medidas de prevención de riesgos laborales que se adopten.*

precepto impone al empleado la actuación diligente y de buena fe respecto del cumplimiento de las “*obligaciones concretas de su puesto de trabajo*”. La obligación de denunciar sólo está presente en determinados puestos y profesiones, por lo que la buena fe resulta argumento insuficiente para fundamentar la existencia de un deber genérico de denuncia de irregularidades<sup>571</sup>.

Los códigos de conducta aportan una base más sólida sobre la que basar la obligación de denuncia. La eficacia jurídica de estos instrumentos ha sido objeto de diversos pronunciamientos judiciales (SSTS 8 de febrero de 2005 y 7 de marzo de 2007, entre otras) que han mantenido que, a pesar de que las empresas carecen de un poder unilateral normativo, al emanar sus disposiciones de un auténtico poder jurídico de corte unilateral (el poder de dirección del empresario, artículo 20 del TRLET) crean obligaciones en el trabajador concretando la esfera de actuación debida por éste. Esta facultad de la empresa podría abrir el camino a la incorporación, vía código ético, de la obligación genérica de denuncia.

Los códigos éticos no pueden sobrepasar el ejercicio regular del poder de dirección y que éste debe circunscribirse a las instrucciones relativas a la ejecución del contrato<sup>572</sup>. Al final la situación acaba siendo muy similar a la que aparecía bajo el argumento de la buena fe. El poder de dirección del empresario cuenta con otros límites que también pueden resultar significativos en este contexto. El Tribunal Supremo en sentencia de 7 de marzo de 2007 señaló que “(...) *el poder de dirección no puede entenderse como una facultad arbitraria y omnímoda, sino que se encuentra sometido a determinadas limitaciones, debiendo utilizarse con el máximo respeto a los derechos del trabajador y a su dignidad humana...*”.

---

c) *Cumplir las órdenes e instrucciones del empresario en el ejercicio regular de sus facultades directivas.*

d) *No concurrir con la actividad de la empresa, en los términos fijados en esta ley.*

e) *Contribuir a la mejora de la productividad.*

f) *Cuanto se deriven, en su caso, de los respectivos contratos de trabajo*”.

<sup>571</sup>GARCIA MORENO, B., “Whistleblowing...”, ob. cit., p. 222.

<sup>572</sup>Art. 20.2 ET.

GOÑI señaló que la delación obligatoria para todo tipo de conductas conduciría a *“resultados poco satisfactorios, a un diseño cuasi policial de empresa, poco acorde con el máximo respeto a los derechos del trabajador, a su libertad y dignidad, dado que el trabajador se convierte en guardián y confidente del empresario”*. Es complicado encontrar en la legislación laboral herramientas que justifiquen o que amparen la obligación genérica de denunciar irregularidades.

Desde la perspectiva penal, el argumento más recurrente es el proporcionado por el artículo 450.1 CP<sup>573</sup>, que castiga a quien *“pudiendo hacerlo con su intervención inmediata y sin riesgo propio o ajeno, no impidiere la comisión de un delito que afecte a las personas en su vida, integridad o salud, libertad o libertad sexual”*.

GOÑI manifiesta que *“sólo con los argumentos empleados para establecer el deber penal de actuación, se podría justificar fácilmente la obligación de revelar del trabajador, sin necesidad de que venga formalmente exigido por un código”*. El deber de denuncia impuesto por el CP (art. 450) persiste independientemente de que el delito tenga lugar en el entorno laboral o fuera de él, existiría una obligación de los trabajadores —como la de cualquier otro ciudadano— de denunciar las conductas mencionadas en el precepto. Esa obligación no es referida al canal de denuncia interna. El empleado que decida acudir al Fiscal o a la policía también estará actuando conforme al CP. El canal corporativo podría ser una de las opciones al alcance del trabajador para cumplir con el deber de actuación que le impone el CP, pero desde luego no la única<sup>574</sup>. Cuando se tratase de delitos contra bienes jurídicos distintos a los mencionados en el art. 450 CP, o se tratara de situaciones no tipificadas penalmente, o de infracciones ya consumadas, la posibilidad de

---

<sup>573</sup>“El que, pudiendo hacerlo con su intervención inmediata y sin riesgo propio o ajeno, no impidiere la comisión de un delito que afecte a las personas en su vida, integridad o salud, libertad o libertad sexual, será castigado con la pena de prisión de seis meses a dos años si el delito fuera contra la vida, y la de multa de seis a veinticuatro meses en los demás casos, salvo que al delito no impedido le correspondiera igual o menor pena, en cuyo caso se impondrá la pena inferior en grado a la de aquél” (art. 450.1 CP).

<sup>574</sup>GARCIA MORENO, B., “Whistleblowing...”, ob. cit., pp. 222-223.

esgrimir este precepto desaparece. Por ello, la argumentación basada en el “deber penal de actuación” es débil para fundamentar la obligatoriedad del uso del canal.

### **3. Delimitación del ámbito del canal de denuncia**

Desde el punto de vista territorial, es importante que en el caso de Grupos de empresas (formado por entidades ubicadas en distintos países) se defina previamente cuál de todas llevará la gestión de las denuncias (que normalmente suele coincidir con la matriz del Grupo). No obstante, dependiendo de los países de ubicación de las empresas puede ser recomendable que, debido a las diferencias culturales y legislativas, se establezcan diferentes grupos de recepción y resolución (p.e. Comité de Denuncias de América Latina, Comité de Denuncias de Europa, Comité de Denuncias de Oriente Medio, etc.) de forma que, por un lado, permitan una gestión eficaz de estos canales y, por otro lado, animen a los sujetos a denunciar los comportamientos que, igual en un modelo tan amplio y con muchas diferencias culturales, no se hubieran atrevido a reportar<sup>575</sup>.

#### **3.1 Delimitación del ámbito material**

La mayoría de la doctrina opina que a través del canal de denuncia sólo se pueden denunciar la comisión de actos contrarios a la ley en el seno de la empresa o en perjuicio de éstas y las infracciones de su Código Ético de Conducta<sup>576</sup> (Hechos Denunciables).

Tal y como hemos analizado, los canales de denuncias aparecieron con fuerza en el panorama corporativo a raíz de los escándalos financieros de la pasada década, pero la entrada en escena de los whistleblowers hay que buscarla más atrás y, muchas veces desvinculada de irregularidades de contenido económico. Los casos de Ford (1978), Firestone (1973), la Hooker Chemical Company (1975) o el Challenger (1986) muestran que lo que ha

---

<sup>575</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 614-615.

<sup>576</sup> MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1242.

movilizado tradicionalmente a los whistleblowers han sido situaciones de peligro para bienes como la vida o la salud de las personas y la protección del medio ambiente<sup>577</sup>. Estos canales también han adquirido relevancia como mecanismos de prevención del acoso sexual y el mobbing. Sin embargo, hay quien considera que ésta no es la vía más adecuada para descubrir este tipo de comportamientos y aboga por restringir el ámbito de los canales a irregularidades contables, fiscales, de organización interna y las relacionadas con el mercado de valores. Es decir, las de contenido económico y las que causen —o puedan causar— una alteración en el funcionamiento de la empresa.

Otro sector, también partidario de un uso restrictivo del canal, propone un criterio delimitador distinto: la gravedad de la conducta. Deslindar las conductas denunciables en función de su gravedad y no a través de su delimitación material objetiva puede plantear problemas. En la consideración de grave no siempre coincide la jurídica o la económica, lo que puede generar confusión entre los potenciales usuarios del canal. Algunos de los defensores de esta configuración apuestan por circunscribir el ámbito material del canal a las conductas tipificadas como ilícitos penales o administrativos.

La opción más seguida por las grandes compañías es la de considerar como comportamientos susceptibles de denuncia aquellos contrarios al código ético de la compañía. La mayoría de estos códigos recogen como propia la normativa legal y tipifican como infracción del código lo que es una infracción penal o administrativa, añadiendo como violaciones del código ético los incumplimientos de los protocolos establecidos para la prevención de las infracciones. Esta opción supone una significativa ampliación del ámbito material del canal<sup>578</sup>.

De cara a la efectividad de la política de cumplimiento de la empresa es aconsejable no restringir el acceso al canal, sino favorecer su utilización ante

---

<sup>577</sup>HASSINK, H./ DE VRIES, M. / BOLLEN, L., "A Content Analysis of Whistleblowing Policies of Leading European Companies", *Journal of Business Ethics*, vol. 75, Issue 1, 2007, pp 25–44.

<sup>578</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., pp. 218-219.

cualquier sospecha. De este criterio —“If in doubt, report”— parten muchos de los *compliance programs* de las grandes compañías norteamericanas. Resulta preferible llevar a cabo la criba en un momento posterior, bien una vez efectuado un análisis preliminar de los hechos decidiendo no continuar con la investigación, bien una vez terminada la investigación decidiendo no imponer sanción alguna<sup>579</sup>.

Dentro del ámbito material del canal, es necesario delimitar el contenido de las denuncias: el grado de certeza exigido al denunciante sobre la información reportada.

Una posición excesivamente permisiva incentivará la denuncia de meros rumores y facilitará el camino a denuncias de mala fe, realizadas con el propósito de perjudicar a un compañero o superior o, incluso, para beneficiarse de la protección brindada al denunciante y evitar un despido o una sanción disciplinaria, argumentando que ello constituiría un castigo por la información revelada. Una postura muy exigente requiriendo al denunciante que para utilizar el canal esté plenamente acreditado que los hechos que va a denunciar son ciertos, las denuncias serán escasas y sin que afecten generalmente a las altas jerarquías o a cuestiones importantes que serán especialmente ocultadas. La utilización de un criterio subjetivo parece la opción más adecuada, de forma que sería suficiente que el denunciante tenga una creencia razonable sobre la veracidad de la información que denuncia.

Al diseñar estos instrumentos de información hay que optar entre la conveniencia de acotar los posibles objetos de denuncia o permitir al denunciante la máxima libertad en el relato de los hechos denunciados. La limitación del objeto de denuncia- puede efectuarse sin especiales dificultades técnicas a través de un diseño de los aplicativos de denuncia on line que obligue al denunciante, mediante un catálogo cerrado de infracciones, a especificar el motivo de su denuncia y puede tener como ventaja el actuar

---

<sup>579</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., pp. 219-224.



como filtro de informaciones sobre hechos carentes de toda trascendencia desde un punto de vista jurídico. Desde una perspectiva penal, ambas opciones son admisibles, siempre y cuando, en el caso de optarse por la primera, se incluya un catálogo amplio de infracciones susceptibles de denuncia, pues una relación excesivamente limitada podría interpretarse como una muestra por parte de la empresa de falta de interés en recibir información acerca de determinados hechos.

Cuando se opte por un sistema que limite las posibles irregularidades objeto de una eventual denuncia es aconsejable reservar un espacio para que el denunciante pueda exponer con sus propias palabras los hechos de los que haya tenido conocimiento, pues no cabe descartar que en el diseño del aplicativo se hayan omitido algunas potenciales irregularidades o que el empleado tenga dudas en encuadrar los hechos denunciados en una determinada categoría. Es recomendable facilitar técnicamente la posibilidad, en el caso de aplicativos en línea, de que el informante pueda adjuntar elementos de prueba (documental) que doten de mayor verosimilitud a su denuncia y faciliten una posterior investigación interna<sup>580</sup>.

## **3.2 Delimitación del ámbito subjetivo**

### **3.2.1 Legitimación activa**

Todo sujeto obligado por el Código Ético de Conducta de la empresa o "Persona Sujeta" tiene la obligación moral inexcusable de denunciar internamente cualquier Hecho Denunciable del que tenga conocimiento. También podrá formular una denuncia interna cualquier persona que tenga conocimiento de la comisión de un Hecho Denunciable, sin que resulte necesario que ostente la condición de Persona Sujeta<sup>581</sup>.

Desde el punto de vista subjetivo, al tratarse de un canal interno establecido en la entidad, su uso por los empleados de la misma es evidente, sin

---

<sup>580</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 183-184.

<sup>581</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1242.

embargo, los hechos presuntamente delictivos podrían realizarse también por personas que, sin ser empleados, desarrollen otro tipo de labores en la compañía o estén vinculados con otro tipo de relación<sup>582</sup>. La cuestión es si se considera que para que el canal de denuncias internas sea eficaz es necesario que al mismo tengan acceso los empleados de la organización y todo aquél que mantenga con la misma un vínculo contractual de derecho laboral, mercantil o civil como puede ser el caso de colaboradores, proveedores, subcontratados, etc. con independencia de la modalidad contractual que determine su relación con la misma, tal y como lo define la AEPD en su Informe 128/2007<sup>583</sup>.

Las personas que pueden tener conocimiento de irregularidades en la empresa son diversas (trabajadores, proveedores, clientes, terceros que no tengan relación directa con la corporación) pero en mi opinión no todos deberían estar legitimados para usar el canal. La difusión de la existencia del canal entre un grupo tan amplio de potenciales delatores y la complejidad que supondría en el desarrollo de la investigación posterior son inconvenientes a tener en cuenta, en relación con los beneficios que se pueden obtener.

Para algunos autores, el criterio para establecer la legitimación activa debe ser la existencia de interés legítimo. Una formulación de estas características se encuentra con la dificultad de determinar la existencia del mismo sin haber entrado a conocer del asunto<sup>584</sup>.

Se recomienda acudir a criterios objetivos como, por ejemplo, tener una relación laboral o mercantil con la entidad. Así, trabajadores, proveedores y

---

<sup>582</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 614.

<sup>583</sup> Informe de AEPD 128/2007 "(...) Como se indica en la consulta, los denunciantes y denunciados a los que se refiere el sistema que pretende crearse serán en todo caso empleados de la compañía, es decir, se encontrarán, en general, vinculados a la misma por una relación laboral, siendo trabajadores de la misma o, en su caso y en un sentido amplio, mantendrán con la compañía un vínculo derivado de un contrato de arrendamiento de servicios con algún tipo de compromiso de exclusividad. En consecuencia, todas las personas cuyos datos pueden ser tratados como consecuencia del establecimiento de procedimientos de denuncia mantendrán con la sociedad un vínculo contractual de derecho laboral, civil o mercantil (...)" (punto IV 9º pár.).

<sup>584</sup> GARCIA MORENO, B., "Whistleblowing...", ob. cit., pp. 215-216.

demás contratistas, es decir, los sujetos más próximos a la empresa a las posibles irregularidades quedarían habilitados para utilizar el canal. Los consumidores, los trabajadores que no se atrevieron a denunciar en su momento cuando estaban en la empresa y, en general, todos los que de alguna manera afecta la actividad de la empresa habrá de recurrir a vías de denuncia alternativas.

Los medios de comunicación o las autoridades son las alternativas escogidas por los delatores que no podían o no querían utilizar el canal de denuncia interno. La propia entidad podría proporcionar a estos colectivos de stakeholders una alternativa a su canal de denuncia interno; ésta posibilidad proporcionaría a la entidad un instrumento adicional para controlar la información sobre irregularidades. El establecimiento de dos canales diferenciados, otorgándole a los usuarios de uno y otro estatutos diferentes, permitiría evitar las desventajas derivadas de una ampliación excesiva de los criterios de legitimación, sin renunciar a parte de la información<sup>585</sup>.

De acuerdo con el análisis realizado anteriormente, resulta dudosa-especialmente en España- la cuestión de si en estos procedimientos cabe aceptar denuncias anónimas o aquellas en las que el sujeto se identifica mediante seudónimo.

Desde el punto de vista de la eficacia en la prevención del delito un sistema que acepta denuncias anónimas puede parecer que tendrá mayor capacidad de descubrir delitos frente a otro que rechace esas informaciones<sup>586</sup>. Es posible que trabajadores predispuestos a denunciar no lo hagan si tienen que identificarse, por temor a represalias o por no aparecer como delatores ante sus compañeros. Un sistema que admita el anonimato puede ayudar a vencer estos inconvenientes pero el hecho de que no sea necesario revelar la

---

<sup>585</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 216.

<sup>586</sup>El Dictamen 1/2006 (p. 11) apunta a que la admisión de denuncias anónimas puede ir en detrimento de la eficacia de la medida, entre otros motivos, por una supuesta mayor dificultad de las investigaciones cuando el denunciante no se identifica, la menor fiabilidad que en principio cabe atribuir a las fuentes anónimas o, incluso, el riesgo de dañar la convivencia entre empleados.

identidad del denunciante aumenta el riesgo de que el buzón de denuncia se utilice para realizar falsas imputaciones, si bien este peligro puede compensarse exigiendo al denunciante anónimo que aporte algún tipo de evidencia de sus afirmaciones para que éstas puedan considerarse verosímiles y den lugar a una investigación interna<sup>587588</sup>.

Con el ánimo de garantizar la credibilidad de las denuncias y evitar abusos es aconsejable que se informe a los trabajadores de las consecuencias laborales e incluso penales que pueden sufrir en el caso de denunciar a alguien falsamente; así como que cuando se dé a conocer la existencia de estos procedimientos se informe expresamente a los trabajadores de que no podrán sufrir ningún tipo de represalia laboral por el hecho de haber informado de buena fe acerca de conductas irregulares. Con independencia de las responsabilidades en las que puedan haber incurrido ellos mismos en caso de haber tomado parte en esos hechos, pues la empresa no está en condiciones de eximir al empleado de tal responsabilidad, especialmente si ésta tiene naturaleza jurídico-penal<sup>589</sup>.

Tal y como hemos visto anteriormente, en España la regulación administrativa de la materia parece no aceptar la posibilidad del anonimato en el caso de los sistemas que comporten tratamiento automatizado de datos o. Esa es la interpretación de la LOPD que sostiene la AEPD en el Informe nº 2007/0128 de su Gabinete Jurídico<sup>590</sup>. Es una opinión más estricta a la que impera en Estados Unidos, donde la legislación permite garantizar a las empresas el anonimato a las denuncias internas<sup>591</sup>, a la previamente contenida en el

---

<sup>587</sup> El Code of Practice británico aconseja que no se incentiven las denuncias anónimas, no tanto por razones de legalidad, sino porque el anonimato dificulta las posteriores investigaciones o el contacto con la persona denunciante y propicia el abuso de las denuncias (4.5.4).

<sup>588</sup> RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 179, 178 y 181.

<sup>589</sup> Interesantes al respecto las consideraciones del Code of Practice británico, especialmente apartados 4.8 y 4.9.

<sup>590</sup> Apartado 5 del Informe ([https://www.agpd.es/portaIwebAGPD/canaIdocumentacion/informes\\_juridicos/otras\\_cuestiones/index-ides-idphp.php](https://www.agpd.es/portaIwebAGPD/canaIdocumentacion/informes_juridicos/otras_cuestiones/index-ides-idphp.php)). Crítico con esta perspectiva, y con la del grupo de trabajo europeo, ALONSO GALLO, J., "Los programas de cumplimiento", ob. cit., pp. 183-184.

<sup>591</sup> QUIGLEY, S. K., "Whistleblower...", ob. cit., p. 292.

Dictamen elaborado por el Grupo de Trabajo comunitario<sup>592</sup> o, en las recomendaciones recogidas en el Código Unificado de Buen Gobierno de la CNMV española<sup>593</sup>.

En el Dictamen del Grupo de Trabajo comunitario se señala que "por lo que respecta a las normas de protección de datos, los informes anónimos plantean un problema específico con respecto al requisito esencial de que los datos personales solo deberían recopilarse de manera leal. Como norma, el Grupo de Trabajo considera que solo los informes identificados deberían comunicarse a través de programas de denuncia de irregularidades para satisfacer este requisito". Continúa señalando que "el Grupo de Trabajo es consciente de que algunos denunciadores podrían no encontrarse siempre en situación o tener disposición psicológica para presentar informes identificados. También es consciente del hecho de que las quejas anónimas son una realidad dentro de las sociedades, incluso y especialmente en ausencia de sistemas de denuncia de irregularidades confidenciales y organizados, y que esta realidad no puede ignorarse". Se concluye admitiendo la posibilidad excepcional de admitir tales denuncias si no se fomenta el anonimato y se dedica un especial cuidado y celeridad a las investigaciones<sup>594</sup>.

Desde el punto de vista del Derecho penal no debería interpretarse que perjudica a las empresas que no incluyeran la posibilidad del anonimato los tribunales no deberían interpretar, que por no haber incluido tal opción de denuncia anónima la empresa habría renunciado a dotar sus procedimientos del grado de eficacia necesario para beneficiarse de la correspondiente atenuación. El considerar que estos procedimientos solo deben activarse

---

<sup>592</sup>GOÑI SEIN, J.L., pone de manifiesto cómo el informe español es mucho más restrictivo con las denuncias anónimas, añadiendo que "*la prohibición de aceptar denuncias anónimas coloca en una muy difícil coyuntura a las empresas estadounidenses con presencia en territorio español porque se enfrentan, por un lado, al riesgo de ser sancionadas por la Agencia Española de Protección de Datos si no cumplen con la orientación indicada y, por otro, se exponen a que las autoridades de los EE.UU. les sancionen si no cumplen con las exigencias de la Ley SOX de permitir presentar denuncias de forma anónima*" ("Sistema de denuncia...", ob. cit., p. 337).

<sup>593</sup>P. 44.

<sup>594</sup>Pp. 11-12.

cuando la información sea creíble es una razón adicional perfectamente legítima para no incluir la opción del anonimato<sup>595</sup>.

El que en las denuncias anónimas no se contemple en los procedimientos prefijados de denuncia no tiene que significar que cuando se reciban denuncias anónimas o por otras vías no estén obligados a reaccionar si éstas tienen cierto grado de verosimilitud<sup>596</sup>. La omisión de actuación ante esas denuncias puede ser indicio de una falta de ejercicio de debido control sobre los empleados que permita sostener la responsabilidad de la persona jurídica en los términos del inciso II del art. 31 bis 1 CP o, incluso, del dolo de los directivos responsables, pudiendo dar lugar a responsabilidad de la persona jurídica y de personas físicas. En los procedimientos debe preverse que cuando se reciba una denuncia anónima verosímil la empresa actuará diligente en orden a comprobar su veracidad<sup>597</sup>.

Aunque no se admitan denuncias anónimas, con el fin de proporcionar mayor eficacia del sistema es aconsejable<sup>598</sup> garantizar a los denunciantes de buena fe que la empresa mantendrá la confidencialidad respecto de su identidad, al objeto de evitar represalias. El informe del Gabinete Jurídico de la AEPD consideró que la confidencialidad es compatible con el marco legal vigente en materia de protección de datos y que de esa normativa no cabe extraerse el derecho del denunciado a acceder a la identidad del denunciante<sup>599</sup>. En España, no puede garantizarse a los informantes la confidencialidad hasta el punto de que la empresa pueda negarse a facilitar esa información; ante un requerimiento judicial en ese caso la empresa debe revelar tal identidad, de

---

<sup>595</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 181-182.

<sup>596</sup>Se coincide plenamente en este punto con lo manifestado por GOÑI SEIN, J.L., "Sistemas de denuncia...", ob. cit., p. 338, en su crítica por poco práctica a la postura de la Agencia Española de Protección de Datos. Desde un punto de vista jurídico-penal es más evidente aún, si cabe, que una empresa no puede permanecer impasible ante la recepción de lacto de información anónima verosímil y, en consecuencia, parecería mucho más adecuado que tal hipótesis se regulara adecuadamente en los procedimientos de denuncia.

<sup>597</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 182-183.

<sup>598</sup>Cfr. por ejemplo el Código de Conducta de SACYR VALLEHERMOSO, p. 38 (extraído de <http://www.gruposyv.com/syv/repositorio/syv/ficheros/14/CODIGODECONDUCTASYV2010.pdf>) o el IBERDROLA (cfr. supra nota 45), p. 12.

<sup>599</sup>Cfr. apartado V del Informe 2007/0128.

no hacerlo, los responsables de la negativa pueden incurrir en un delito de desobediencia<sup>600</sup>.

### **3.2.2 Legitimación pasiva**

Son susceptibles de ser denunciadas (Personas Denunciables) por medio del canal de denuncia: los administradores, los directivos, los empleados, los asesores, los subcontratistas, los distribuidores y los proveedores de la empresa, y en general, cualquier persona o entidad que cometa un hecho denunciabile<sup>601</sup>.

Para valorar positivamente la eficacia ex ante de un sistema de denuncia como medida de descubrimiento y prevención del delito debe admitir que cualquier persona relacionada con la empresa, sea directivo o trabajador, sea susceptible de ser denunciado. La limitación de los posibles denunciados requerirá de una justificación muy fundada, pues en caso contrario puede ser valorado por el juez penal como un indicio de falta de interés en el descubrimiento de determinados hechos.

El marco legal vigente en materia de protección de datos no impone ninguna limitación en cuanto a posibles denunciados. El Dictamen 1/2006 señala que el Grupo de Trabajo "deja a la discreción de los responsables del tratamiento de datos, con posible verificación de las autoridades competentes, la determinación de si dichas restricciones son adecuadas en las circunstancias específicas en las que operen"<sup>602</sup>.

### **3.3 Delimitación del ámbito territorial**

A la hora de definir el procedimiento del canal de denuncias hay que determinar cuál es el ámbito territorial en el caso de grupos de empresas

---

<sup>600</sup>De hecho, el aviso de que la confidencialidad no podrá preservarse en caso de reclamación de las autoridades tanto administrativas como judiciales se contiene en Códigos de Conducta como, por ejemplo, el de IBERDROLA <http://www.iberdrola.es/webibd/gc/prod/es/doc/normascodigoiberdrola.pdf>

<sup>601</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1242.

<sup>602</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. p. 183.

ubicadas en distintos países y definir previamente cuál de ellas llevará la gestión de las denuncias que suele ser la matriz. Dependiendo de los países de ubicación de las empresas hay que tener en cuenta las diferencias legislativas, pues pueden establecerse diferentes órganos de recepción y resolución, de forma que permitan una gestión eficaz de estos canales<sup>603</sup>. Hay que tener presente en este sentido las diferencias culturales.

## **4. Organización**

### **4.1 Cuestiones básicas**

La responsabilidad de implementar un canal de denuncia le corresponde a la entidad, pero ello no supone que necesariamente sea ella quien lo gestione. Puede encargarse a algún miembro o departamento de la entidad, y también puede externalizarse, cediendo su gestión a otra entidad especializada o a un despacho jurídico.

El modelo externalizado o *outsourced* tiene diversas ventajas frente a la gestión interna. Cada vez es más frecuente la externalización. Desde la perspectiva de la empresa, se considera que mejora la efectividad del canal. Los encargados de recibir las denuncias, de custodiar los documentos, de realizar la investigación y de imponer o proponer una sanción serán personas independientes e imparciales, no tendrán un interés por una solución en un determinado sentido y que no estarán contaminadas por las opiniones de trabajadores y de superiores de la entidad. Se asegura al whistleblower que su denuncia será adecuadamente valorada, que la investigación se realizará con todas las garantías y que las medidas que en su caso se adopten serán las más apropiadas. Esta independencia de los gestores del canal cabe sostener que se consigue mejor si éstos son personas ajenas a la empresa y

---

<sup>603</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 614-615.



no trabajadores de la propia entidad y por tanto, compañeros del delator y del acusado<sup>604</sup>.

La gestión externa, si queda en manos de un despacho jurídico, puede ofrecer ventajas respecto a la protección de la información que llega al canal. Los hechos denunciados, la identidad del denunciante y el resultado de la investigación constituyen material sensible cuyo uso la entidad puede pretender controlar. En un proceso judicial, el requerimiento del Juez hace decaer cualquier pretensión de confidencialidad salvo la debida al secreto profesional. Externalizar la gestión del canal se presenta como la mejor opción para salvaguardar la información que se obtenga por medio de la hotline.

Desde el punto de vista corporativo, pueden derivarse ventajas a efectos de responsabilidad. Con independencia del alcance del debido control requerido por el artículo 31.bis del CP para evitar la responsabilidad penal de la entidad por los delitos cometidos por sus empleados en provecho de la entidad, la implementación y el funcionamiento correcto de un canal de denuncia es un claro indicio de que la entidad ha actuado responsablemente en la prevención de la comisión de actos ilícitos. No es requisito necesario el que el canal sea gestionado de forma externa para que su existencia sea tomada en consideración, pero la externalización de la gestión del canal a través de un ente especializado proporciona garantías de su buen funcionamiento y de actuación responsable.

El modelo outsourced presenta ventajas para la entidad y para el denunciante. Si el gestor externo del canal fuera un abogado o un despacho jurídico, la protección de la información frente al requerimiento judicial también beneficiaría al whistleblower. Su identidad podría continuar oculta

---

<sup>604</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., pp. 216-217.

incluso durante el proceso penal, evitando así una de las circunstancias que más desincentivan al delator: verse envuelto en un largo proceso penal<sup>605</sup>.

Por ello, con el fin de garantizar mayores cotas de confidencialidad e independencia, algunas empresas optan por externalizar los sistemas de recepción y tratamiento de denuncias, que pasan a depender de otra entidad cuyos servicios se contratan. En algunos casos la externalización sólo alcanza a la implantación y mantenimiento del aplicativo on line y a la recepción de la información, que es canalizada inmediatamente hacia el departamento interno de la empresa para investigarla. En otros casos, el servicio del proveedor externo incluye la realización de la investigación interna que se efectúa para comprobar la veracidad de la denuncia<sup>606</sup>. Algunos grupos multinacionales recurren a este sistema ya que les permite extender el ámbito de aplicación a los países en los que operan sus empresas y resolver posibles problemas normativos, culturales e idiomáticos, ya que estos proveedores suelen garantizar funcionamiento del procedimiento atendiendo a esas particularidades. En Alemania, es frecuente distinguir entre dos grandes clases de receptores de denuncias: el *compliance officer* interno y el *ombudsman* externo, que suele ser un abogado<sup>607</sup>.

También debe señalarse que la externalización puede ser una forma de organización con especial sentido en el caso de pequeñas o medianas empresas, a las que generalmente le resultará costoso el mantenimiento de una estructura propia de recepción e investigación de denuncias y tendrán dificultades para garantizar independencia de responsables del procedimiento. Desde el punto de vista penal, también puede ser defendible que la externalización no tiene que considerarse *per se* un método más adecuado de gestión de las denuncias pues también es cierto que la empresa

---

<sup>605</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., pp. 217-218.

<sup>606</sup>El Code of Practice británico subraya la necesidad de que estos sistemas se ajusten a la normativa aplicable en materia de protección de datos personales.

<sup>607</sup>Cfr. en tal sentido LUTTERBACH, C., "Die strafrechtliche Würdigung...", ob. cit., p. 50 y KOCH, ZIS, 10/2008, p. 501. Según este último autor, a diferencia de los compliance officers los abogados externos tienen un deber de confidencialidad garantizado penalmente y no están obligados a declarar como testigos.

externa tiene un interés económico en satisfacer las expectativas de la empresa que la haya contratado y ello la expone a presiones similares a las que pueden soportar ciertos cargos situados en la propia organización empresarial<sup>608</sup>. La empresa externa puede recibir las denuncias e investigar, pero la toma de decisiones a partir del resultado (posibles despidos o denuncias penales, por ejemplo) corresponde a los responsables de la empresa contratante, por tanto, si éstos tuvieran interés en ocultar esas irregularidades podrían hacerlo<sup>609</sup>.

Otra forma de externalización de denuncias es la que en la que la recepción de la información y las potestades de investigación y decisión le corresponde a un órgano externo del que se hayan dotado las empresas de un determinado sector, en virtud de su voluntad de autorregularse<sup>610</sup>.

Los medios disponibles para comunicar las informaciones son también muy diversos, siempre recomendable el ofrecimiento de varios de ellos, para que sea el denunciante quien elija aquél que considera oportuno. Los medios tradicionales han sido: correo postal, el fax o las entrevistas personales, aunque han perdido relevancia frente a otras alternativas<sup>611</sup>.

---

<sup>608</sup>En caso de externalización deben cumplirse, además, ciertas exigencias específicas de la normativa en materia de protección de datos: cfr. al respecto GOÑI SEIN, J.L., "Sistemas de denuncia...", ob. cit., p. 352 y el Dictamen 1/2006, pp. 17-18.

<sup>609</sup>Como afirma GOÑI SEIN, J.L., "Sistemas de denuncia...", ob. cit., pp. 352-353, "de nada sirve encargar a un proveedor externo la Investigación, si no se proporcionan garantías de independencia por parte de las personas que reciban esta información, lo que es especialmente importante cuando la denuncia involucre o implique directa o indirectamente a la dirección ejecutiva o a los responsables de la empresa"

<sup>610</sup>El ejemplo en España es el Reglamento de los Órganos de Control del Sistema de Autorregulación de la Industria Farmacéutica, que tiene como cometido velar por el cumplimiento de los códigos de conducta de este sector y, en especial, del Código de Buenas Prácticas de Promoción de Medicamentos y de Interrelación de la Industria Farmacéutica con los Profesionales Sanitarios (Cfr. [http://www.farmaindustria.es/Farma\\_Public/Codigo/CPS/index.htm](http://www.farmaindustria.es/Farma_Public/Codigo/CPS/index.htm)). El art. 8.1 de este texto dispone que "el procedimiento se incoará por denuncia de cualquier persona que tenga interés legítimo en que se proceda en relación con una determinada actividad de interrelación con los profesionales sanitarios o con las organizaciones de pacientes, o por denuncia de la Unidad de Supervisión Deontológica".

Se trata, no obstante al tenor del precepto, de un procedimiento claramente pensado para que sean empresas competidoras las que procedan a denunciar las prácticas ilícitas pues las exigencias formales de las denuncias son numerosas (necesidad de aportar original y seis copias y de cumplimentar diversos apartados relacionados en el Propio texto: cfr. apartado 8.2).

<sup>611</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 218.

Las líneas telefónicas o buzones de voz y el email son, a priori, los medios preferidos aunque este último plantea algunos problemas en cuanto a la protección de la identidad del delator: no es viable en los casos de denuncias anónimas, pues a una cuenta de correo electrónico hay asociado un nombre; y aunque sería posible admitir las denuncias confidenciales a través de este sistema, la garantía de protección se vería mermada: un simple forward del correo que contiene la denuncia a quien no está autorizado al tratamiento de datos en el canal podría conllevar serias consecuencias para el delator y para la empresa.

En los últimos años, las posibilidades de la red han ganado terreno: habilitar un banner en la página web oficial de la compañía o incluir una aplicación en su intranet a estos efectos son algunos de los mecanismos utilizados por empresas y por trabajadores<sup>612</sup>.

Por otra parte se plantea cuáles deben ser los canales de denuncia. Es posible establecer diversos canales para que la información del empleado o tercero denunciante llegue a los encargados de impulsar las correspondientes investigaciones, los más frecuentes son: el correo postal y electrónico, el teléfono o el fax. Para asegurarse de que el sistema será valorado como eficaz por un juez penal se debe prever todos los medios razonablemente posibles para la recepción de información. Una vez previsto el correo electrónico, poca efectividad aporta el correo postal, el teléfono o el fax. Hay quien sostiene que existen razones de peso para considerar que una empresa que dispone de un sistema accesible de correo electrónico pueda verse perjudicada en términos jurídico-penales por no haberse dotado de medios adicionales<sup>613</sup>.

Es desaconsejable prever un sistema que solo admita la denuncia mediante correo postal, su falta de agilidad puede ser interpretada por un juez como muestra de un escaso interés en proporcionar por parte de la empresa la

---

<sup>612</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 218.

<sup>613</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 188-189.

recepción de denuncias. Igual parecer puede aplicarse a cualquier sistema que imponga al denunciante excesivas cargas formales (presentación de copias escritas, cumplimentación de determinados formularios o modelos especialmente farragosos etc.). Si se optara por el teléfono como único canal o junto a otros convendría contar con medios para grabar las conversaciones a fin de que, si es necesario posteriormente puedan ser utilizadas como justificación de la investigación interna y como prueba en un juicio.

Con independencia del canal de denuncia escogido, es aconsejable que dedique específicamente al envío y recepción de denuncias y que solo sea accesible para las personas expresamente autorizadas. Así se logrará garantizar la efectiva confidencialidad del medio o los medios previstos, exigencia básica que deben cumplir para su efectividad estos procedimientos<sup>614</sup>. Ha de valorarse positivamente la posibilidad que ofrecen algunos sistemas on line de que el aplicativo de denuncia permita envío de información, y que el responsable de su gestión pueda comunicarse con el denunciante para aclarar los términos de la información aportada<sup>615</sup>. Esta opción permite descartar con mayor conocimiento las informaciones carentes de interés, y a su vez facilitar la obtención de pruebas que sirvan para acreditar la denuncia<sup>616</sup>.

Otro tema fundamental es ante quién hay que denunciar. En Derecho español, actualmente no se establece que el receptor de la denuncia deba ser un determinado cargo o departamento dentro de la empresa<sup>617</sup>. El Código Unificado de Buen Gobierno de la CNMV recomienda a las sociedades cotizadas que encomienden al Comité de Auditoría el establecimiento y

---

<sup>614</sup>Cfr. al respecto las consideraciones de GOÑI SEIN, J.L., "Sistemas de denuncia...", ob. cit., p. 325.

<sup>615</sup>Ofrecen tal posibilidad sistemas como el "Business Keeper Monitoring System" (<http://www.business-keeper.com/the-basic-principle.html>).

<sup>616</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. p. 188.

<sup>617</sup>Sobre esta cuestión GOÑI SEIN, J.L., "Sistemas de denuncia...", ob. cit., pp. 326 ss. Este autor pone de manifiesto, con mención de concretos ejemplos, cómo en la práctica el sujeto receptor de las quejas varía de unas compañías a otras. La Sarbanes-Oxley Act, en cambio, impone que las denuncias vayan directamente a la comisión de auditoría.

seguimiento de procedimientos de whistleblowing interno<sup>618</sup>. El Dictamen 1/2006 del Grupo de Trabajo establece directrices en relación con la normativa de protección de datos que pueden trasladarse al ámbito jurídico-penal. Se recomienda que las empresas establezcan *"una organización específica dentro de la sociedad o del grupo dedicada a tratar los informes de los denunciantes y que dirija la investigación"*, señalando que esa organización *"deberá estar compuesta de personal especialmente formado y dedicado, limitado en su número y vinculado contractualmente por obligaciones"*. Se advierte que *"este sistema de denuncia de irregularidades debería estar estrictamente separado de otros departamentos de la sociedad, tales como el departamento de recursos humanos"*. Estas observaciones se fundamentan en la denominada *"política de puerta abierta"* con la que se pretende *"crear canales de comunicación que permitan que el empleado se dirija directamente a la dirección sin pasar por sus superiores jerárquicos"*<sup>619</sup>.

El Code of Practice elaborado por Public Concern at Work y la British Standards Institution (apt. 3.2) recomienda que en el procedimiento estén implicados los departamentos de auditoría interna, cumplimiento normativo y recursos humanos, con la finalidad en este último caso de garantizar que intervendrán en la investigación interna las personas más adecuadas, pero sin participar directamente en la investigación, para de este modo no perder independencia a la hora de tomar decisiones. Se recomienda que en la información que se dé a los empleados sobre los procedimientos de denuncia se les aconseje que, en primera instancia, denuncien ante sus superiores inmediatos, como recurso más sencillo y natural dentro de la propia organización de la empresa<sup>620</sup>.

---

<sup>618</sup>BACIGALUPO ZAPATER, E., "Responsabilidad penal...", aptdo VI, ob. cit., atribuye la tarea a un departamento especializado de cumplimiento normativo con un compliance officer al frente, vinculándose dicho departamento con las *"competencias de las comisiones de cumplimiento y de control interno a las que se refieren las recomendaciones 44 y 45 del Código Unificado de Buen Gobierno de las Sociedades Cotizadas"*. Sobre los departamentos encargados del cumplimiento normativo en la empresa cfr. ALONSO GALLO, J., "Los programas de cumplimiento", ob. cit., pp. 170-171.

<sup>619</sup>ALONSO GALLO, J., "Los programas de cumplimiento", ob. cit., p. 180.

<sup>620</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 184-185.

En el diseño de este aspecto del procedimiento interno de denuncia pueden proponerse algunas directrices con objeto de poder hacerlo valer como medida eficaz de descubrimiento y prevención del delito ante un tribunal.

En primer lugar el receptor de la denuncia debe ser una persona con conocimientos jurídicos suficientes para discriminar de entrada las informaciones que pueden tener interés de aquellas otras que carecen de relevancia no solo jurídico-penal, sino legal. Puede ser que la persona denunciante además quiera revelar determinados hechos, o pida consejo sobre cómo proceder en adelante. Por ello es necesario que la persona que le asesore tenga conocimientos fiables sobre las consecuencias futuras del comportamiento del whistleblower<sup>621</sup>.

En segundo lugar, debe ser una persona o grupo de personas que, dentro de la organización empresarial, tengan independencia respecto de los departamentos con mayor riesgo de realización de prácticas ilícitas, bien por comisión activa o por omisión y estén en condiciones reales de garantizar la confidencialidad a la persona denunciante<sup>622</sup>. En Estados Unidos, la Federal Deposit Insurance Corporation ha señalado que "cuanta más independencia se utilice para administrar una hotline, mayor confianza tendrán los denunciadores para informar de irregularidades"<sup>623</sup>.

Deben tener capacidad de impulsar la investigación interna y la posibilidad de acceso directo a los órganos de dirección y administración de la entidad y a otros posibles órganos de control o a los socios. Con esta última previsión se pretende dotar al cargo de autonomía suficiente por si las denuncias se refieren a posibles irregularidades cometidas por los más altos cargos de la empresa. No es imprescindible el que sea un cargo específico y exclusivo

---

<sup>621</sup>El Code of Practice elaborado por Public Concern at Work y la British Standards Institution (apt. 3.7) diferencian incluso entre las hotlines de denuncia y las helplines de asesoramiento.

<sup>622</sup>En tal sentido afirma GOÑI SEIN, J.L., "Sistemas de denuncia...", ob. cit., pp. 350-351 que "una premisa básica para la identificación de las conductas fraudulentas o irregulares mediante denuncia no anónima es la existencia de un órgano independiente de gestión de las denuncias (...) el mecanismo de denuncia debe presentar las características de un sistema imparcial y objetivo o, de lo contrario, su valencia o eficacia será nula".

<sup>623</sup>Financial Institution Letter 80/2005 (cfr. supra nota 47).

cuyo único objetivo sea la gestión de denuncias, esa posibilidad está en relación con las dimensiones de la empresa.

Por último señalar que en el proceso de designación de la persona o personas encargadas de llevar a cabo la investigación se han de excluir a personas que, por acción u omisión, puedan haber contribuido a la conducta irregular que debe investigarse<sup>624</sup>.

## 4.2 Figuras implicadas

La estructura organizativa que debe asumir las funciones de recepción de denuncias, investigación de los hechos y, en general, todas aquellas acciones que conlleva la gestión íntegra de un sistema de denuncias, debe estar integrado por un equipo multidisciplinar pero que cuente con la confianza y el respaldo de la Dirección, ya que va a gestionar información que, por su sensibilidad, en caso de una mala utilización, puede poner en peligro la reputación de la entidad y causar graves daños.

A continuación se detalla una estructura organizativa para la gestión íntegra del canal de denuncias<sup>625</sup>:

1. El Comité de Denuncias Internas, es el órgano que debe ostentar la mayor responsabilidad en un canal de denuncias. Su función principal es hacer cumplir el procedimiento de denuncias, garantizar su confidencialidad en todo el proceso y una correcta y eficaz gestión del sistema interno de denuncias.

Para su imparcialidad en los hechos investigados es recomendable que sea un órgano colegiado, independiente dentro de la organización, o formado por los responsables de las áreas que de una forma directa o indirecta pueden estar relacionados con la denuncia, así: el Director de Auditoría Interna, el Director de Asesoría Jurídica, el Director de Recursos Humanos, el Director de Responsabilidad Social Corporativa, el *Compliance Officer*. De entre los

---

<sup>624</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 185-186 y 190.

<sup>625</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 620-621.



miembros del Comité de Denuncias Internas deberá designarse un Secretario cuya principal función sea, entre otras, la de levantar Actas de las reuniones. Será importante revisar si los miembros del Comité están afectados por un conflicto de intereses. Si se recibieran comunicaciones que hicieran referencia a su persona, a personas de su confianza o, en el caso del Responsable de Instrucción, a alguna adscrita al Departamento. En tal caso, el miembro del Comité, o el Responsable de la Instrucción, inmediatamente deben informar al Comité y abstenerse de participar en el tratamiento de la denuncia.

Entre sus principales funciones deberán contemplarse, como mínimo: a) recepcionar la denuncia por cualquiera de las formas oficialmente admitidas para la entrada de las mismas; b) decidir motivadamente si la denuncia se desestima o si se procede a su estudio y tramitación conforme al procedimiento; c) designar, por cada denuncia, al Responsable de la fase de instrucción; d) aprobar de forma motivada las excepciones al procedimiento general aprobado e implantado; e) exigir el cumplimiento de las obligaciones requeridas por la normativa de protección de datos; f) reportar directamente al Presidente del Consejo de Administración o al Consejero Delegado.

2. El Responsable de Instrucción es la figura encargada de gestionar la fase de instrucción/inspección de los hechos denunciados. En la mayoría de los supuestos, es el Director de Auditoría Interna o el *Compliance Officer*, pero puede ser otro responsable en virtud de la especialidad de la denuncia (caso de acoso laboral...).

Entre sus principales funciones se encuentran: a) designar al instructor concreto que ha de llevar a cabo la investigación de la concreta denuncia; b) marcar al Instructor prioridades y plazos de ejecución; c) aprobar el informe emitido con el resultado de la investigación de la denuncia; d) supervisar el cumplimiento de la implantación de las medidas de seguridad implantadas sobre las denuncias, para garantizar la confidencialidad y seguridad.

3. El Instructor será designado por el Responsable de Instrucción, generalmente, entre el personal de su Departamento o que se encuentren su bajo responsabilidad jerárquica o funcional. Sus funciones comprenden: a) investigar los hechos y recopilar las evidencias necesarias que permitan sustentar los resultados de la investigación; b) elaborar el Informe, bajo la supervisión del Responsable de la Instrucción; c) dar soporte al Comité de Denuncias en las funciones que se le encomienden; d) documentar y registrar en los sistemas establecidos al efecto, las denuncias recibidas; e) documentar y registrar en los sistemas establecidos al efecto, todas las acciones realizadas; f) cumplir con las exigencias de la normativa de protección de datos<sup>626</sup>.

#### 4.3 Ejemplos prácticos de sociedades cotizadas españolas

Empresas	Canal de denuncia interno	Comunicación	Denuncia	Destinatario
<b>Abertis</b>	Sí. Mención en el Código Ético	Formulario online (disponible en la intranet), correo postal, correo electrónico	Irregularidades de naturaleza financiera y contable. Incumplimiento del Código de Conducta. Irregularidades en la organización.	Comité de Auditoría.
<b>Acciona</b>	Sí. Mención en el Código Ético	Correo postal, correo electrónico (disponible en la intranet)	Conductas irregulares relacionadas con la contabilidad, el control, la auditoría o cualquier incumplimiento o vulneración de las conductas recogidas en el	Comisión del Código

<sup>626</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 621-622.

<b>Empresas</b>	<b>Canal de denuncia interno</b>	<b>Comunicación</b>	<b>Denuncia</b>	<b>Destinatario</b>
			Código Ético.	
<b>Sacyr</b>	Sí. Mención en el Código Ético. Línea de asesoramiento y denuncia.	Correo electrónico	Situaciones de incumplimiento o de riesgo de las conductas reguladas en el Código Ético.	Órgano de Cumplimiento del Código de Conducta
<b>Bankia</b>	Sí. Mención en el Código Ético. Canales de comunicación.	Accediendo a la plataforma. Canal confidencial denuncias o por vía telemática.	Cualquier incumplimiento del Código Ético	Gestión externa por la empresa PWC
<b>Gamesa</b>	Sí. Mención en el Código Ético.	Denuncia escrita dirigida al presidente del órgano de administración en el que se integre o superior jerárquico; correo electrónico	Actuaciones que falten a la ética, la integridad o atente contra los principios recogidos en el Código de Conducta	Unidad de cumplimiento normativo
<b>Indra</b>	Sí. Mención en el Código Ético. Canal Directo	Correo electrónico	Irregularidades que se detecten en relación con el cumplimiento del Código.	Unidad de cumplimiento normativo.
<b>Grifols</b>	Sí. Mención en el Código Ético. Ethics Point.	Vía telemática	Podrán ser anónimas. Irregularidades que se detecten en relación con la ejecución del Código de Conducta.	Gestión externa. Ethics Point
<b>Amadeus</b>				
<b>ACS</b>	Sí. Mención en el Código Ético. Canal Ético.	Correo electrónico o correo postal	Conductas irregulares de cualquiera de las empresas que forman parte del	Comité de Seguimiento del Código General de Conducta

<b>Empresas</b>	<b>Canal de denuncia interno</b>	<b>Comunicación</b>	<b>Denuncia</b>	<b>Destinatario</b>
			Grupo ACS o cualquier incumplimiento de las normas recogidas en el Código Ético	
<b>BME</b>	Sí. Mención en el Informe de Responsabilidad Social Corporativa	Vía telemática (intranet). Comunicación de forma anónima	Cualquier irregularidad en los sistemas internos de control y gestión de riesgos.	Comisión de Auditoría
<b>Mapfre</b>	Sí. Mención en el Código Ético. Cumplimiento del Código Ético y de Conducta	Correo electrónico y/o correo postal	Incumplimiento o vulneración de cualquiera de los principios y normas éticas o de conducta establecidas en el Código.	Comité de Ética.
<b>REE</b>	Sí. Mención en el Código Ético. Sistema para la detección y tratamiento de los posibles incumplimientos, denuncias, consultas y sugerencias	Vía electrónica en la web de cada empresa y Servicio de Atención Dígame	Presuntos incumplimientos por faltas éticas, mercantiles, financieros, contables, etc., que se detecten del Código Ético por una de las empresas del Grupo o de sus empleados	Gestor Ético (actuación de forma independiente) y defensor de los grupos de interés, con la colaboración del presidente del Grupo REE y de los presidentes de las Comisiones de Auditoría y de Gobierno y Responsabilidad Corporativa
<b>Inditex</b>	Sí. Mención en el Código Ético. Cumplimiento del Código y	Correo postal, correo electrónico o fax	El Comité de Ética podrá actuar por propia iniciativa o a	Comité de Ética: Secretario General y Director de

<b>Empresas</b>	<b>Canal de denuncia interno</b>	<b>Comunicación</b>	<b>Denuncia</b>	<b>Destinatario</b>
	Comité de Ética		instancia de cualquier empleado de Inditex, fabricante, proveedor o de un tercero del incumplimiento o vulneración de los principios o normas éticas que se encuentren recogidas en el Código de Conducta	Cumplimiento Normativo, director de Auditoría Interna, Director de Responsabilidad Social Corporativa, Director de RR.HH
<b>OHL</b>	Sí. Mención en el Código Ético. Canal Ético de Comunicación	Vía web o vía correo postal	Descubrir posibles irregularidades ante los principios y normas del Código Ético de Conducta	Comisión de Auditoría, Cumplimiento y Responsabilidad Social Corporativa
<b>Iberia</b>	Sí. Mención en el Código Ético de Conducta. Incumplimientos	Web corporativa, intranet o vía telefónica	Conductas irregulares en cualquiera de las empresas que forman parte del Grupo Iberia o cualquier incumplimiento de las normas recogidas en el presente Código	Unidad de Cumplimiento en la Dirección de Riesgos y Seguridad
<b>Técnicas Reunidas</b>	Sí. Mención en el Informe de la Memoria Anual. Código Ético. Buzón del Código	Web corporativa (intranet)	Indicios razonables de algún incumplimiento de la normativa interna o externa	Comité de Respuesta

<b>Empresas</b>	<b>Canal de denuncia interno</b>	<b>Comunicación</b>	<b>Denuncia</b>	<b>Destinatario</b>
			de la compañía	
<b>Arcelormittal</b>	Sí. Mención en el Reporte de Sustentabilidad. Política sobre Denuncias de situaciones ilegales dentro de la empresa	Web corporativo	Situación ilegal dentro de la empresa, relacionadas con la contabilidad, auditoría o en cuestiones bancarias o sobornos que tenga lugar dentro de la compañía y sus filiales	Unidad de Cumplimiento Normativo
<b>Jazztel</b>				
<b>Mediaset</b>	Sí. Mención en el Informe de Responsabilidad Social Corporativa.	Página Web (Intranet)	Irregularidad, fraude o corrupción, así como cualquier incumplimiento al Código	Consejeros Independientes, quienes deben elevar el caso a la Comisión de Auditoría y Cumplimiento
<b>Repsol</b>	Sí. Mención en el Código Ético. Canales de comunicación con la Comisión de Ética	Correo postal o vía telemática. Comunicación confidencial o anónima	Temas o incidencias de contabilidad y controles internos o auditorías que afecten a Repsol	Comisión de Auditoría y Control del Consejo de Administración Dirección de Auditoría Corporativa. Unidad de seguridad corporativa. Repsol te escucha
<b>Iberdrola</b>	Sí. Mención en el Código Ético. Buzón Ético	Vía telemática que estará disponible en el apartado denominado Buzón ético del Portal del	Conductas que puedan implicar la comisión de alguna irregularidad o de	Unidad de cumplimiento normativo

<b>Empresas</b>	<b>Canal de denuncia interno</b>	<b>Comunicación</b>	<b>Denuncia</b>	<b>Destinatario</b>
		empleado	algún acto contrario a la legalidad o a las normas de actuación del Código Ético	
<b>Enagás</b>	Sí. Mención en el Código Ético. Canal Ético	Correo electrónico	Comunicación de irregularidades o incumplimiento del Código	Comité de Supervisión de los Principios de Actuación
<b>Día</b>	Sí. Mención en el Código Ético. Comité ético.	Correo electrónico, correo postal	Comunicación de posibles irregularidades o incumplimientos del Código	Comité Ética Grupo y director de Cumplimiento Normativo
<b>Gas natural</b>	Sí. Mención en el Código Ético. Aceptación y cumplimiento del Código		Incumplimiento o mala práctica que pudieran observar en el desempeño de sus actividades profesionales	Superior jerárquico o a la Comisión del Código Ético
<b>Ebro foods</b>	Sí. Mención en el Código Ético. Protocolo de actuación de denuncias internas	Correo electrónico	Incumplimiento de los principios recogidos en el presente Código.	Presidente de la Comisión de Auditoría y Control
<b>Bankinter</b>	Sí. Mención en el Código Ético. Procedimiento de sanción de infracciones del Código de Ética Profesional		Infidelidad o fraude de los empleados, como los que traigan causa de su dolo o negligencia profesional constitutiva de una infracción del Código de Ética Profesional, del Reglamento	Comité de Seguimiento del Código de Ética Profesional

<b>Empresas</b>	<b>Canal de denuncia interno</b>	<b>Comunicación</b>	<b>Denuncia</b>	<b>Destinatario</b>
			Interno de Conducta del Mercado de Valores o de otras normas internas del Banco en el ámbito de la ética profesional y del cumplimiento normativo	
<b>Santander</b>	Sí. Mención en el Código Ético. Canal de denuncia	Vía telefónica, correo electrónico, correo postal	Comisión de un acto presuntamente ilícito o de un acto de incumplimiento del Código General o de los códigos y manuales sectoriales	Dirección de Cumplimiento
<b>Ferrovial</b>	Sí. Mención en la Web Corporativa. Buzón de denuncias	Vía telemática (Intranet). Anónima o Nominativa	Irregularidades, incumplimientos y comportamientos contrarios a la ética y la legalidad	Comité Gestor
<b>Sabadell</b>	Mención en el Código Ético.	Correo electrónico	Inquietud sobre el cumplimiento ético en su ámbito de trabajo	Comité de Ética Corporativa
<b>Telefónica</b>	Sí. Mención en el Código Ético	Vía telemática (Intranet)	Incumplimiento de los principios de actuación	
<b>Popular</b>	Sí. Mención en la página web corporativa. Línea Ética	Vía telemática	Mala conducta o fraude que se desarrolle en el interior del banco.	
<b>Viscofan</b>	Sí. Mención en		Incumplimiento o	Oficina Ética



<b>Empresas</b>	<b>Canal de denuncia interno</b>	<b>Comunicación</b>	<b>Denuncia</b>	<b>Destinatario</b>
	el Código Ético. Obligatoriedad y resolución de conflictos		vulneración, con respecto a las normas contenidas en este Código de Conducta	
<b>BBVA</b>	Sí. Mención en el Código Ético. Integridad Personal. Actitud Responsable	Correo electrónico o vía telefónica	Incumplimiento de la legalidad vigente	Superior jerárquico, directivos de los departamentos de Asuntos Legales o Recursos Humanos con responsabilidad directa. Departamentos de cumplimiento Normativo. Dirección Corporativa de Cumplimiento
<b>CaixaBank</b>	Sí. Mención en el Informe Corporativo. Canal de denuncias		Incumplimiento del Código Ético o vulneración de cualquier norma a la cual se adhiera la compañía	Canal de atención de CaixaBank
<b>FCC</b>	Sí. Mención en el Código Ético. Aceptación y cumplimiento	Vía postal o vía telemática (Intranet)	Incumplimiento o vulneración que pudieran, eventualmente observar	Comité de Seguimiento del Reglamento Interno de Conducta

## **5. Procedimiento**

### **5.1 Consideraciones generales**

Es imprescindible que exista en la entidad un procedimiento documentado por escrito en el que se regulen todos los extremos propios del canal de denuncias. Este procedimiento debe ser aprobado formalmente por la Alta Dirección y ser de obligado cumplimiento. Un documento en el que se regule todo el trámite de una denuncia: desde la comunicación inicial del comportamiento irregular hasta su resolución o archivo.

El procedimiento debe ser divulgado de manera eficaz en lo que se refiere a su existencia y a sus características. Es recomendable que se incluya en la Intranet de la entidad, en la página Web que la entidad tiene disponible para el público en general (si el ámbito es abierto), en los contratos de los empleados, en los contratos con clientes y proveedores y, en general, a través de cualquier medio que permita la circulación de esta información en la entidad (campañas de difusión y de concienciación, circulares, etc.)<sup>627</sup>.

Es preciso que se detallen o se haga referencia expresa al documento en el que se pueden encontrar las acciones que pueden ser objeto de denuncia, no siendo suficiente una descripción genérica. Es necesario que se establezca y se garantice al denunciante que no tendrá represalias por parte de la entidad. Es importante advertir que tanto en el caso de contravenir lo previsto en el procedimiento como en el caso de realizar denuncias falsas será de aplicación el régimen disciplinario existente en la entidad. Con independencia del estándar que se elija, es esencial que los empleados conozcan las consecuencias derivadas de la presentación de denuncias falsas, a sabiendas que lo son. Las denuncias de mala fe deben ser objeto de sanción disciplinaria en la empresa y así ha de constar en el reglamento interno de whistleblowing y en cualquier documento o publicidad relativa al canal. Además, en esa publicidad es recomendable incluir información sobre otro

---

<sup>627</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 627.

tipo de responsabilidades que puedan derivarse de un mal uso de la hotline como la posible responsabilidad civil por la lesión del derecho al honor o la comisión de un delito de injurias o de calumnias. Este tipo de advertencias evitará un uso abusivo o malintencionado del canal de denuncias<sup>628</sup>.

Es importante que el procedimiento se encuentre documentado por escrito, con una terminología clara y entendible por todo el personal que pueda hacer uso del sistema de denuncias (personal propio o terceros vinculados de una u otra forma a la entidad)<sup>629</sup>.

## **5.2 Procedimiento de denuncia e investigación interna**

Debido al carácter confidencial de la denuncia interna, ésta debe contener:

- 1) el nombre de la empresa a la que se refiere;
- 2) los datos identificativos del denunciante –nombre, apellidos y número de DNI, Número de Identificación de Extranjeros o Número de Pasaporte y nacionalidad–; y
- 3) los hechos denunciados, concretando, en la medida de lo posible, la infracción presuntamente cometida<sup>630</sup>.

Sólo se podrán formular denuncias en las lenguas en las que la empresa tenga negocios, presenciales, por vía telefónica o por escrito, bien mediante la cumplimentación del formulario on-line habilitado al efecto o bien por correo postal, preferiblemente certificado y con acuse de recibo, dirigido a la dirección de la Consultora externa o despacho jurídico o del Oficial de Cumplimiento Normativo de la entidad.

No se podrán formular denuncias internas por ningún otro cauce distinto de los establecidos en la norma.

---

<sup>628</sup>GARCIA MORENO, B., "Whistleblowing...", ob. cit., p. 224.

<sup>629</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 627.

<sup>630</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1243.

Toda persona que formule una denuncia debe tener indicios racionales que sustenten la misma, por lo que la denuncia debe servir acompañada de las pruebas que acrediten los hechos, al menos indiciariamente. Será válido cualquier material probatorio permitido en Derecho, preferiblemente en soporte documental, aunque también son admisibles pruebas testificales – incluido el testimonio del propio denunciante– e instrumentos de reproducción de palabras, imágenes y sonidos. Cualquier prueba debe haber sido obtenida por el denunciante de forma lícita, es decir, con respeto a la ley y los derechos y las garantías constitucionales.

Las denuncias sólo serán admitidas a trámite en el supuesto de que cumplan con lo establecido en la correspondiente regulación.

La persona o las personas denunciadas tienen derecho a conocer que han sido objeto de denuncia y deben recibir notificación de la existencia de ésta y de un resumen de los hechos denunciados con la mayor brevedad y, en todo caso, dentro de un plazo máximo de tres (3) meses a contar desde que se recibió la denuncia. Esta notificación dirigida a la persona o personas denunciadas no incluirá los datos del denunciante<sup>631</sup>.

Una vez recibida una denuncia, la reacción de la empresa debe ser proceder a confirmar la veracidad de la información. La empresa tiene la opción de poner inmediatamente los hechos en conocimiento de las autoridades para que sean éstas las que procedan a su investigación. No puede defenderse la existencia de un deber de denuncia inmediata por parte de la compañía sin proceder antes a una comprobación mínima de la veracidad de la información recibida. El hecho de trasladar sin más a las autoridades la información conlleva el riesgo de perjuicios en la reputación de la propia empresa y de los trabajadores denunciados. Es conveniente verificar la realidad de la denuncia antes de remitirla a la policía, la fiscalía o el juzgado. Atendiendo al artículo 31 bis 4 CP, hay que entender que la eficacia del procedimiento establecido

---

<sup>631</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., pp. 1245-1246.

por una persona jurídica para el descubrimiento y la prevención del delito no puede verse cuestionada por el hecho de haber previsto un procedimiento interno de investigación como primera respuesta.

En términos de efectividad una investigación interna previa de los hechos puede ser más ágil y aportar resultados más esclarecedores y por tanto más efectiva que si se espera a la actuación de funcionarios públicos. La denuncia inmediata a las autoridades es exigible en los supuestos en los que estén en riesgo importantes intereses de terceros, o cuando sea imprescindible y urgente la práctica de diligencias restrictivas de derechos fundamentales (una entrada y registro para evitar la pérdida de instrumentos, efectos o ganancias del delito) o la adopción de medidas cautelares (para evitar la destrucción de pruebas de gran importancia)<sup>632</sup>.

La investigación interna variará en función de cada caso, por ello una regulación exhaustiva de todos sus pormenores en la regulación del procedimiento de denuncia no es exigible<sup>633</sup>. Es importante distinguir el procedimiento stricto sensu de la información sobre dicho procedimiento que se da a los potenciales usuarios, a través de páginas web o de canales internos como pueden ser intranets, cursos de formación etc. Es importante informar al potencial denunciante de aquellos datos que pueden incentivar la denuncia (confidencialidad, protección frente a represalias, etc.). Nada obsta para la efectividad el que determinados aspectos del procedimiento (como lo relativo a las investigaciones internas) tengan carácter reservado, sin perjuicio de informar al trabajador denunciado cuando sus derechos los exijan.

En caso de que se hubiera incurrido en un defecto subsanable al formular la denuncia, se le puede conceder al denunciante un plazo razonable (diez días hábiles) para que subsane el defecto, advirtiéndole en este caso de que se

---

<sup>632</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. p. 189.

<sup>633</sup>Advierte GOÑI SEIN, J.L, cómo en la mayoría de "líneas éticas" accesibles al público la información que se da a los usuarios sobre las reacciones de la empresa una vez recibida la información es más bien escasa, lo que se explica a su juicio por la voluntad de generar un clima favorable a la denuncia. "Sistemas de denuncia...", ob. cit., p. 327.

puede proceder al archivo de la denuncia si el defecto no es subsanado en plazo.

Si la denuncia no cumpliera con lo establecido en la regulación, por el motivo que fuera, o no se hubieran subsanado los defectos en plazo se ha de proceder a su archivo.

Si la denuncia es admitida a trámite, el Oficial de Cumplimiento Normativo procederá a la apertura de un expediente en el que podrán llevarse a cabo cuantas actuaciones resulten oportunas y practicarse las pruebas que se estimen necesarias para el debido esclarecimiento y determinación de los hechos. El plazo para la tramitación del expediente no debe exceder de un plazo razonable (por ejemplo dos meses) a contar desde la fecha de su apertura<sup>634</sup>.

Si para efectuar la investigación se necesitan conocimientos especializados o la intervención de expertos<sup>635</sup>, la entidad debe facilitar al investigador los medios materiales y personales necesarios, ya sean internos o externos.

Todas las actuaciones deben documentarse debidamente y que en su caso se dé fe del contenido de las diligencias por más de un sujeto. La designación de un instructor y un secretario es recomendable. El objetivo del procedimiento es verificar la información recibida y hacer acopio de pruebas que en su caso, sirvan para la acreditación del posible delito ante un tribunal.

En la investigación debe respetarse la confidencialidad, que se ha garantizado al denunciante.

El procedimiento debe prever la audiencia del denunciado. El momento de la misma variará en función de las necesidades de cada investigación. En algunos supuestos será oportuno no llevarlo a cabo hasta que la investigación

---

<sup>634</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1244.

<sup>635</sup>Para detectar, por ejemplo, la presencia de productos contaminantes en los alimentos que produce una empresa o en los residuos que genera.

haya avanzado; en otros puede ser la primer actuación, como ocurrirá en los casos en que el denunciante haya aportado inicialmente pruebas significativas.

El procedimiento ha de respetar los derechos fundamentales de las personas investigadas. Su vulneración puede comportar la posterioridad nulidad procesal de las pruebas obtenidas. Es fundamental el respeto a las limitaciones impuestas por el Derecho laboral a tales actuaciones indagatorias<sup>636</sup>.

El Gabinete Jurídico de la AEPD recomendó comunicar al trabajador o directivo denunciado la existencia de la denuncia en un plazo máximo de tres meses desde el momento de registro de los datos<sup>637</sup>. El documento WP117 recomienda que la comunicación al denunciado se produzca tan pronto como se reciba la denuncia, si bien admite que esa comunicación se demore, sin fijar un plazo máximo, en aquellos casos en los que "exista un riesgo importante de que dicha notificación pondría en peligro la capacidad de la sociedad para investigar de manera eficaz la alegación o recopilar las pruebas necesarias"<sup>638</sup>.

La tramitación del expediente concluirá con un informe del Oficial de Cumplimiento Normativo en el que dará cuenta de las actuaciones llevadas a cabo, de la prueba practicada y de los hechos que puedan considerarse acreditados, dejando constancia de las recomendaciones que crea oportuno realizar<sup>639</sup>.

Si al finalizar la investigación queda constatada la existencia de indicios de un delito, ello debe quedar recogido en un informe final, que ha de ponerse a disposición de los órganos correspondientes de la empresa que sean competentes para: a) adoptar decisiones en el ámbito laboral (sanciones,

---

<sup>636</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 189-190.

<sup>637</sup>Informe 2007/0128 apartado VII.

<sup>638</sup>Citado en apartado VII del Informe 2007/0128.

<sup>639</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., p. 1244.

incluyendo el posible despido, por lo general el departamento de recursos humanos); b) denunciar los hechos a las autoridades administrativas o judiciales; c) adoptar medidas reparatoras para los que hayan sido perjudicados y, d) establecer medidas correctoras para prevenir de forma más eficaz que los hechos no se produzcan en el futuro.

La empresa debe adoptar las medidas necesarias para que quede constancia de las investigaciones internas llevadas a cabo y su resultado, pues es el medio de demostrar ante un tribunal que un procedimiento de denuncia es efectivo, acreditando la existencia de investigaciones previas y sus resultados<sup>640</sup>.

El informe del Oficial de Cumplimiento Normativo será elevado al Presidente del Comité de Auditoría, si fuera cotizada, o en su caso, al Director de la Asesoría Jurídica de la empresa, que dará traslado del mismo al Presidente y/o al Consejero delegado, con el fin de que cualquiera de ellos, indistintamente, pueda adoptar las medidas de investigación a través del Grupo de Respuesta ante el Fraude y legales que consideren oportunas.

Las alegaciones, denuncias o incidentes podrían llegar a implicar a distintos departamentos de la empresa (*Compliance*, Legal, Recursos Humanos, Riesgos, etc.). Por ello, es importante que la entidad establezca un plan de respuesta ante el fraude y que las investigaciones ante la recepción de una denuncia por la comisión de un hecho delictivo las lleve a cabo la persona especialista en la materia investigada, estando todos los departamentos coordinados entre sí, a través del Oficial de Cumplimiento Normativo quien, previa comunicación al Grupo de Respuesta ante el Fraude (GRF), remitirá la denuncia al Equipo de Investigación (EI) para que realice la investigación oportuna, enviando una vez finalizada la investigación un informe al GRF.

---

<sup>640</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 190-191.



El GRF está compuesto por los siguientes directores: Oficial de Cumplimiento Normativo, Director de Auditoría Interna, Director de la Asesoría Jurídica, y Director de Recursos Humanos.

El equipo de investigación (EI) ante hechos graves o muy graves deberá gestionar la correspondiente investigación. El EI será nombrado por el GRF y, dependiendo de la materia objeto de investigación, estará compuesto por personal interno de la empresa o por personal externo (consultora, despacho de abogados, etc.). La investigación interna debe mantenerse de manera confidencial y debe trascender lo menos posible. El EI podrá utilizar todos los medios posibles humanos y materiales que precise y debe involucrar a la persona o personas que entienda necesario para la averiguación de los hechos y del responsable o responsables de la comisión de los mismos<sup>641</sup>.

Una vez concluida la investigación, el EI remitirá el informe al GRF, quien decidirá si actuar o no actuar, establecer medidas disciplinarias, de despido o ejercitar acciones penales y/o civiles.

La decisión adoptada por el GRF, respecto a la denuncia e informe recibido del EI, si la ley así lo exigiera, deberá ser comunicada al representante de los trabajadores.

El expediente completo deberá ser custodiado por el director de Recursos Humanos o por la persona que éste designe.

En el fenómeno del *Criminal Compliance* no se puede hablar de una privatización del control de la criminalidad sin hacer referencia a la privatización del proceso penal<sup>642</sup>.

---

<sup>641</sup>MESIA MARTÍNEZ, C., "El procedimiento...", ob. cit., pp. 1244-1245.

<sup>642</sup>SIEBER, U. "Programas de *compliance* en el Derecho penal de la empresa. Una nueva concepción para controlar la criminalidad de empresa" (trad. Abanto/ Vásquez), en Urquiza Olaechea/ Abanto Vásquez/ Salazar Sánchez (coords.), *Dogmática penal de derecho penal económico y política criminal Homenaje a Klaus Tiedemann*, Fondo Editorial, Lima, 2011, p. 206; KNAUER, "Interne Ermittlungen (Teil I)-Grundlagen", en *ZWH*, n° 2, 2012, p. 41. Parte de la doctrina entiende que, como consecuencia de esta privatización, las actuaciones del empresario en las

Las prácticas que las empresas implementan para investigar y eventualmente sancionar las ilicitudes van adquiriendo un papel de mayor relevancia, a la vez que se tiende a exigir mayores requisitos en la autorregulación e implementación de los sistemas de control idóneos y en la prevención de las irregularidades<sup>643</sup>. En este sentido, se puede constatar la existencia de un segundo sistema de regulación, paralelo al estatal, que impone a las empresas la obligación de prevenir, descubrir y sancionar las infracciones de la ley<sup>644</sup>

Una vez que se ha tomado la decisión de investigar la supuesta comisión de los delitos en el seno de la empresa, corresponde a los abogados de la misma o, incluso, a abogados externos, recopilar todas las posibles pruebas que lo evidencien para ponerlas a disposición de la junta directiva, que deberá adoptar en el seno de la empresa una decisión vinculante. Esto pone de manifiesto la equivalencia que se produce entre la privatización del proceso penal y la investigación interna y, que se hace especialmente patente cuando se analizan los fines preventivos y de obtención de la verdad que se persiguen con las *internal investigations*, en sintonía con los fines del proceso penal<sup>645</sup>. Es casi imposible no comparar, en este sentido, dichas actividades empresariales con las de un fiscal o un juez<sup>646</sup>.

No obstante, y pese a esta equivalencia, no debe olvidarse que las investigaciones empresariales presentan una naturaleza claramente divergente por su carácter privado. Es la misma *empresa* la que decide el

---

investigaciones internas podrían imputársele al Estado. Al respecto, KNIERIM, "Erfordernisse und Grenzen der Internal Investigations", en Rotsch (ed.), *Wissenschaftliche und praktische Aspekte der nationalen und internationalen Compliance-Diskussion*, p. 85. Contrario a esta opinión, JAHN, "Ermittlungen in Sachen Siemens/ SEC", en *StV*; n° 1, 2009, p. 45.

<sup>643</sup>KNAUER, C. "Interne...", ob. cit., p. 42.

<sup>644</sup>REEB, P. *Internal Investigations. Neue Tendenzen privater Ermittlungen*, Duncker & Humblot, Berlin, 2011, pp. 1 y s. MONTIEL, J. P., "Sentido y alcance de la investigaciones internas en la empresa", en AA.VV., *Responsabilidad de la empresa y compliance. Programas de prevención, detección y reacción penal*, dirs. S. Mir, M. Corcoy y V. Gomez, Buenos Aires, 2014, pp. 487 y 488.

<sup>645</sup>KINDHÄUSER, U., *Strafprozessrecht*, Nomos, Baden-Baden, 2006 (2ª ed.), § 1, n° 9; VOLK, *Grundkurs StPO*, 7ª ed., § 3, nm. 1, C. H. Beck, München, 2010.

<sup>646</sup>MONTIEL, J. P., "Sentido y alcance...", ob. cit., p. 488.

inicio y la finalización de las investigaciones y la que adopta la decisión de fondo. Esto último se contrapone a los supuestos de colaboración entre los particulares y el Estado (como en el caso de informes proporcionados por las empresas a las autoridades estatales en el marco de una investigación judicial), en los que le corresponde al Estado asumir el dominio del proceso de *detectiori* y *reaction*. Como consecuencia de lo anterior, puede reconocerse que una primera característica de las investigaciones internas es que es un particular el detenta el "señorío" de la investigación<sup>647</sup> y decide de forma autónoma y exclusiva, teniendo en cuenta los intereses de la empresa para investigar o colaborar con la justicia. También se puede poner en relación con el hecho de que las sanciones adoptadas por la empresa en ningún caso representan una pena, dada la falta de carácter público y de contenido estigmatizante. Es más, tanto las sanciones (rescisión contractual, reparación del daño, etc.)<sup>648</sup> como las restantes consecuencias (programas de amnistía)<sup>649</sup> que se puedan derivar a los responsables de los ilícitos, son cuestiones que quedan en el ámbito del Derecho laboral y del Derecho civil<sup>650</sup>.

Las investigaciones empresariales pueden repercutir positivamente tanto en el Estado como en la empresa. Así, en el caso del Estado, las *internal investigations* le permiten esclarecer las conductas sospechosas e introducirse en la estructura empresarial de forma más eficiente que mediante

---

<sup>647</sup> Sobre el "principio del dominio" como elemento delimitador entre investigaciones privadas e investigaciones estatales mediante actores privados, cfr. en detalle REEB, *Internal Investigations...*, ob. cit., pp. 8 y ss.

<sup>648</sup> En relación a estas concretas sanciones, cfr. MASCHMANN, F. "Vermeidung von Korruptionsrisiken aus Unternehmenssicht -Arbeits- und Zivilrecht, Corporate Governance-", en Benz/Dieners/Dölling *et. al.* (eds.), *Handbuch der Korruptionsprävention*, C. H. Beck, München, 2007, nm. 154 y ss. Desde una perspectiva general, WAUSCHKUH, "Sanktionierung nach Abschluss der Untersuchungen", en Moosmayer/Hartwig (eds.), *Interne Untersuchungen. Praxisleitfaden für Unternehmen*, Beck, München, 2012, pp. 67 y ss.

<sup>649</sup> WEISSE, "Ausgewählte arbeitsrechtliche Aspekte und Amnistie", en Moosmayer/ Hartwig (eds.), *Interne Untersuchungen. Praxisleitfaden für Unternehmen*, C. H. Beck, Munich, 2012, pp. 58 y ss.; POTINECKE/ BLOCK, "Gesellschaftliche Rahmenbedingungen und Beratung der Unternehmensführung", en Knierim/Rübenstahl/Tsambikakis (eds.), *Internal Investigations. Ermittlungen im Unternehmen*, C. F. Müller, Heidelberg *et. al.*, 2013, nm. 168 y ss.

<sup>650</sup> MONTIEL, J. P., "Sentido y alcance...", ob. cit., pp. 488-489.

la puesta en marcha de todo el aparato burocrático<sup>651</sup>. No olvidemos que la finalidad última de las investigaciones internas es la de conocer la naturaleza y la extensión de las conductas incorrectas cometidas en el seno de un colectivo<sup>652</sup>. En el caso de las empresas, encuentran fuertes incentivos para realizar este tipo de investigaciones<sup>653</sup>, puesto que el saneamiento de una empresa contribuye a mejorar su imagen en el mercado<sup>654</sup>, y puede ser un factor relevante para justificar la exclusión<sup>655</sup> o la atenuación<sup>656</sup> de la responsabilidad penal. Un ejemplo de ello es el caso *Siemens* por el que, pese a los elevados costes que supuso la investigación interna, les compensó por la rebaja de la sanción pecuniaria<sup>657</sup>.

Todo ello puede explicar la amplia expansión de este fenómeno en los últimos años, tanto en el ámbito académico como en el práctico. En particular, en el ámbito práctico se evidencia cómo estas investigaciones ya dejan de ser un mecanismo propio de las grandes empresas y se extiende también a las empresas medianas. En Alemania, las empresas medianas (o hasta incluso pequeñas de hasta 100 miembros) comienzan a someterse a procesos de auto limpieza<sup>658</sup>.

---

<sup>651</sup>McKENDALL/DEMARR/JONES-RIKKERS, "Ethical Compliance Programs and Corporate Illegality: Testing the Assumptions of the Corporate Sentencing Guidelines", en *Journal of Business Ethics*, n° 37, 2002, p. 369.

<sup>652</sup>PROPPER, E. *Corporate Fraud Investigations and Compliance Programs*, Oceana Publications, New York, 2000, pp. 52 y s.

<sup>653</sup>MOMSEN, C. "Internal Investigations zwischen Mitwirkungspflicht und strafprozessuale Selbstbelastungsfreiheit", en *ZIS*, n° 6, 2011, p. 510.

<sup>654</sup>NESTLER, N., "Internal Investigations: Definition und rechtstatsächliche Erkenntnisse zu internen Ermittlung in Unternehmen", en AA.VV., *Internal Investigations. Ermittlungen im Unternehmen*, coords. Knierim/ Rügenstahl/ Tsambikakis, edit. C. F. Müller, Heidelberg, 2013, p. 29.

<sup>655</sup>Como mostraré más adelante, ello puede ocurrir cuando la investigación empresarial permite mostrar que el delito no es consecuencia de un defecto de organización. Con todo, el traslado de esta última posibilidad al Derecho penal español parece algo discutible, atendiendo a la redacción del art. 31 bis CP.

<sup>656</sup>Cfr. entre otros, JAHN, M. "Ermittlungen...", ob. cit., p. 41.

<sup>657</sup>Gracias a la colaboración prestada por Siemens AC a las autoridades y a la realización de investigaciones internas, una multa inicial que se calculaba en varios miles de millones de euros logró acordarse en alrededor de mil millones de euros (€ 395.000.000 acordados con la Fiscalía de Múnich y € 600.000.000 con la *Securities and Exchange Commission* [SEC] y el Departamento de Justicia estadounidense).

<sup>658</sup>MONTIEL, J. P., "Sentido y alcance...", ob. cit., pp. 490-491.

No cabe duda de que las investigaciones internas son un fenómeno en expansión en el terreno del Derecho penal empresarial. Ello se desprende de la amplia literatura alemana aparecida en los últimos cinco años<sup>659</sup>. Los escándalos WordCom, Parmalat, Enron, Merck & Company, Riggs Bank y Siemens AG, entre otros, contribuyeron de forma decisiva a que los gobiernos de los Estados Unidos y de algunos miembros de la Unión Europea adoptaran medidas que han sido determinantes del auge de las *internal investigations* así como del *Criminal Compliance*. Según el estudio realizado por Michels en el año 2010, prácticamente la mitad de las sociedades de capital de los Estados Unidos ya realizaban investigaciones internas en el año 2008<sup>660</sup>. Así pues, las *internal investigations* no suponen ninguna novedad en EE.UU, al contrario de lo que sucede en la estructura jurídica continental.

Las investigaciones internas no sólo han servido para identificar a los responsables de las infracciones cometidas dentro de la empresa, sino que también han sido un instrumento que ha permitido ofrecer explicaciones al Estado y a la sociedad en general sobre negaciones cuestionables, acreditar el cumplimiento de requerimientos legales en materias vinculadas a la salud o al medio ambiente, influir en la estrategia empresarial, etc.<sup>661</sup>.

Es necesario delimitar conceptualmente las investigaciones internas para poder distinguirlas de otras medidas empresariales que presentan una

---

<sup>659</sup> Además de los innumerables artículos de revista, en el último año y medio han aparecido voluminosos libros colectivos y monografías, cfr. KNIERIM/ RÜBENSTAHL/TSAMBIKAKIS (eds.), *Internal Investigations. Ermittlungen im Unternehmen*, C. F. Müller, Heidelberg et. al., 2013, *passim*; MOOSMAYER/HARTWIG (eds.), *Interne Untersuchungen. Praxisleitfaden für Unternehmen*, C. H. Beck, München, 2012, *passim*; WEWERKA, *Internal Investigations. Private Ermittlungen im Spannungsfeld von strafprozessualen Grundsätzen und Anforderungen eines globalisierten Wirtschaftsstrafverfahrens; eine Problemanalyse unter besonderer Berücksichtigung des Falles Siemens*, Peter Lang Verlag, Frankfurt a.M. et. al., 2012, *passim*; SPEHL/GRÜTZNER, *Corporate Internal Investigations*, C.H. BECK, MÜNCHEN, 2012, *passim*; RÖDIGER, K. *Strafverfolgung von Unternehmen, Internal Investigations und strafrechtliche Verwertbarkeit von "Mitarbeitergeständnissen"*, Peter Lang Verlag, Frankfurt a.M. et. al., 2012, *passim*; REEB, P., *Internal Investigations...*, cit., *passim*.

<sup>660</sup> MICHELS, K. "Internal Corporate Investigations and the Truth", en *Seton Hall Law Review*, n° 40, 2010, pp. 84 y ss.

<sup>661</sup> HEMPHILL, T. /CULLARI, F. "Corporate Governance Practices: A Proposed Policy Incentive Regime to Facilitate Internal Investigations and Self-Reporting of Criminal Activities", en *Journal of Business Ethics*, n° 87, 2009, p. 334.

estructura análoga, con distinta finalidad. Cuando una empresa "investiga", debe tenerse en cuenta tanto como cuando toma declaraciones a sus trabajadores, cuando recurre a investigadores privados para averiguar un presunto hecho de corrupción, como cuando los propios auditores de la empresa revisan los documentos contables en su actividad. Desde una perspectiva clásica del control de la criminalidad empresarial, las investigaciones internas desempeñan un papel importante. La palabra "control", en términos generales, permite entender como medidas de control, las averiguaciones realizadas por los investigadores privados. Sin embargo, es necesario distinguir, en términos estrictos, las *actividades de control* de las de *investigación empresarial*, sin perjuicio de los muchos puntos en común que pueden existir, para poder entender el espectro de las investigaciones internas<sup>662</sup>. En ese sentido, supone especialmente un "control" (sin perjuicio de un mínimo componente "investigativo") la actividad cotidiana de los auditores en una empresa, puesto que se encargan de revisar, examinar y evaluar los resultados de un determinado sector de gestión<sup>663</sup>. De ahí la existencia de auditores de distintos sectores como de gestión contable, medioambiental, etc. Ahora bien, frente a dicho "control empresarial" aparece la "investigación empresarial", que se configura como principalmente *reactiva*<sup>664</sup>. Es decir, se "enciende" esa competencia cuando existe la sospecha de que se ha cometido un ilícito o bien cuando la comisión del

---

<sup>662</sup> MONTIEL, J. P., "Sentido y alcance...", ob. cit., pp. 491-495.

<sup>663</sup> Sobre la noción de "control" en este terreno del *Corporate Governance* ver, entre otros, DE CLEYN, "Compliance of Companies with Corporate Governance Codes: Case Study and Listed Belgian SMEs", en *Journal of Business Systems, Governance and Ethics*, n° 1, 2008, pp. 2 y ss.

<sup>664</sup> SAHAN, S., "Unternehmensinterne Untersuchungen aus rechtsanwaltlicher Perspektive", en AA.VV., *Compliance und Strafrecht*, coords. Kühlen/Kudlich/Ortiz de Urbina, edit. C. F. Müller, Heidelberg, 2012, p. 171 existe edición en español a cargo de KÜHLEN, L./ MONTIEL, J.P., /ORTIZ DE URBINA GIMENO, I., *Compliance y teoría del Derecho penal*, Marcial Pons, Barcelona, 2013; NESTLER, N., "Internal...", ob. cit., p. 21; BÜHRER, R. "EinrichtungeinerinternenUntersuchungsabteilung und deren Prozesse", en Moosmayer/Hartwig (eds.), *Inteme Untersuchungen. Praxisleitfaden für Untemehmen*, C. H. Beck, Munich, 2012, p. 101; REEB, P. *Internal Investigations...*, cit., p. 20. En cambio, entiende PROPPER, E. *Corporate...*, ob. cit., p. 53, que solamente tendrán una naturaleza *reactiva* aquellas investigaciones que se inician con motivo de una citación judicial de las autoridades estatales.

delito es bastante evidente y ya existe un proceso judicial en marcha<sup>665</sup>. Por tanto, el concepto de las investigaciones internas comprende, de la misma forma que ocurre en el proceso penal, aquellas actividades destinadas a (intentar) "reconstruir el pasado" y a adoptar medidas a partir de los hechos acreditados, sin limitarse a meras actividades que supongan un control genérico<sup>666</sup>.

Pues bien, en el ámbito de la gestión empresarial, de cara a diseñar su estructura interna y planificar los gastos de gestión, cabe preguntarse por la existencia de un deber de realizar una investigación. Especialmente relevante es, a la hora de encontrar una posible justificación de aquellas conductas empresariales que, en el marco de estas investigaciones lesionan bienes tipificados jurídicamente, determinar si existe o no semejante deber desde un punto de vista jurídico y, en su caso, explicar dónde debe encuadrarse este deber de "autolimpieza". Sobre todo, cuando se trata de las intromisiones que realizan los investigadores en la intimidad de los trabajadores, a través del acceso a sus ordenadores o a sus correos electrónicos o mediante la captación de imágenes por cámaras de video vigilancia.

Resulta esencial distinguir entre las diferentes esferas de protección, puesto que se dan ciertos supuestos en que las intromisiones en la intimidad de los trabajadores pueden ser toleradas quedando al margen de la tipicidad, a diferencia de otras injerencias en la intimidad que, por su gravedad *-pero también por las particularidades de la relación laboral-*, no pueden ser toleradas, incluso cuando el lesionado haya dado su consentimiento (la

---

<sup>665</sup>De otra opinión, ESTRADA I CUADRAS, A. / LLOBET ANGLI, M. "Derechos...", cit., pp. 201 y S., quienes caracterizan como investigaciones internas procesos preventivos que, en mi opinión, deberían caracterizarse más bien como de "control".

<sup>666</sup>Ello no debe llevar a negar la clara interdependencia que existe entre las competencias empresariales de "controlar" e "investigativas". De hecho, las sospechas que llevan a la implementación de las investigaciones internas surgen normalmente no sólo a partir de denuncias externas o del sistema de *whistleblowing*, sino también a partir de los informes presentados por los auditores. Esta delimitación tampoco niega cierto componente de "controlar" que en el fondo tienen las investigaciones internas (cfr. KNAUER, C. "Interne...", cit., p. 42). MONTIEL, J. P., "Sentido y alcance...", ob. cit., pp. 495-496

captura de imágenes en baños o vestuarios, exámenes genéticos compulsivos, la interceptación de correspondencia electrónica estrictamente personal o el registro de taquillas, implican la realización de las conductas tipificadas en los arts. 197 y ss. CP). No obstante, se dan determinados supuestos en los que el empresario puede realizar alguna de estas conductas para salvaguardar un interés superior, como la seguridad de la empresa o de los trabajadores y en circunstancias excepcionales<sup>667</sup>.

En estos casos, la dignidad del trabajador y que se mantenga la proporcionalidad en las medidas adoptadas, resultan esenciales para poder encontrar una causa de justificación a tales conductas. Como consecuencia de la inaplicabilidad del estado de necesidad y de legítima defensa (por la falta de actualidad o inminencia de la agresión o el peligro) se centra la atención en la eximente del cumplimiento de un deber. Cabe plantearse si existe o no un deber de realizar las investigaciones internas y si se puede justificar la intromisión de esta manera en la intimidad de los trabajadores.

De esta forma, si se tienen en cuenta las exigencias de un buen gobierno empresarial derivadas de los *Compliance Programs*, resulta lógico concluir que dicho deber existe. Las investigaciones internas son fundamentales para el mantenimiento de un sistema general de cumplimiento de la legalidad y para garantizar su verdadero seguimiento. Permiten disuadir a futuros transgresores de incurrir en conductas ilícitas y ayudan a detectar fallos en la organización empresarial y en el *Compliance Management*. Para poder garantizar el buen funcionamiento de este *Compliance Management* se deben realizar investigaciones internas. Pese a ello, es muy difícil encontrar en la legislación alemana, estadounidense y española un deber legal que obligue a las empresas a someterse a un proceso de autolimpieza<sup>668</sup>.

---

<sup>667</sup>MONTIEL, J. P., "Sentido y alcance...", ob. cit., pp. 500-501.

<sup>668</sup>MONTIEL, J. P., "Sentido y alcance...", ob. cit., pp. 501-502.



Además, tal y como ya hemos mencionado, las investigaciones internas suponen para la empresa un coste económico elevado, por lo que no todas disponen de los recursos necesarios para poder realizarlas<sup>669</sup>. Esto supone que, en ocasiones, algunas empresas se ven obligadas por motivos económicos a tener pretensiones más modestas a la hora de investigar la sospecha de un delito. Por otra parte, el inicio de una investigación no es un hecho que pase inadvertido para los accionistas. Si ésta no se realiza de forma correcta, ya sea por exceso o por defecto, puede también incidir negativamente en el valor de las acciones de la empresa<sup>670</sup>. Asimismo, que los investigadores realicen prácticas excesivamente abusivas puede generar responsabilidad en la empresa por infracciones penales, laborales y del Derecho de protección de datos<sup>671</sup>. Por lo que en la decisión de dar inicio a una investigación se pone de manifiesto una serie de factores con incidencia jurídica y económica que deben ponderarse<sup>672</sup>.

Además, la fuerte presión que reciben las empresas para adecuarse a las exigencias generales del *Compliance Management* con el fin de evitar incurrir en responsabilidad jurídica y penal llevan a los órganos de gobierno a tomar medidas destinadas a evitar o disminuir al mínimo los costes jurídicos y reputacionales, iniciando las investigaciones a la más mínima sospecha<sup>673</sup>. Esto supone para la empresa la necesidad de adoptar una decisión que sea materialmente acertada en relación con las cuestiones jurídicas y económicas

---

<sup>669</sup>SAHAN, S. "Unternehmensinterne...", cit., pp. 174 Y s. El caso Siemens es un excelente ejemplo de ello: las investigaciones le costaron a la empresa cerca de mil millones de euros (cfr. KUHLEN, L., "Grundfragen von Compliance und Strafrecht", AA.VV., *Compliance und Strafrecht*, coords. Kuhlen/Kudlich/Ortiz de Urbina, C. F. Müller, Heidelberg, 2012, pp. 9 y ss.) e incluso ya para 2008 la empresa alemana gastó € 63.000.000 entre la contratación de asesores externos para que realicen las investigaciones internas y medidas para evitar fallas del sistema de control. Cfr. el informe de Siemens de 26 de abril de 2007 en [www.siemens.com](http://www.siemens.com). Analizando en la doctrina este punto MOMSEN, C. "Internal...", cit., p. 510.

<sup>670</sup>PROPPER, E. *Corporate...*, ob. cit., pp. 58 y s.

<sup>671</sup>Cfr. dictamen de la BRAK N° 35/2010, p. 7. Cfr. también SCHÜRRLE, T. /OLBERS, L.A.M. "Praktische...", cit., p. 179, cit., p. VI; GERKE/RICHTER, "Die Vertretung von Arbeitsgebern in (Arbeits-) Strafverfahren", en Gerke/Kraft/Richter, *Arbeitsstrafrecht. Strafrechtliche Risiken und Risikomanagement*, C. F. Müller, Heidelberg et. al., 2012, nm. 104.

<sup>672</sup>PICKETT, S. *Internal Investigations: A Basic Guide Anyone Can Use*, Wiley, Southern Gate, 2008, p. 27.

<sup>673</sup>PROPPER, E. *Corporate...*, cit., pp. 10 y ss.; SAHAN, "Unternehmensinterne...", cit., p. 175.

planteadas y que sea, además, veloz. Se plantea para la empresa una encrucijada de la que difícilmente puede salir completamente ilesa<sup>674</sup>.

Así pues, la exigencia de celeridad en el inicio de las investigaciones conduce a cuestionar si el nivel de sospecha requerido para iniciarlas debería ser superior a un proceso judicial ordinario. Esto puede afirmarse intuitivamente, si se parte de la consideración de que las facultades coercitivas e investigativas de la empresa en un Estado de Derecho deben ser menores a las de las autoridades públicas que ostentan la legitimidad política para ello. No obstante, si se tiene en cuenta cuál es la función que el mismo Estado quiere asignarle al empresario a la hora de prevenir delitos, podría afirmarse, al menos, que las investigaciones puedan iniciarse cuando se cuenta con los mismos niveles de sospecha que se aceptan para iniciar una investigación judicial<sup>675</sup>. Además, las empresas se ven compelidas (fácticamente) a colaborar tanto a nivel nacional como internacional con las autoridades, por lo que dicha intuición inicial supondría colocar al empresario en una situación de cuasi-inexigibilidad<sup>676</sup>.

El hecho de que una empresa active un mecanismo de "autolimpieza" no significa que tenga lugar una investigación con dimensiones idénticas o equiparables a las de un proceso penal. Una vez que la investigación se inicia, corresponde a la junta directiva analizar la oportunidad y las medidas que serán adoptadas, teniendo en cuenta la envergadura del problema<sup>677</sup>, atendiendo, además a la debida proporcionalidad. A título de ejemplo, un "rumor de pasillo" sobre el soborno a un funcionario público por parte de un empleado no implica automáticamente que el empresario pueda revisar los correos electrónicos personales y laborales, taquillas, etc.<sup>678</sup>. Las medidas

---

<sup>674</sup>MONTIEL, J. P., "Sentido y alcance...", ob. cit., pp. 507-509.

<sup>675</sup>En este sentido, MOMSEN/GRÜTZNER, "Verfahrensregeln...", cit., p. 1793.

<sup>676</sup>MONTIEL, J. P., "Sentido y alcance...", ob. cit., p. 509.

<sup>677</sup>PROPPER, E. *Corporate...*, cit., pp. 51 y s.

<sup>678</sup>BUCHERT/JACOB-HOFBAUER, "Hinweisgebersysteme des Unternehmens", en Knierim/Rübenstahl/Tsambikakis (eds.), *Internal Investigations. Ermittlungen im Unternehmen*, C. F. Müller, Heidelberg et. al., 2013, nm. 39.

adoptadas dependerán de la gravedad del delito que se sospecha y de la certeza que sobre la misma exista<sup>679</sup>. En este tipo de casos resulta conveniente la adopción de otras medidas menos invasivas. Es más, sería esperable que la empresa decida iniciar una investigación cuando, a partir de suficientes y fundadas sospechas, esté en condiciones de concluir que existe la probabilidad, *según leyes de la experiencia*, de que el delito ha tenido lugar<sup>680</sup>. En definitiva, la junta directiva solamente puede acordar la realización de una investigación corporativa cuando tenga, como mínimo, una sospecha fiable de que se ha cometido un ilícito<sup>681</sup>.

Sin embargo, las investigaciones internas no sólo permiten averiguar los delitos cometidos en contra de la empresa (imaginemos una apropiación indebida o el espionaje industrial), sino que también permite averiguar los delitos cometidos contra otros trabajadores, como el acoso sexual u otras infracciones al código ético que no constituyen necesariamente hechos delictivos<sup>682</sup>. Esto último debe ser tenido en cuenta a la hora de realizar una investigación interna ya que cuando discurre o puede discurrir de manera paralela a una investigación pública (ya sea judicial o administrativa) es necesario comprobar su compatibilidad<sup>683</sup>.

Ya hemos hecho referencia a que las investigaciones internas se activan por la existencia de una sospecha de irregularidad. Son una herramienta de

---

<sup>679</sup>PAUTHNER-SEIDEL, S. "§ 27: Compliance-Managementsysteme für Unternehmensrisiken im Bereich des Wirtschaftsstrafrechts", en Hauschka (ed.); *Corporate Compliance*, C. H. Beck, München, 2010 (2ª ed.), nm. 50.

<sup>680</sup>SAHAN, S. "Unternehmensinterne...", cit., p. 174. Sobre los conceptos de sospecha y de probabilidad necesarios para el inicio de una investigación judicial (aplicable, según lo visto, al comienzo de las investigaciones empresariales), cfr. KÜHNE, H., *Strafprozessrecht. Eine systematische Darstellung des deutschen und europäischen Strafverfahrensrechts*, C. F. Müller, Heidelberg et. al., 2010 (8ª ed.), nm. 327 y ss.

<sup>681</sup>Por esta razón encuentro conceptualmente discutible que puedan existir (como tales) "investigaciones internas" en las que no haga falta contar con una sospecha. Considerando posible distinguir entre investigaciones empresariales que exigen sospechas y otras que no, ESTRADA I CUADRAS, A. /LLOBET ANGLÍ, M. "Derechos...", cit., p. 201. Es más, como entiende correctamente KÜHNE, H. *Strafprozessrecht...*, cit., nm. 336, resulta conceptualmente insostenible hablar de una investigación sin sospecha.

<sup>682</sup>NIETO MARTIN, A., "Investigaciones internas", en AA.VV., *Manual de cumplimiento penal en la empresa*, dir. A. Nieto Martin, Valencia, 2015, pp. 231-232.

<sup>683</sup>MONTIEL, J. P., "Sentido y alcance...", ob. cit., pp. 510-511.

cumplimiento de carácter reactivo. El canal de denuncias es la primera fuente para el conocimiento de esa sospecha. La necesidad de contar con un procedimiento de investigaciones internas es una consecuencia lógica de la existencia de dicho canal, pero no supone la única vía para poder conocer de una irregularidad. Por ejemplo, una noticia de prensa, demandas de carácter civil, quejas de los consumidores, denuncias o querellas, notificaciones judiciales, etc., son también hechos que pueden, e incluso deben, dar lugar a la apertura de una investigación.

Los colegios de abogados en algunos países (como Alemania o EEUU) han elaborado reglas deontológicas para salvaguardar los conflictos que pueden darse entre la representación de los intereses de la empresa y el de los empleados investigados, cuando es un abogado externo el que realiza las investigaciones internas. Puesto que deben ser las empresas las que establezcan su marco jurídico, es recomendable que adopten un Código de investigaciones internas. Por ello, la existencia de normas internas preestablecidas, aprobadas por la dirección de la empresa y además, conocidas por todos los empleados permite la realización de las investigaciones y evita el que se cometan errores o que la investigación no se haga de forma correcta, lo que puede implicar importantes perjuicios para la empresa.

El inicio de la investigación interna no sólo supone para la empresa tener que asumir importantes costes sino que también, afecta a los derechos de las personas investigadas. Se exige un mínimo de certeza en la sospecha atendiendo al principio de proporcionalidad. Dicho de otro modo, aquellos que tienen la capacidad para abrir la investigación estarían empleando los instrumentos de la empresa de una forma contraria al deber y, de otra, estarían lesionando indebidamente el honor u otros derechos fundamentales, como la intimidad o el secreto de las comunicaciones, de los afectados, lo que podría dar lugar a reclamaciones por daños y perjuicios.

En el caso de que la fuente de conocimiento sea el canal de denuncias, resulta necesaria la certeza de la verosimilitud de los hechos como diligencia exigible a aquellas personas u órganos encargados de iniciar la investigación, para evitar las denuncias de mala fe y sancionarlas internamente. No olvidemos que una de las funciones de las investigaciones internas es la de impulsar a las empresas a que averigüen hechos en circunstancias en las cuales el Estado aún no se encuentra legitimado para abrir una investigación, al no existir una sospecha razonable para ello. Por lo que el empresario tiene derecho (con un grado de sospecha mucho menor) a investigar y conocer, qué ocurre en la actividad que desarrolla. Las investigaciones internas se fundamentan en el poder de dirección del empresario, ámbito al que no tiene sentido trasladar los límites que marcan el ejercicio del *ius puniendi*<sup>684</sup>.

La ejecución de una investigación interna constituye una obligación de los directivos de una entidad, como manifestación de su poder de dirección. Poder asegurar que la empresa respete la legalidad es una consecuencia del buen gobierno corporativo y la responsabilidad social, así como de la obligación de evitar los riesgos legales que para la entidad significa la realización de una infracción penal o sancionadora administrativa. Aparte de la posible responsabilidad penal en que pueda incurrir el directivo o los encargados de cumplimiento por no realizar esta investigación (partiendo de un análisis conjunto del derecho de sociedades y del derecho sancionador, penal y administrativo), su no ejecución en caso de que se derive un perjuicio para la persona jurídica, puede dar lugar a la interposición de acciones de responsabilidad social contra el administrador.

Sin embargo, este deber de la empresa de realizar una investigación interna no es automático, sino que responde a cierta discrecionalidad. Y en este sentido deben tenerse en cuenta tres indicadores.

---

<sup>684</sup>NIETO MARTIN, A., "Investigaciones internas", ob. cit, pp. 233-237.

El primero de ellos es el daño que puede ocasionar a la entidad en el supuesto de no realizar la investigación, si se tiene conocimiento de una posible infracción. La investigación se hace necesaria en los casos en los que se haya cometido una infracción continuada que se prolonga en el tiempo, cuando existe el riesgo de que la infracción se haya convertido en una práctica habitual o cuando la sospecha se refiere a una infracción que aún no ha sido consumada o se encuentra en una fase preparatoria (por ejemplo, existen sospechas de que se está construyendo una caja negra). Ello no sólo para evitar la imposición de sanciones contra la empresa, sino para evitar cualquier otro tipo de daño, como pueden ser daños de carácter económico, pérdida de mercados, o incluso la prohibición de contratar con la Administración Pública. Por todo ello, cuando la infracción ha perjudicado patrimonialmente a la entidad y la investigación resulta necesaria para identificar a los responsables y ejercer las acciones legales correspondientes, el deber de iniciar la investigación no plantea duda al respecto.

El segundo indicador de la discrecionalidad en las investigaciones internas es el de mejorar el sistema de prevención, esto es, el debido control de la entidad. En los supuestos en los que la infracción ponga de manifiesto un defecto grave en el sistema, éste debe ser subsanado. En este caso, la investigación interna puede plantearse desprovista de fines represivos, tratando de buscar una colaboración de todos para descubrir las lagunas en el sistema de prevención. Por lo que las investigaciones resultan especialmente idóneas, en estos supuestos, para el caso de accidentes laborales, o en general, comportamientos imprudentes que tienen lugar en el desarrollo de la actividad de la empresa.

El tercer indicador hace referencia a que de la efectiva vigencia del código ético de la empresa y de las políticas que de él se derivan, depende de que sus infracciones sean o no sancionadas. Una de las condiciones para que un sistema de cumplimiento sea efectivo es que se sancionen disciplinariamente sus infracciones. En caso contrario, carecería de sentido la implementación

de un canal de denuncias, si los empleados supieran que las infracciones no iban a ser ni tan siquiera investigadas. Uno de los indicadores que debe examinarse en el proceso penal como prueba de que el sistema de prevención es el correcto, es el registro de sanciones e investigaciones internas. No obstante, la importancia de investigar, y en su caso, de sancionar adquiere mayor relevancia cuando la infracción es cometida por un alto directivo de la entidad.

Ahora bien, la apertura o la continuación de una investigación interna puede, sin embargo, ser más discutida en aquellos casos en los que ya se ha iniciado una investigación penal o administrativa, partiendo de la idea de que la capacidad de investigación del Estado es más eficaz que la que se puede realizar internamente por la empresa y, hace innecesaria esta última.

Pero esto no significa que la investigación penal o administrativa sea necesariamente más eficaz que la investigación interna. Los empleados tienen en la investigación interna un deber de veracidad que no tienen siempre en el proceso penal y, la empresa puede acceder con mayor facilidad a determinados medios de prueba como correos electrónicos o locales. Los hechos investigados en el proceso penal pueden ser distintos a los que resultan de interés en la investigación interna. La función de esta última no se limita a descubrir al responsable de la infracción, sino que trata de analizar por qué en la empresa aparecen comportamientos irregulares o las deficiencias que presenta el programa de prevención. Es evidente que la finalidad de la investigación interna es más amplia que la de la investigación penal. No obstante, en ocasiones, la existencia de una investigación penal supone la coartada perfecta en una organización para que todo siga igual.

Puesto que son los administradores los que asumen el deber de instaurar un programa adecuado de prevención y de ejercitar el debido control, son también los órganos competentes (puede delegarse en el comité ético o en el *compliance officer*, o en personas u órganos más cercanos cuando se trate

de empresas regionales o grupos) para decidir sobre la apertura de la investigación. Precisamente, por las importantes repercusiones que puede tener la apertura de una investigación y por la especial necesidad de que esté legitimada, resulta aconsejable que el Consejo de Administración tenga conocimiento inmediato de aquellos hechos que, por su gravedad, puedan tener especial alcance en la actividad de la sociedad<sup>685</sup>.

El hecho de que la investigación pueda abrirse por el órgano de cumplimiento cuando la misma pueda afectar a un miembro del Consejo o directivo supone un signo de calidad del programa instaurado.

De esta forma, se designará la persona que va a hacerse cargo de la investigación si se concluye que los hechos son verosímiles (al amparo de una investigación preliminar) y el órgano competente considera necesaria la investigación.

Por lo que la primera pregunta que se plantea es si la investigación debe ser realizada por un abogado externo, o en cambio debe realizarse internamente. Esta decisión depende de múltiples factores tales como el coste de la externalización o la existencia de personas dentro de la entidad con capacidad suficiente para realizar una investigación. Las grandes empresas pueden incluso disponer de un equipo especializado.

Por otra parte, un factor determinante es en qué medida los hechos sobre los que versa la investigación están judicializados o pueden llegar a estarlo, puesto que, en el caso de estarlo debe valorarse hasta qué punto los servicios jurídicos o auditores internos cuentan con el secreto profesional y la capacidad de preservar la confidencialidad de los documentos generados por la investigación frente al juez, fiscal o las autoridades administrativas. Puesto que una investigación puede comprender diversos países y estas circunstancias dependerán de cómo se regule en sus ordenamientos, será

---

<sup>685</sup> NIETO MARTIN, A., "Investigaciones internas", ob. cit, pp. 237-238.



necesario previamente comprobar cuál es la situación legal en cada uno de ellos. Salvo excepciones, como en materia de blanqueo de capitales o infracciones en el mercado de valores, la empresa no tiene obligación de colaborar en la investigación pública y denunciar los hechos. No obstante, puede resultar conveniente cooperar con la investigación por razones de estrategia procesal.

En los supuestos en que la investigación interna está conectada con un proceso penal, ya se haya iniciado o ésta sea previsible, lo normal debe ser que la investigación interna sea dirigida por el abogado que representa a la empresa o, al menos, que exista una estrecha coordinación entre ambos<sup>686</sup>.

Es importante hacer mención a la relación que se plantea entre los responsables del canal de denuncias y los encargados de realizar la investigación, puesto que puede producirse entre sus funciones un conflicto de intereses. Los responsables del canal tienen como cometido la defensa de la confidencialidad y la protección del denunciante, por lo que la colisión se hace especialmente patente cuando se atribuye a un servicio de ombudsman (como puede ser un abogado externo) la gestión del canal de denuncias.

Por ello, lo razonable es que se busque un cierto grado de especialización y se evite cualquier conflicto de intereses en los casos de haber optado por la investigación interna. Es frecuente que las investigaciones de mobbing o acoso sexual sean dirigidas por los encargados del departamento de recursos humanos, mientras que las relacionadas con fraudes de empleados a la empresa por los auditores internos, si son relativas a la calidad de productos, medio ambiente o protección de los trabajadores por las personas responsables en estas materias dentro de la empresa. En estos casos, adquiere especial relevancia la imparcialidad de estas personas debido precisamente a su proximidad con la materia objeto de la investigación.

---

<sup>686</sup>NIETO MARTIN, A., "Investigaciones internas", ob. cit, pp. 238-239.

El nombramiento de la persona responsable para realizar la investigación debe ir acompañado de una orden del órgano competente para decidir sobre la apertura de la investigación, en la que se deberá fijar los objetivos y la duración de la misma. También se debe determinar si la investigación tiene únicamente como objetivo corregir los fallos del sistema, sin que vayan a derivarse la imposición de sanciones disciplinarias, si responde a una cierta o posible cooperación con una investigación penal o administrativa o si implica la adopción de medidas disciplinarias. Y en este sentido, el presupuesto básico del *fair trial* en las investigaciones internas es la información a los empleados sobre su finalidad. De esta forma se permite evaluar cuáles van a ser sus respuestas y su grado de implicación en la investigación.

Así pues, la persona encargada de la investigación debe proceder a redactar un plan de la investigación (aprobado expresamente por el órgano interno que ha ordenado la misma) en el que se especifique su duración, el calendario de trabajo previsible, la lista de personas que van a ser entrevistadas, los documentos a los que se va a tener acceso, las sedes o despachos que pueden ser registrados, etc.

Tanto la orden como el plan de investigación suponen un instrumento fundamental para poder asegurar la proporcionalidad de los medios a emplear y determinar con antelación, el coste de la investigación. Además, son básicos para legitimar la investigación y transferir el poder necesario al director de la investigación, de forma que su actividad no se vea cuestionada dentro de la empresa. De algún modo, se puede equiparar la aprobación del plan de la investigación con el control similar que realiza el juez de garantías en relación a las medidas de investigación que pretende realizar el fiscal. Por todo ello, cualquier modificación que sufra el plan debe ser comunicada por su director al órgano o persona competente para decidir la apertura de la investigación con el fin de que sea aprobada o autorizada. Esto se complica cuando la investigación se realiza en varios países, puesto que es necesario

que en el plan se compruebe y se señale expresamente la legitimidad de las medidas en cada uno de ellos<sup>687</sup>.

Otra cuestión que debe plantearse en el plan de investigación, es la de determinar quién va a formar parte del equipo. De esta forma, cuando la investigación deba ser realizada por un abogado externo, se nombrará a un coordinador externo que conozca bien la organización y que se encargue de la interlocución con los distintos departamentos afectados junto con otro personal interno o externo que, en su caso, debe participar. En este sentido, los encargados de protección de datos, de seguridad informática, los servicios de auditoría interna, etc., pueden resultar de gran utilidad.

Por último, el principio *need to know* debe tenerse en cuenta en el momento de la apertura de la investigación (ya sea por el órgano competente para ello o por su director). Del mismo modo a lo que ocurre en el proceso penal, las empresas pueden no querer hacer pública la investigación o que se conozcan sólo algunos aspectos de la misma, con el objetivo de evitar cualquier daño reputacional o un daño al honor de la persona que está siendo objeto de la investigación, o cuando se trate de secretos industriales o de la empresa. El conocimiento de la estrategia de la investigación o de diversas actuaciones puede frustrar sus objetivos, adquiriendo especial relevancia el factor sorpresa en la realización de algunas de las actividades de investigación. Por ello, el principio *need to know* se configura como un equivalente al secreto del sumario en el proceso penal, hasta el punto de que la violación de este principio puede dar la voz de alarma y acabar con el factor sorpresa, que necesita toda investigación<sup>688</sup>.

Ahora bien, la mayor parte de los peligros que se pueden derivar se refieren a la fase relativa a su ejecución, como consecuencia de la utilización de medios de investigación que vulneren derechos fundamentales.

---

<sup>687</sup> Los requisitos para acceder a los correos electrónicos o proceder a registrar el despacho de un directivo que se exigen en un país o en otro pueden ser distintos.

<sup>688</sup> NIETO MARTIN, A., "Investigaciones internas", ob. cit, pp. 241-243.

La empresa lleva a cabo las investigaciones internas con el objetivo de atenuar o evitar la responsabilidad penal, pero atentar indebidamente al derecho a la intimidad o al secreto de las comunicaciones de las personas investigadas, puede constituir un delito contra la intimidad. El acceso a los correos electrónicos contenidos en los sistemas informáticos de la empresa, sin haber advertido previamente a los empleados de la ausencia de privacidad en su uso, los registros indebidos de documentos que se encuentran en el despacho de un empleado o en archivos de carácter personal que la empresa autoriza a crear en los ordenadores de trabajo, constituyen los típicos ejemplos en los que sería fácil afirmar que los delitos han sido cometido por cuenta y en provecho de la persona jurídica, y por tanto generar responsabilidad.

Pero no sólo pueden cometerse delitos contra la intimidad. El hecho de amenazar indebidamente a un empleado con el despido en caso de no colaborar con la investigación (la técnica conocida como el talk or walk), puede dar lugar a un delito de amenazas, cuando el empleado tenga derecho a guardar silencio y no colaborar con la investigación.

Tiene especial trascendencia en el proceso penal, ya que si se han vulnerado los derechos fundamentales a través de medidas de investigación esto impide, según la doctrina mayoritaria, que este material probatorio pueda ser utilizado posteriormente en el mismo. Es más, si tenemos en cuenta la teoría del fruto del árbol envenenado, podría incluso cuestionarse la validez de las pruebas que se obtuvieran directamente a partir de esta circunstancia. Ello impediría o reduciría la posibilidad de que la persona jurídica pudiera beneficiarse de la atenuante de colaboración y además entorpecería la investigación penal o administrativa, afectando a sus posibilidades de defensa<sup>689</sup>.

---

<sup>689</sup>Por esta razón, debe examinarse la legitimidad y proporcionalidad de cada uno de los medios así como de la forma en que éstos son desarrollados. Que la empresa cuente con un Código de

La información necesaria para esclarecer los hechos puede encontrarse tanto dentro de la empresa (documentos, información que puedan suministrar los empleados), como fuera de ella (registros públicos o páginas web). En el supuesto de que un directivo haya cometido un fraude, comprobar qué patrimonio tiene, en qué empresas participa directa o indirectamente o quién ha podido servirle como testaferro para ocultar los bienes sustraídos, puede resultar muy útil. Lo mismo puede ocurrir en los casos de corrupción, donde puede ser necesario conocer las posibles vinculaciones del empleado con el funcionario público o conocer la identidad del agente comercial que se ha contratado en un tercer país para que represente a la empresa.

Que una empresa acceda a información externa puede ser muy costoso. No obstante, existen multitud de fuentes de información públicas que pueden ser utilizadas. A título de ejemplo, registros públicos (de la propiedad, mercantil, civil, tributarios...), búsquedas en internet o en prensa de todo tipo, las agencias de información crediticia, etc. Gracias a la sociedad de la información, el e-government, fenómenos como las redes sociales, las Web 2.0, como Google, etc., se ha permitido que los datos de cualquier persona o empresa puedan ser vendidos, recopilados en bases de datos y analizados. Surge así una nueva industria, esto es, la industria de la inteligencia (corporate intelligence), especializada en la recolección y en el análisis de esta información, para ponerla al servicio de las empresas como parte del negocio de la denominada gráficamente “minería de datos” (data mining)<sup>690</sup>.

La segunda gran fuente de información son los documentos internos de la entidad, por lo que resulta esencial, como parte del éxito del programa interno de cumplimiento, establecer previamente qué documentos van a ser esenciales en el futuro para una defensa penal.<sup>691</sup>

---

investigaciones internas en el que se establezcan los principios y las garantías básicas, permite reducir los riesgos en la misma.

<sup>690</sup> NIETO MARTIN, A., "Investigaciones internas", ob. cit, pp. 243-244.

<sup>691</sup> Corresponde a los responsables del cumplimiento procurar que estos documentos se conserven debidamente, no sean destruidos y que se elaboren de forma para que no se ponga en duda su

En aquellos casos en los que la investigación tenga por objeto la imposición de sanciones disciplinarias, los investigados tienen derecho a las garantías que se establecen en el TRLET. No obstante, dada la parquedad en el ámbito de la legislación laboral, resulta necesario especificar cuáles son los derechos de la persona investigada en aquellos supuestos en los que pueda ser objeto de sanciones disciplinarias.

Como consecuencia de lo anterior, un modelo de cumplimiento que responda a la promoción de determinados valores éticos debería recoger los derechos básicos de todo proceso justo, lo que implica tener en cuenta los siguientes derechos<sup>692</sup>:

- Derecho a ser informado con claridad de los hechos que se le imputan. Corresponde a la empresa escoger la forma en que llevará a cabo esta información, siendo lo más conveniente hacerlo a través de entrevista personal.
- La facultad del investigado para revisar las distintas pruebas tales como documentos, entrevistas, etc. que existen en su contra así como el expediente de la investigación antes de que se adopte decisión alguna. Sin embargo, esta facultad encuentra un límite y es que no puede ser desvelada la identidad de la persona que, confidencialmente, ha realizado una comunicación o denuncia.
- El derecho del investigado a hacer alegaciones y presentar ante la persona o equipo que realiza la investigación la prueba que considere oportuna (nuevos testigos, documentos, etc.).
- Si lo desea la persona investigada puede contar con la asistencia de un abogado para que esté presente durante las entrevistas o el acceso al

---

autenticidad. En este punto, el cumplimiento normativo debe ponerse en conexión con una adecuada política de seguridad de la información.

<sup>692</sup>NIETO MARTIN, A., "Investigaciones internas", ob. cit, p. 257.

expediente. En este caso, la empresa no tiene por qué abonar los honorarios en que se hayan incurrido.

- El derecho a la presunción de inocencia y el derecho a no declarar contra uno mismo.

Debe tenerse en cuenta que no existe ninguna norma en nuestro ordenamiento relativa a cuál es el papel de los representantes de los trabajadores en estos casos, salvo que se trate de un procedimiento que afecte a un delegado sindical.

La investigación debe concluir con un informe final que habrá de presentarse al órgano o la persona que en la empresa la ha ordenado. Este informe puede ser oral, en el caso de que la empresa haya decidido mantener reservada la información resultante de la investigación y evitar el riesgo de que pueda ser entregada a terceros por razones de estrategia de defensa. Sin embargo, se considera preferible, con carácter general, concluir con un informe escrito, que contenga los hechos y todos los aspectos relativos a la investigación que se consideren convenientes. Este informe debe evaluar el sistema de cumplimiento de la empresa, indicando, los errores que hayan detectado y que han hecho posible la infracción incluyendo, además, las posibles propuestas de mejoras que se recomiendan. También puede incluir una propuesta para la imposición de sanciones disciplinarias dependiendo de cómo la empresa haya configurado su sistema de cumplimiento<sup>693</sup>.

Así pues, cuando se impongan sanciones disciplinarias y los hechos que han motivado la investigación sean conocidos, el resultado de la misma debe hacerse público, por regla general, para que exista conciencia de que el sistema de cumplimiento funciona efectivamente y que la empresa lo toma en serio. De esta forma, garantizar la transparencia aumenta la legitimidad del

---

<sup>693</sup>NIETO MARTIN, A., "Investigaciones internas", ob. cit, pp. 257-258.

sistema y por tanto su cumplimiento por parte de los miembros de la organización<sup>694</sup>.

El hecho de que la investigación interna sea parte del derecho de defensa, al amparo de los objetivos mencionados, supone que no puede ser prohibida por el juez o fiscal. En este sentido, resulta irrelevante que la investigación interna, además de estos objetivos de defensa, persiga otros objetivos puramente internos como puede ser la imposición de sanciones disciplinarias o la mejora de su sistema de cumplimiento. Es más, incluso puede entenderse que estos objetivos son necesarios para mostrar judicialmente que existe un programa de cumplimiento eficaz.

Ahora bien, el que las investigaciones internas sean legítimas no implica, de un lado, que estén exentas de limitaciones y, de otro, que no sea aconsejable informar de su existencia al juez de instrucción y al fiscal. No cabe duda que toda investigación que implique la comisión de delitos contra la administración de justicia, serán ilícitas como también lo serán aquellos actos de investigación que se hacen contra prohibiciones expresas del Ministerio Fiscal o del juez instructor (como por ejemplo si se acuerda el precinto de ordenadores o locales de la empresa, ningún medio de investigación interna puede afectarlos). Si bien es cierto que no puede decirse que exista una base legal que permita al juez prohibir que el abogado de la defensa o el director de la investigación se entrevisten con alguien (a diferencia de lo que sucede en Francia en el que sí que existe una prohibición expresa de entrevistarse con personas que van a ser testigos en el proceso penal), el instructor del proceso penal puede mostrar cierto recelo a que la empresa realice entrevistas a las personas físicas directamente implicadas en la investigación, debido a que puede no ser ni aconsejable ni útil<sup>695</sup>.

---

<sup>694</sup>NIETO MARTIN, A., "Investigaciones internas", ob. cit, p. 258.

<sup>695</sup>NIETO MARTIN, A., "Investigaciones internas", ob. cit, p. 265.



Se plantean determinados comportamientos que pueden ser sancionados administrativamente, en el caso de investigaciones administrativas o penalmente, como delitos contra la administración de justicia. Destruir u ocultar pruebas relevantes durante el transcurso de una investigación interna o aleccionar a los empleados para que realicen determinadas declaraciones testimoniales pone de manifiesto, no sólo que la empresa carece de una cultura corporativa de cumplimiento con la legalidad sino, además, que no se ha ejercido con seriedad el debido control.

En relación con la protección de la información generada mediante una investigación, éstas dan lugar a una gran cantidad de información que resulta de utilidad para la persecución del delito. Por ello se plantea la cuestión relativa a, en qué medida esta información es accesible al Estado o, más concretamente, a sus órganos de persecución penales o administrativos, quienes pueden exigir a la empresa que entregue esta información o, incluso, decidan apoderarse de la misma a través de la entrada y registro en los locales de la empresa, sus directivos o sus asesores externos (abogados, auditores, consultores...).

Esto último lo podemos poner en conexión con los problemas que plantea el secreto profesional y su extensión. Para ello debemos partir de dos supuestos diferentes. El primero de ellos se refiere a cuando la investigación interna puede estar conectada con un hecho delictivo que previsiblemente dará lugar a la apertura de un proceso penal en el que la entidad puede verse implicada. En este caso, lo normal será además que la dirección de la investigación recaiga sobre un abogado. Un supuesto diferente es el de aquellas investigaciones internas que no guardan una relación previsible con un proceso penal, o aquellas que tienen carácter prospectivo y que en realidad son auditorías internas<sup>696</sup>.

---

<sup>696</sup>NIETO MARTIN, A., "Investigaciones internas", ob. cit, p. 266.

La información que procede de una investigación interna está protegida por el secreto profesional del abogado (art. 542.3 LOPJ), el derecho de defensa (art. 24 CE) y la exención de no declarar prevista en el art. 416 de la LECr, cuando guarda relación con el derecho de defensa. En este contexto, el derecho de defensa refuerza los contenidos del secreto profesional del abogado, puesto que permite y obliga al mismo a preservar la información que le ha suministrado su cliente o terceros mediante cualquier tipo de comunicación. Esto incluye cualquier escrito, nota, dictamen, etc., que haya podido realizar internamente el abogado con el fin de preparar la estrategia de defensa. De este modo, la información que en el derecho anglosajón se protege a través del denominado *work product privilege* queda, en nuestro sistema protegida por el secreto profesional y el derecho de defensa. Además, el secreto de las comunicaciones y la inviolabilidad del domicilio permiten blindar ésta información a los poderes públicos encargados de la investigación. Cualquier orden de entrada y registro en un despacho de abogados con el fin de obtener información (documentos, archivos de ordenador...) que están protegidos por el derecho de defensa supone una vulneración del art. 24 de la CE.

No obstante, sobre esta materia hay dos cuestiones que resultan especialmente controvertidas. La primera es la relativa a la existencia del secreto profesional en relación a los abogados de empresa. Cuestión que, en relación a las investigaciones internas adquiere especial relevancia, pues con frecuencia será el asesor jurídico de la corporación a quien se le encargue la ejecución de la investigación, lo que supone además un importante ahorro de costes<sup>697</sup>.

Ahora bien, la posición del *in house lawyer* en relación al secreto profesional no se regula de forma uniforme en los diferentes ordenamientos, entre otras razones, porque el abogado de empresa tiene una posición diferente. En el

---

<sup>697</sup> NIETO MARTIN, A., "Investigaciones internas", ob. cit, pp. 266-267.

derecho de la UE, el TJUE ha negado en el asunto AKZO (STJUE de 14.9.2010) que el abogado de empresa pueda acogerse al secreto profesional, señalando como principal argumento su falta de independencia al estar vinculado por relación laboral con su cliente, lo que le vincula a sus órdenes y a su estrategia comercial. Para el TJUE el secreto profesional encuentra su fundamento en la función del abogado como colaborador de la justicia, que se considera como un interés público a preservar. Dado que esta función sólo puede cumplirse cuando quien ejerce como abogado es independiente, el TJUE niega la existencia de secreto profesional.

Este asunto es particularmente importante porque supone el *leader case* en este punto de la jurisprudencia constitucional europea, que necesariamente debe tenerse en cuenta por los tribunales constitucionales internos o el TEDH, como punto de partida. Por otra parte, la confidencialidad se plantea precisamente en relación a la elaboración del programa de cumplimiento de la empresa. La Comisión desea acceder a una serie de notas y comunicaciones entre abogados y clientes efectuadas al confeccionar el programa de cumplimiento en materia de derecho de la competencia.

No obstante, y pese a la importancia de la sentencia del TJUE, debe tenerse en cuenta que en lo que se refiere al derecho español de *lege lata* los abogados de empresa sí que gozan del secreto profesional, en el ejercicio de su actividad de asesoría jurídica. Y en este sentido, ninguna de las normas legales o deontológicas que regulan el ejercicio de la profesión hace excepción alguna en relación a su estatus<sup>698</sup>.

Por ello, lo más prudente es que las investigaciones internas que estén vinculadas con un proceso penal o administrativo iniciado o de previsible iniciación, sean dirigidas por un abogado externo. Esto último servirá para proteger de manera más eficaz toda la información que en ella se genera como las comunicaciones entre los miembros del equipo, las diferentes notas

---

<sup>698</sup> NIETO MARTIN, A., "Investigaciones internas", ob. cit, pp. 267-268.

o escritos que quedarán protegidas por el secreto profesional y custodiada por el abogado externo. De este modo, se refuerza su protección, dada la imposibilidad de obtener una orden de entrada y registro con el fin de acceder a información cubierta por el secreto profesional.

En el caso de que la dirección de la investigación se realice por abogados internos, resulta conveniente en cualquier caso, que en la documentación que genere la investigación se haga constar expresamente que su objetivo es el de recabar información para el asesoramiento legal de la empresa, y, en su caso, su defensa en un procedimiento judicial o administrativo.

El segundo aspecto conflictivo de las investigaciones internas vinculadas a un proceso penal en relación al secreto profesional, es determinar exactamente el círculo de personas protegidas por el mismo. No olvidemos que el secreto profesional puede abandonarse cuando el abogado (ya sea interno o externo) tenga el consentimiento por parte de su cliente (cuando se trate de una persona jurídica) para revelar la información protegida, por lo que se plantea una clara situación de conflicto entre el derecho de la empresa a colaborar con la investigación, revelando la información obtenida mediante el secreto profesional, y la de aquellas personas físicas que han colaborado con la investigación, especialmente al ser entrevistadas. El director de la investigación interna debe dejar bien claro a los empleados, que actúan con la exclusiva finalidad de defender los intereses de la empresa y que la información que se aporte será utilizada atendiendo a sus intereses procesales<sup>699</sup>.

En caso contrario, si los empleados han aportado información creyendo que el abogado defendía sus intereses, constituye una violación del secreto profesional y de sus derechos de defensa, la comunicación de la información aportada por los mismos al proceso penal. Por último, en este caso el

---

<sup>699</sup>NIETO MARTIN, A., "Investigaciones internas", ob. cit, pp. 268-269.

abogado podría ser incluso responsable de un delito de prevaricación de abogados tipificado en el art. 467 CP<sup>700</sup>.

## **6. Gestión del canal de denuncias internas en un grupo empresarial**

Los grupos empresariales suelen abarcar entidades que se encuentren localizadas en diversos países, en cuyo caso habrá que tener en cuenta la diversa normativa de cada Estado. Si se decidiera que los requisitos y funcionamiento del canal de denuncias se aplican por igual en todas las Entidades del Grupo, se debe especificar los requisitos de la normativa que sea más restrictiva. Cabe optar por aplicar criterios comunes menos exigentes, estableciendo sistemas más restrictivos únicamente para aquellos países cuya limitación sea mayor.

En este sentido debe señalarse que si revisamos el Dictamen 1/2006 del Grupo de Trabajo del artículo 29 y el Informe 0128/2007 de la AEPD en los que se contemplan los extremos que deben ser observados por las entidades que pretendan implantar un canal de denuncias para cumplir con la normativa de protección de datos, nos encontramos con significativas diferencias. En el primero de ellos, se establece una preferencia por la confidencialidad, siendo consciente del hecho de que las denuncias anónimas son una realidad en toda organización y concluye que ese tipo de denuncias serán aceptadas pero siempre como excepción a la regla general; en el segundo se establece que para poder garantizar la exactitud e integridad de la información se ha de evitar la existencia de denuncias anónimas. Dicha diferencia supone que, si la entidad que va a gestionar el sistema de denuncias está localizada en un Estado fuera de España, se puede permitir la interposición de denuncias anónimas, mientras que si la entidad se encuentra en España, el criterio del anonimato debe ser eliminado a fin de cumplir con el criterio de la AEPD<sup>701</sup>.

---

<sup>700</sup>NIETO MARTIN, A., "Investigaciones internas", ob. cit, p. 269.

<sup>701</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 639-640.

En los Grupos de empresas es cuestión relevante la del flujo de datos de la denuncia. Así puede ocurrir que la empresa matriz (o la que gestiona el tratamiento y respuesta de las denuncias internas planteadas en el Grupo) sea una organización que se encuentre: a) en un país dentro del Espacio Económico Europeo (EEE); b) en un país cuyo nivel de protección ha sido considerado equiparable al europeo por la Comisión o por la AEPD; c) en una Entidad estadounidense que se encuentre adherida a los principios de "Safe Harbour".

En caso de no estar en ninguno de los supuestos anteriores, se estará produciendo lo que se conoce como una Transferencia Internacional de Datos (TID). Ésta se define como la comunicación a y/o acceso de datos desde países que se encuentran fuera del EEE o desde países que no cuentan con un nivel adecuado de protección (según la Comisión Europea o la Agencia de Protección de Datos) o desde una entidad estadounidense que no esté adherida a los principios de "Puerto Seguro". En este supuesto, la normativa española exige que, previamente a cualquier comunicación y/o acceso desde estos supuestos, se haya solicitado y obtenido la autorización al Director de la AEPD<sup>702</sup>. El proceso de autorización puede durar hasta un máximo de 3 meses desde la solicitud<sup>703</sup>.

Esto supone que, en caso de que una organización envíe información y/o permita el acceso desde una entidad (aunque sea de su grupo empresarial) que se encuentre en alguno de los supuestos anteriores, sin la preceptiva autorización del Director de la AEPD, la organización podría ser sancionada por un incumplimiento de la normativa de Protección de Datos (artículo 33 y 34 LOPD, Título VI y Título IX. Capítulo V del RLOPD<sup>704</sup>)<sup>705</sup>.

---

<sup>702</sup>Son muchas las TID aprobadas dentro de los Grupos de Empresas que tienen por objeto, los mecanismos Whistleblowing ([www.agpd.es](http://www.agpd.es)).

<sup>703</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 640.

<sup>704</sup>El artículo 33 de la LOPD cuyo epígrafe es Norma general establece:

"1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con

Desde el punto de vista territorial, es importante que en el caso de Grupos de empresas (formado por entidades ubicadas en distintos países) se defina previamente cuál de todas llevará la gestión de las denuncias (que normalmente suele coincidir con la matriz del Grupo). No obstante, dependiendo de los países de ubicación de las empresas puede ser recomendable que, debido a las diferencias culturales y legislativas, se establezcan diferentes grupos de recepción y resolución (p.e. Comité de Denuncias de América Latina, Comité de Denuncias de Europa, Comité de Denuncias de Oriente Medio, etc.) de forma que, por un lado, permitan una gestión eficaz de estos canales y, por otro lado, animen a los sujetos a

---

*destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.*

*2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurren en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".*

El artículo 34 de la LOPD cuyo epígrafe es Excepciones establece:

*"Lo dispuesto en el artículo anterior no será de aplicación:*

*a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.*

*b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.*

*c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.*

*d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.*

*e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.*

*f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.*

*g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.*

*h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.*

*i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.*

*j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquella sea acorde con la finalidad del mismo.*

*k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado. TÍTULO VI RLOPT. Transferencias internacionales de datos (arts. 65 a 70)".*

<sup>705</sup> ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., p. 641.

denunciar los comportamientos que, igual en un modelo tan amplio y con muchas diferencias culturales, no se hubieran atrevido a reportar<sup>706</sup>.

## **7. Reacciones de la empresa ante el resultado de la investigación**

El artículo 31 bis.4 del CP diferencia entre las medidas de descubrimiento y las de prevención del delito a los efectos de apreciar la atenuación para la que empresa cuente con ellas. Los procedimientos internos de denuncia son un medio para la averiguación de hechos ya acontecidos, pero si se diseñan adecuadamente podrían aportar una dimensión preventiva y así su capacidad atenuante de la responsabilidad penal. La capacidad preventiva de estas medidas puede valorarse en dos sentidos: la mera previsión de estos canales de denuncia puede aumentar las probabilidades de descubrimiento de las irregularidades, lo que puede tener un efecto disuasorio para posibles infractores; y a su vez, el descubrimiento de los hechos que a través de este sistema puede permitir detectar deficiencias en los mecanismos de control e introducir medidas correctoras que eviten esos hechos en el futuro. Ambas dimensiones deberían tenerse presentes en el momento de valorar judicialmente el grado de eficacia de estos sistemas.

Una cuestión compleja en relación con los sistemas internos de denuncia es cómo la empresa debe comprometerse a reaccionar si comprueba la veracidad de la información recibida. Si la investigación confirma la realización de actos ilícitos por parte de directivos o empleados ello es un motivo justificado para adoptar medidas de tipo laboral contra ellos. La cuestión está en plantearse si la empresa está obligada a proceder a denunciar a sus propios directivos o trabajadores ante la jurisdicción penal<sup>707</sup>.

En los procedimientos de denuncia de empresas españolas publicados en internet se anuncian consecuencias laborales para el trabajador, pero en general no se expresa el compromiso de proceder a la denuncia de los

---

<sup>706</sup>ARMENTIA MORILLAS, P., "Canal de Denuncias", ob. cit., pp. 614-615.

<sup>707</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 191-192.



hechos a las autoridades. En la página web de SACYR VALLEHERMOSO, se hace referencia a sanciones laborales "sin perjuicio de cuantas otras responsabilidades sean exigibles en Derecho al infractor, cuya actuación, lejos de beneficiar a la empresa, ataca sus principios básicos de actuación, basados en el más escrupuloso respeto a la ley"<sup>708</sup>. El BANCO DE SANTANDER establece en su código de conducta que "*el incumplimiento del Código General puede dar lugar a sanciones laborales, sin perjuicio de las administrativas o penales que, en su caso, puedan también resultar de ello*"<sup>709</sup>. En estos textos no se menciona que las empresas se autoimpongan la obligación de denunciar los delitos de los que tengan conocimiento<sup>710</sup>.

Hay que valorar los deberes de denuncia de acuerdo con la legislación penal. Hay que distinguir entre los supuestos en los que la entidad haya sido víctima de las irregularidades descubiertas y aquellos en que se haya beneficiado de una conducta de sus directivos o empleados en perjuicio de terceros o de la colectividad. En el primer caso que no da lugar, a responsabilidad de la propia persona jurídica perjudicada, la empresa no debe temer ninguna consecuencia en caso de no denunciar. En el segundo caso sí puede dar lugar a responsabilidad de la empresa si se cumplen los restantes requisitos del art. 31 bis CP, el hecho de denunciar puede suponer que se abra un procedimiento contra el empleado responsable, y se corre el riesgo de que se impute a la propia empresa, al menos se le exija responsabilidad civil de acuerdo con el art. 120 CP, por no haberse ejercido el debido control sobre el empleado. Ante la posibilidad de imputación de la empresa hay que cuestionarse, si es exigible el compromiso de autodenuncia para beneficiarse de una posible atenuación. La respuesta debe ser afirmativa. El hecho de que el legislador incentive a las empresas con la correspondiente atenuación, incluso exención, en caso de contar con medidas eficaces de descubrimiento y prevención de delitos se justifica por la voluntad de que desde las propias

---

<sup>708</sup><http://www.gruposyv.com/syv/repositorio/syv/ficheros/14/CODIGODECONDUCTASYV2010.pdf>.

<sup>709</sup>P. 26. <http://www.santander.com>

<sup>710</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. p. 192.

empresas se contribuya a esclarecer hechos en los que exista un interés público en perseguirlo, por la necesidad de proceder a su castigo y por la pretensión de compensar a las víctimas por el daño causado. El que una empresa investigue un posible delito y una vez comprobado finalmente lo resuelva exclusivamente en el ámbito interno, por ejemplo con medidas disciplinarias, no contribuye a la satisfacción de las citadas pretensiones<sup>711</sup>.

La previsión de un procedimiento de denuncia interna que no incluya el compromiso de poner los hechos en conocimiento de las autoridades, no debe ser considerada una medida eficaz de descubrimiento del delito que pueda dar lugar a beneficios jurídico-penales. La LECr establece un deber de denuncia que aunque conlleva una sanción meramente simbólica para el caso de incumplimiento, es plenamente vigente cuando se trata de comprobar si una empresa muestra su "*compromiso con la legalidad*"<sup>712</sup>.

Podría replicarse que el hecho de prever que el procedimiento puede culminar con sanciones laborales para el trabajador tiene un efecto preventivo. La adopción de esas medidas no garantiza la satisfacción del interés público en la sanción del posible delito ni la reparación a la víctima del daño causado, como segundo motivo de interés público para privilegiar a quienes se dotan de estos procedimientos. Por ello, si una empresa no quiere establecer en el procedimiento interno el deber de denunciar a sus empleados y a ella misma en caso de descubrir un delito, al menos debería disponer de que tras la comprobación de la veracidad de la denuncia, se ponga en contacto con la víctima para resarcirla de los perjuicios causados.

---

<sup>711</sup>A dicha conclusión parece que necesariamente debe llegarse si se parte de concepciones como aquellas que fundamentan la responsabilidad de las personas jurídicas en la implicación de las empresas en una "nueva tarea pública, la prevención y el esclarecimiento de comportamientos delictivos", como sostiene NIETO MARTÍN, "Responsabilidad social, gobierno corporativo y autorregulación: sus influencias en el derecho penal de la empresa", PolCrim, núm. 5, 2008, p. 17. Añade este autor que "si la empresa ha cumplido de forma razonable con las exigencias de organización que le impone el ordenamiento no será sancionada. Ello conduce a que la empresa en lugar de aliarse con el infractor individual e intentar encubrir su responsabilidad, coopere con la administración de justicia, en cuanto que sabe que este comportamiento atenuará o excluirá su sanción".

<sup>712</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 192-193.

Esta propuesta interpretativa no supone que esta circunstancia atenuante se superponga con las otras tres previstas en el artículo bis 4 CP: confesión, aportación de pruebas y reparación del daño. Estas tres últimas requieren que la denuncia y la reparación se hayan llevado efectivamente a cabo, mientras que, para apreciar la aquí analizada, basta que con el establecimiento de las medidas para el descubrimiento y prevención de delitos futuros culmine en el compromiso de proceder a la denuncia de los hechos penalmente ilícitos de los que pueda tener conocimiento. Esto supone que si, además de implantar este procedimiento, en un caso concreto la empresa efectivamente confiesa, repara y aporta pruebas, puede beneficiarse de atenuantes muy importantes que, de acuerdo con los arts. 66 y 66 bis CP, podrán suponer la imposición de una pena inferior en dos grados a la prevista.

La confirmación por una empresa de que un empleado ha cometido un delito supone frecuentemente la simultánea constatación de que los controles internos no han funcionado correctamente y han permitido la comisión del hecho delictivo. De acuerdo con el artículo 31 bis.4 del CP, para medir la eficacia de un procedimiento de denuncia además de que éste tenga previstas actuaciones tendentes a aclarar (y eventualmente a denunciar) los hechos ya acontecidos, es necesario que la empresa establezca medidas para evitar que en el futuro esos comportamientos o similares se vuelvan a producir<sup>713</sup>.

Si la empresa donde se ha producido el delito no contaba con un programa de prevención es necesario que el que plan que se diseñe antes de la apertura del juicio oral establezca medidas de control relacionadas con el foco de riesgo que ha motivado la imputación de la empresa. Si ese plan ya existía, deberá acreditarse que se han llevado a cabo las actuaciones oportunas para modificar o reforzar los controles ya previstos, al haberse

---

<sup>713</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. pp. 193-194.

mostrado ineficaces para lograr una prevención eficaz de las conductas delictivas. A los efectos de acreditar estas iniciativas las mismas han de documentarse debidamente ante el juez<sup>714</sup>.

A principios del siglo XXI han ocurrido numerosos escándalos financieros que han conmocionado el mundo y han hecho reflexionar a los políticos de ambos lados del Atlántico. Especialmente importantes por su gravedad han sido los casos Enron y WorldCom y años más tarde los casos Lehman Brothers, Siemens, UBS y AIG<sup>715</sup>. Estos escándalos demostraron la necesidad de revisar la efectividad de los estándares de contabilidad, la regulación de la auditoría, y los principios de ética y buen gobierno de las compañías y demostraron la importancia de los whistleblowers.<sup>716</sup>

---

<sup>714</sup>RAGUÉS I VALLÈS, R., "Los procedimientos internos...", ob. cit. p. 194.

<sup>715</sup>TARANTINO, A., *Governance, Risk, and Compliance Handbook*. Wiley. 2008, pp. 113-116.

AGRAWAL, A./ CHADHA, S., "Corporate Governance and accounting scandals", *Journal of Law and Economics*, vol. XLVIII, 2005, pp. 371 y ss; COFFEE, J. F., *Gatekeepers. The professions and corporate governance*. Oxford, 2006, pp. 4, 11, 15, 16, 18, 24; SCHWARTZ, M. / WATKINS, S. *Power Failure: The Inside Story of the Collapse of Enron*, New York, 2003; COFFEE, J. C., Jr, "What Caused Enron - A Capsule Social and Economic History of the 1990s", *Cornell Law Review*, vol. 89, Issue, 2004, pp. 268 y ss. SOLOMON, J./ SOLOMON, A., *Corporate Governance and accountability*, Londres, 2004, pp. 31-35.

<sup>716</sup>AYALA, A. /BARGUEN, G. S. "A Market Proposal for Auditing the Financial Statements of Public Companies" extraído de <http://www.webcitation.org/5tZ0THjI8>

## VII. CONCLUSIONES

- I. Para comprender el Cumplimiento Normativo es necesario conocer el porqué de su origen y su evolución a lo largo de la historia. En las dos primeras décadas del nuevo milenio, el fenómeno del Compliance ha surgido como una respuesta necesaria a lo escándalos financieros que han contribuido a crear la grave crisis mundial que aún seguimos sufriendo.
- II. Actualmente, es un hecho que la mejor forma de prevenir conductas delictivas es fomentar una cultura ética y unos valores comunes entre todos los integrantes de la empresa. Los valores de la empresa son los pilares más importantes de cualquier organización. Los valores de una organización son los valores de sus miembros, y especialmente los de sus dirigentes. Por ello, es fundamental que la cultura ética de la una empresa sea de verdad acogida por sus dirigentes y la prediquen con su ejemplo, lo que se ha llamado el *tone from the top*.
- III. Debemos saber que una cultura empresarial ética es un presupuesto básico para que exista la responsabilidad social corporativa, lo cual también es un presupuesto fundamental para poder cumplir con el buen gobierno en la empresa. El cumplimiento normativo necesariamente se apoya en el buen gobierno corporativo, entendiendo por gobierno corporativo los mecanismos de lucha contra cualquier abuso de poder por parte de los directivos de una compañía.
- IV. Esta ética autoimpuesta por las empresas pasa a ser una forma de *soft law*, la cual se comprometen a cumplir las empresas constituyéndose como un mecanismo de control de ciertos delitos en el seno de las organizaciones empresariales. Estos mecanismos han dejado de ser meras declaraciones o recomendaciones para pasar a constituir verdaderas obligaciones entre los empleados, pudiendo sancionarse disciplinariamente a los mismos si no las cumplieran.

- V. Es evidente que confiar en esta propia autorregulación de las empresas sin establecer unos incentivos o desincentivos legislativos podría convertir a los programas de cumplimiento en papel mojado que sólo sirvan como meros instrumentos de marketing de las empresas frente a la opinión pública.
- VI. En España, la responsabilidad penal de las personas jurídicas fue introducida en el ordenamiento jurídico español mediante la reforma del 2010 del Código Penal. El 1 de julio de 2015 entró en vigor la Ley Orgánica 1/2015 que modifica el Código Penal profundizando en todas aquellas cuestiones que integran esta responsabilidad penal y, en concreto, los elementos que deben concurrir para que la empresa pueda quedar exonerada de responsabilidad, ya que establece, que la adopción y la aplicación efectiva de un programa de cumplimiento normativo puede actuar y servir como un factor eximente o atenuante cuando una empresa esté sujeta a la responsabilidad penal por los delitos cometidos por sus directivos, administradores o empleados.
- VII. El propósito principal de los denominados programas de cumplimiento es asegurar que las actividades de la empresa no incumplan la legislación vigente y aplicable, e incluso más, no vulneren los propios estándares éticos autoimpuestos por la empresa.
- VIII. Las compañías multinacionales con programas de cumplimiento normativo bien establecidos, deben ser conscientes de que la mera traducción al idioma local del programa, no será suficiente para cumplir con los requisitos establecidos por el nuevo Código Penal - aunque supondrá un claro beneficio tenerlo, sobre todo, sí es el reflejo de la existencia de una verdadera cultura de cumplimiento dentro de la organización.
- IX. La reforma Penal del año 2015 aclaró que dentro de los programas de cumplimiento un elemento esencial es la implantación de un sistema de

denuncia interna de irregularidades (whistleblowing). Las empresas deben establecer estos canales o cauces de información para que cualquier empleado, agente o representante que detecte alguna conducta potencialmente criminal o un incumplimiento grave del programa de cumplimiento de la compañía, pueda denunciar o poner el hecho en conocimiento del órgano encargado del control y supervisión de la prevención penal, con garantías de confidencialidad y sobre todo pudiendo garantizar el anonimato del denunciante.

- X. El "Código de buen gobierno de las sociedades cotizadas", de 18 de febrero de 2015 se caracteriza por la voluntariedad de sus recomendaciones, que quedan sometidas a la regla "cumplir o explicar". En el Informe Anual del Gobierno Corporativo ha de constar dicho cumplimiento o su correspondiente explicación (artículo 540.4 g TRLSC).

En relación con los sistemas de información y control interno se recomienda que a la comisión de auditoría además de las funciones previstas en la Ley, le corresponda entre otras la función de *"establecer y supervisar un mecanismo que permita a los empleados comunicar, de forma confidencial y, si resulta posible y se considera apropiado, anónima, las irregularidades de potencial trascendencia, especialmente financieras y contables, que adviertan en el seno de la empresa"* (Recomendación 42.1.c).

- XI. La implantación de este canal de denuncias internas posee doble vertiente: por permitir a la sociedad reaccionar ante el conocimiento de determinados actos irregulares o ilegales ya cometidos; y puede ayudar a inhibir a una persona de realizar algún comportamiento irregular o ilegal que, sin la existencia de este canal de reporte, pudiera estar tentado a realizar.

XII. El mecanismo del canal de denuncias no deja de suscitar recelos, especialmente por cierta predisposición contraria a la delación en el contexto cultural europeo. Asimismo, también plantea interesantes debates de encaje con determinados derechos fundamentales de raigambre constitucional.

XIII. Las palabras whistleblower o whistleblowing no debieron ser utilizadas en sentido despectivo, con connotaciones de "traidor" "chivato". Es un instrumento para descubrir hechos graves, malas prácticas llevadas a cabo en las empresas que pueden perjudicar a los empleados, accionistas y a los ciudadanos o sociedad en general.

XIV. Es interesante contrastar las diferentes experiencias que han vivido los whistleblowers ya que encontramos relatos totalmente opuestas a las vivencias positivas y negativas que han traladan los mismos.

XV. Después de mi investigación considero que los principales requisitos que debe cumplir un procedimiento de denuncia para poder ser considerado en Derecho español una medida eficaz de descubrimiento y prevención del delito son los siguientes:

1. Los empleados tienen el derecho a ser informados de la existencia de un mecanismo de supervisión y control del programa de ética para la detención de conductas criminales o de gravedad por parte de los mismos. El procedimiento de denuncia debe darse a conocer a los potenciales usuarios, que han de poder acceder a él fácilmente.
2. Los usuarios pueden formar parte de la empresa (empleados o directivos), y también pueden ser cualquier persona que haya podido tener conocimiento de conductas ilícitas (clientes o proveedores...). La AEPD ha subrayado que, además de los empleados, podrán establecerse canales de denuncia en relación



a aquellas personas con los que la organización mantenga un vínculo contractual de derecho laboral, civil o mercantil y siempre que existía pleno conocimiento por parte de las personas cuyos datos pudieran ser tratados.

3. Para que esos canales puedan ser utilizados por todas las personas que están vinculadas a la misma, es necesario que se dispongan diversos procedimientos para hacer llegar esas irregularidades. Entre las posibles vías de denuncia debe preverse siempre el correo electrónico, y otros como el teléfono o el correo postal. Siempre ha de quedar constancia documental de la denuncia y demás actuaciones derivadas.
4. En España, el canal debe garantizar el tratamiento confidencial de las denuncias presentadas a través de los sistemas de *whistleblowing*, de forma que se evite la existencia de denuncias anónimas, garantizándose así la exactitud e integridad de la información contenida en los mismos.
5. La protección del whistleblower frente a las represalias de la organización o de sus compañeros constituye una de las principales preocupaciones en esta materia, ya que un empleado sólo se decidirá a denunciar una irregularidad de un superior o de un compañero si tiene la certeza de que ello no le reportará consecuencias negativas.

Estas represalias pueden revestir las más diversas formas y generar un detrimento a los derechos e intereses del denunciante, los cuales pueden ser laborales, económicos o de otra índole. A raíz de ello el tratamiento y regulación de la gestión de denuncias implica la creación e implementación de mecanismos que tiendan a proteger al denunciante, resguardando sus derechos e intereses.

En el marco de un programa de cumplimiento, la certeza de la ausencia de represalias sólo se consigue si el compromiso de la entidad con el programa, con la prevención y el castigo de ilícitos es auténtico, y es que la falta de una cultura corporativa adecuada, merma la efectividad del canal y de toda la política de cumplimiento.

Si no se ponen los medios adecuados a disposición de los empleados para que se pueda hacer uso de estos canales de denuncia, si las denuncias realizadas no llegan a manos de personas que disponen de autonomía e independencia para su manejo, y si la empresa no informa de forma clara y expresa sobre su absoluto rechazo a cualquier tipo de represalia, entonces muy difícilmente se cumplirán los estándares que rigen el funcionamiento de un adecuado buzón de denuncias por infracciones cometidas en el seno de la empresa.

6. El receptor de la denuncia debe de ser una persona con un grado suficiente de independencia suficiente jerárquica en la empresa y con acceso directo al Consejo de Administración de la misma.
7. La compañía debe iniciar una investigación al recibir una denuncia que cumpla con unos criterios mínimos establecidos por la misma. La investigación debe respetar los derechos de la persona denunciada y debe tratar de conseguir pruebas del hecho denunciado. La investigación concluirá con un informe, que será ser puesto a disposición de los órganos de la empresa con capacidad decisoria en materia laboral, con competencia para decidir sobre la eventual reparación que corresponde a la víctima y en su caso para trasladar la información a las autoridades administrativas o judiciales.

8. En el diseño del procedimiento la empresa debe declarar el compromiso de que, en caso de confirmar la veracidad de una denuncia, además de adoptar las medidas internas oportunas, pondrá los hechos en conocimiento de las autoridades y contactará con los potenciales perjudicados para reparar los daños ocasionados.
9. La empresa debe prever un plan de actuación que le permita corregir los mecanismos de control que puedan haber fallado e introducir de manera rápida los cambios necesarios para evitar que el hecho denunciado se vuelva a producir.
10. Un sistema interno de denuncia que reúna todas estas exigencias debería ser considerado por un juez penal como una medida eficaz de descubrimiento y prevención del delito. Ello no significa que, sólo por este hecho, el juez deba considerar que en cualquier delito cometido la empresa haya ejercido el debido control sobre su empleado o aplicar automáticamente el correspondiente atenuante del CP; pero en todo caso, una empresa que cuente con este procedimiento, además de otros medios preventivos adecuados, debería ser contemplada muy favorablemente para la aplicación de la ley lo más beneficiosa posible desde un punto de vista jurídico-penal.
11. Por todo lo expuesto, resulta de extrema importancia que tanto las investigaciones internas como los canales de denuncia confidencial, como mecanismos habituales de los sistemas de *Corporate Compliance*, se muestren escrupulosamente respetuosos con los derechos de los trabajadores.

## BIBLIOGRAFÍA:

- AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª ed., Pamplona, 2016.
- AA.VV., *Compliance. Cómo gestionar los riesgos normativos en la empresa*, coord. C.A. Sáiz Peña, Pamplona, 2015.
- AA.VV., *Estudios Jurídicos en memoria del profesor Emilio Beltrán. Liber Amicorum*, T. I, Valencia, 2015.
- AA.VV., *Gobierno corporativo: la estructura del órgano de gobierno y la responsabilidad de los administradores. Adaptado a la Ley 31/2014, de 3 de diciembre*, dir. A. Martínez-Echevarría, Pamplona, 2015.
- AA.VV., *Manual de cumplimiento penal en la empresa*, dir. A. Nieto Martín, edit. Tirant lo Blanch, Valencia 2015.
- AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014.
- AA.VV., *Responsabilidad de la Empresa y Compliance. Programas de prevención, detección y reacción penal*, dirs. S. Mir Puig, M. Corcoy y V. Gómez, Madrid, 2014.
- AA.VV., *Comentarios al Estatuto de los Trabajadores*, dir. A.V. Sempere, 9ª ed., Pamplona, 2013.
- AA.VV., *Criminalidad de empresa y compliance. Prevención y reacciones corporativas*, dir., J.M. Silva, Barcelona, 2013.
- AA.VV., *El Derecho penal económico en la era compliance*, Tirant lo Blanch, Valencia, 2013.
- AA.VV., *Supervisión en Seguros Privados. Hacia Solvencia II. Actas del Congreso de Ordenación y Supervisión en Seguros Privados*, dirs. V. Cuñat Edo, J. Bataller Grau, Colección Homenajes y Congresos, Valencia, 2013.

- AA.VV., *Cumplimiento normativo. Compliance*, Cuadernos de Derecho para Ingenieros, nº 14, dirs. M.A. Agúndez, J. Martínez-Simancas, Madrid, 2012.
- AA.VV., *Compliance und Strafrecht*, coords. Kuhlen/Kudlich/Ortiz de Urbina, C. F. Müller, Heidelberg, 2012.
- AA.VV., *El nuevo Código penal. Comentarios a la reforma*, dir. J.M. Silva Sánchez, La Ley, Madrid, 2012.
- AA.VV., *Comentarios al Código Penal Español*, dir. Quintero Olivares, 6ª ed., Aranzadi, Pamplona, 2011.
- AA.VV., *Dogmática penal de derecho penal económico y política criminal homenaje a Klaus Tiedeman*, coords. N. Salazar Sánchez y otros, 2 vols., Universidad de San Martín de Porres (USMP), Lima, 2011.
- AA.VV., *Estudios sobre las reformas del Código Penal, operadas por las LO 5/2010 de 22 de junio, y 3/2011, de 28 de enero*, dir. J. Díaz-Maroto y Villarejo, Madrid, 2011.
- AA.VV., *Ética empresarial y códigos de conducta*, dir. J.L. Goñi, Madrid, 2011.
- AA.VV., *Memento Penal Económico y de la Empresa*, coord., Ortiz de Urbina Gimeno, Francis Lefebvre, Madrid, 2011.
- AA.VV., *Responsabilidad penal de las personas jurídicas. Aspectos sustantivos y procesales*, Valencia, 2011.
- AA.VV., *Comentario a la Ley de Defensa de la Competencia*, dirs. J. Massaguer Fuentes, y otros, Pamplona, 2010.
- AA.VV., *Prevención de riesgos laborales. Instrumentos de aplicación*, coords. C. Alfonso Mellado, C. Salcedo Beltrán, e I. Rosat Aced, edits. Tirant lo Blanch, Valencia, 2010.
- AA.VV., *Derecho de la Libre Competencia Comunitario y Español*, coords. Bello Martín-Crespo, M.P. y Hernández Rodríguez, F, Pamplona, 2009.
- AA.VV., *Derecho de la empresa y protección de datos*, dir. A. Recalde, Thomson Aranzadi, Pamplona, 2008.

- AA.VV., *Manual de Derecho de la Competencia*, Tecnos, Madrid, 2008.
- AA.VV., *Trattato di diritto penale*, coords. Grosso/ Padovani/Pagliari, Giuffrè, Milano, 2008.
- AA.VV., *Fraude y corrupción en el Derecho penal económico europeo*, dirs. L. Arroyo Zapatero y A. Nieto Martín, edit. Universidad de Castilla-La Mancha, Cuenca, 2006.
- AA.VV., *¿Libertad económica o fraudes punibles? Riesgos penalmente relevantes e irrelevantes en la actividad económico-empresarial*, coord. J.M. Silva Sanchez, Madrid, 2003.
- AA.VV., "Privatizing regulation: whistleblowing and bounty hunting in the financial services industries", en *Journal of International Law*, vol. 19, 2000, pp. 117-143.
- AA.VV., *Derecho penal económico*, CGPJ, 2001.
- AA.VV., *Comentarios al Código penal*, dir. Cobo del Rosal, Edersa, Madrid, 1999.
- ABOGACÍA GENERAL DEL ESTADO. DIRECCIÓN DEL SERVICIO JURÍDICO DEL ESTADO, *Tratado de Derecho de la Competencia*, Aranzadi, Pamplona, 2013.
- ABRIANI, N., "La responsabilità da reato degli enti: modelli di prevenzione e linee evolutive del diritto societario", en *Analisi giuridica dell'economia*, Bologna, 2009.
- ACHENBACH, H., "Zurechnung unternehmensbezogenen Handelns", en AA.VV., *Handbuch Wirtschaftsstrafrecht*, coords. Achenbach, H./Ransiek, LL. M., edit. C.F. Müller, Heidelberg, 2004, pp. 18-38.
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Creación de denuncias internas en las empresas (mecanismos de *Whistleblowing*)", *Informe Jurídico*, nº 128, 2007.

- AGRAWAL, A./ CHADHA, S., "Corporate Governance and accounting scandals", *Journal of Law and Economics*, vol. XLVIII, 2005, pp. 371 y ss.
- AGUSTINA SANLLEHÍ, J. R., *El delito en la empresa*, Atelier, Barcelona, 2010.
- AGUSTINA SANLLEHÍ, J. R., "Estrategias y límites en la prevención del delito dentro de la empresa", *InDret Penal*, nº 2, 2009.
- ALCALÁ DÍAZ, M.A., "Las normas de gobierno corporativo de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de las entidades de crédito", *Revista La Ley mercantil*, nº 10, 2015, pp. 4-11.
- ALESSANDRI, "Reati colposi e modelli di organizzazione e gestione", en *Analisi giuridica dell'economia*, 2009.
- ALESSANDRI, *Diritto penale e attività economiche*, il Mulino, Bologna, 2010.
- ALFORD, C. F., *Whistleblowers: Broken Lives and Organizational Power*, Cornell University Press, Ithaca, New York, 2001.
- ALIAGA MÉNDEZ, J.A., *Normativa comentada de prevención del blanqueo de capitales*, edit. La Ley, Madrid, 2010.
- ALONSO ALONSO, E., "Los informes de cumplimiento normativo, Compliance", en AA.VV., *Cumplimiento normativo. Compliance*, Cuadernos de Derecho para Ingenieros, nº 14, dirs. M.A. Agúndez, J. Martínez-Simancas, Madrid, 2012, pp. 24 y ss.
- ALONSO DE ESCAMILLA, A., "La responsabilidad penal de los administradores de sociedades mercantiles. Una aproximación desde la perspectiva del compliance", en AA.VV., *Gobierno corporativo: la estructura del órgano de gobierno y la responsabilidad de los administradores. Adaptado a la Ley 31/2014, de 3 de diciembre*, dir. A. Martínez-Echevarría, Pamplona, 2015, pp. 881 y ss.
- ALONSO DE ESCAMILLA, A., *Responsabilidad penal de directivos y órganos de empresas y sociedades*, Tecnos, 1996.

- ALONSO GALLO, J., "Los programas cumplimiento", en *Estudios sobre las reformas del Código Penal, operadas por las LO 5/2010 de 22 de junio, y 3/2011, de 28 de enero*, dir. J. Díaz-Maroto y Villarejo, Madrid, 2011, pp. 144-199.
- ALVAREZ ALONSO, D. *La garantía de indemnidad del trabajador frente a represalias empresariales*, Alicante, 2005.
- ALVAREZ SAN JOSE, M., "La corrupción empresarial como conducta anticompetitiva. El papel armonizador de los programas de compliance en un mercado global", *RDM*, nº 301, 2016, pp. 143-172.
- AMELUNG, K., "Auf der Rückseite der Strafnorm. Opfer und Normvertrauen", en ARNOLD *et al.* (ed.), *Festschrift für Alhin Eser zum 70. Geburtstag - Menschengerechtes Strafrecht*, Beck, München, 2005, pp. 3-24.
- AMELUNG, K., "Bernerkung von Thomas Hillenkamp, Vorsatztat und Opferverhalten", *GA*, 1984, pp. 579-583.
- AMERICAN BAR ASSOCIATION SECTION OF ANTITRUST LAW, *Antitrust Compliance: Perspectives and Resources for Corporate Counselors*, Chicago, 2010.
- ANEIROS PEREIRA, J., "Las obligaciones de prevención del blanqueo de capitales a cargo de determinados profesionales: una fuente de información tributaria", *Revista Técnica Tributaria*, 2010, nº 91, pp. 25-65.
- ARGANDOÑA, A., " Compliance + ética, ¿por qué? (II)", Economía, Ética y RSE, IESE Blog Network, 11 de mayo de 2015. Extraído de: <http://blog.iese.edu/antonioargandona/2015/05/11/compliance-etica-por-que-ii>.
- ARGANDOÑA, A., "La compliance en la empresa", Extraído de: <http://blog.iese.edu/antonioargandona/2014/02/12/la-compliance-en-la-empresa/>



- ARIAS DOMÍNGUEZ, A./RUBIO SÁNCHEZ, F., *El derecho de los trabajadores a la intimidad*, Aranzadi, Pamplona, 2006.
- ARMENTIA MORILLAS, P., "Canal de Denuncias", en el capítulo "Plan de acción e implantación del Compliance Program. Plan de prevención, detección y reacción", en AA.VV., *Compliance. Cómo gestionar los riesgos normativos en la empresa*, coord. C.A. Sáiz Peña, Pamplona, 2015, pp. 610-641.
- ARTAZA VARELA, O., "Programas de cumplimiento. Breve descripción de las reglas técnicas de gestión del riesgo empresarial y su utilidad jurídico penal", en AA.VV., *Responsabilidad de la Empresa y Compliance. Programas de prevención, detección y reacción penal*, dirs. S. Mir Puig, M. Corcoy y V. Gómez, Madrid, 2014, pp. 231 y ss.
- ARTAZA VARELA, O., *La empresa como sujeto de imputación de responsabilidad penal. Fundamentos y límites*, Marcial Pons, Barcelona, 2013.
- ARZT, G., "Der Fall Siemens: Vom teuersten zum lukrativsten Fall der deutschen Geschichte", en Jahn/Kudlich/Streng (eds.), *Festschrift für Heinz Stöckel*, 2010.
- ARZT, G., "Viktimologie und Strafrecht", *Monatsschrift für Kriminologie und Strafrechtsreform*, 1984, pp. 105-124.
- AVGOULEAS, E., "The Reform of "Too-Big-To-Fall" Bank. A New Regulatory Model for the Institutional Separation of "Casino" from "Utility-Banking", *Draft Paper*, 2010. Extraído de: <http://ssrn.com/abstract=1552970>.
- AYALA, A. y IBARGUEN, G.S. "A Market Proposal for Auditing the Financial Statements of Public Companies". Extraído de: <http://www.webcitation.org/5tZ0THjI8>
- AYRES, I. /BRAITHWAITE, J., "Tripartism: Regulatory capture and empowerment", *Law and Social Inquiry* 16, 1991, pp. 435-496.

- AYRES, I./BRAITHWAITE, J., *Responsive Regulation: Transcending the deregulation Debate*, Oxford University Press, New York, 1992.
- BACIGALUPO ZAPATER, E., "Responsabilidad penal y administrativa de las personas jurídicas y programas de "compliance" (A propósito del Proyecto de reforma del Código Penal de 2009)", *Diario La Ley*, nº 7442, 2010.
- BACIGALUPO ZAPATER, E., *Compliance y Derecho penal*, Aranzadi, Pamplona, 2011.
- BAJO FERNANDEZ, M. / GOMEZ-JARA DIEZ, C., "Derechos procesales fundamentales de la persona jurídica", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª ed., Pamplona, 2016, pp. 313 y ss.
- BAJO FERNANDEZ, M., "Vigencia de la RPPJ en el Derecho sancionador español", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª ed., Pamplona, 2016, pp. 25 y ss.
- BALLBÉ, M., "El futuro del derecho administrativo en la globalización: entre la americanización y la europeización", *Revista de Administración Pública*, nº 174, 2007, pp. 215-276.
- BALLBÉ, M./ CABEDO, Y., "La necesidad de administraciones reguladoras en Latinoamérica para prevenir los ataques especulativos, los riesgos financieros y la defensa de los consumidores", *Revista del CLAD Reforma y Democracia*, nº 57, Caracas, 2013, pp. 1 y ss.
- BALLBÉ, M./ MARTÍNEZ, R., *Soberanía dual y constitución integradora. La reciente doctrina federal de la Corte Suprema norteamericana*, edit. Ariel Derecho, Barcelona, 2003.
- BALLBÉ, M./ MARTÍNEZ, R., "Law and Globalization: Between the United States and Europe", en AA.VV., *Global Administrative Law. Towards a Lex Administrativa*, dirs. J. Robalino- Orellana/ J. Rodríguez- Arana, pp. 137 y ss.

- BALLBÉ, M./ PADRÓS, C., *Estado competitivo y armonización europea*, edit. Ariel, Barcelona, 1997.
- BALLBÉ, M. "El futuro del derecho administrativo en la globalización: entre la americanización y la europeización", *Revista de Administración Pública*, núm. 174, 2007.
- BALDWIN, R./CAVE, M., *Understanding Regulation*, Oxford University Press, 1999.
- BANNENBERG, B. y otros, *Compliance: AufbauManagementRisikobereiche*, C.F. Müller, Hamburg, 2010.
- BARROS GARCIA, M., "Problemas derivados de la utilización del correo electrónico e internet en el ámbito laboral", *Actualidad Jurídica*, nº 8, 2004, pp. 51 y ss. Extraído de: <http://www.uria.com/documentos/publicaciones/1235/documento/trib04.pdf?id=2029>
- BASTIA, P., *Sistemi di pianificazione e controllo*, Il mulino, Bologna, 2008.
- BAYNES, L., "Just Pucker and Blow?", en "Analysis of Corporate Whistleblowers, the Duty of Care, the Duty of Loyalty, and the Sarbanes-Oxley Act", *St. John's Law Review*, vol. 76, nº 4, 2002.
- BENSTON, G.J., "The Quality of Corporate Financial Statements and Their Auditors before and after Enron", *Policy analysis*, 2003. Extraído de: <http://www.webcitation.org/5tZ00qlbE>
- BENZ, M., *Selbstbelastungen in außserstrafrechtlichen Zwangslagen*, 2005.
- BETHEL, J. E./FERRELL, A./HU, G., "Legal and Economic Issues in Litigation Arising From 2007-2008 Credit Crisis", en *Prudent Lending Restored: Securitization after the Mortgage Meltdom*, **edits**. Y. Fuchita /R. Herring/ R. Litan, Washington, 2009, pp. 163-235.
- BJØRKELO, B./ HØIVIK BYE, H., "On the appropriateness of research design: Intended and actual whistleblowing", en AA.VV., *International Handbook*

- on *Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 133 y ss.
- BJØRKELO, B./ MADSEN, O.J., "Whistleblowing and neoliberalism: Political resistance in late capitalism economy" en *Psychology and Society*, nº 5, 2013, pp. 28-40.
- BLANCO CORDERO, I., "La prevención del blanqueo de capitales", en AA.VV., *Manual de cumplimiento penal en la empresa*, dir. A. Nieto Martín, Valencia, 2015, pp. 433-435.
- BLANCO CORDERO, I., "Las personas expuestas políticamente (PEP). Riesgo de blanqueo para los sujetos obligados", en *Lavagem de capitais e sistema penal. Contribuições hispano-brasileiras a questões controvertidas*, edit. C. de Carli, 2014.
- BLANCO CORDERO, I., "Eficacia del sistema de prevención del blanqueo de capitales. Estudio del cumplimiento normativo (compliance) desde una perspectiva criminológica", *Eguzkilore. Cuaderno del Instituto Vasco de Criminología*, nº 23, 2009, pp. 117-138.
- BLANCO CORDERO, I., "La confidencialidad de la identidad de los empleados de las instituciones financieras", Parte I y II, en *INFOLAFT*, nº 37 y 38, 23 de mayo y 3 de julio de 2012, Bogotá (Colombia).
- BLANCO CORDERO, I., *El delito de blanqueo de capitales*, 3ª ed., Pamplona, 2012.
- BLUMENBER, A.D., "Retos prácticos de la implementación de programas de cumplimiento normativo", en AA.VV., *Responsabilidad de la empresa y compliance. Programas de prevención, detección y reacción penal*, dir. S. Mir, M. Corcoy, V. Gomez, Madrid, 2014, pp. 273-300.
- BOCK, D., "Stand der strafrechtswissenschaftlichen Compliance-Diskussion in Deutschland", en *Wissenschaftliche und praktische Aspekte der nationalen und internatiolen Compliance-Disleussion*, coord. T. Rotsch, Nomos, Baden-Baden, 2012, pp. 63-76.

- BOCK, D., "Strafrechtliche Aspekte der Compliance-Diskussion – § 130 OWiG als zentrale Norm der Criminal Compliance, *ZIS*, nº 2, 2009, pp, 68 y ss.
- BOCK, D., *Criminal Compliance*, Nomos, Baden-Baden, 2011.
- BONILLA BLASCO, "Los efectos jurídicos del correo electrónico en el ámbito laboral (Comentario a la STSJ Madrid del 23 de abril de 2001)", *RL*, nº 13, 2001.
- BOSUA, R. / MITTON, S. / DREYFUS, S. / LEDERMAN, R., Going public: Researching external whistleblowing in a new media age", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 250 y ss.
- BOWDEN, P., "A Comparative Analysis of Whistleblower Protection. Australian Association for Professional and Applied Ethics", 12th *Annual Conference, Adelaida*, Australia, 2005 pp. 10-11.
- BOWMAN, D./GILLIGAN, G., "Self-Regulation by Industry. Sufficient to Protect the Consumer, the Company and the Technology", *Conference on Nanotech Regulatory Policy, University of California at Los Angeles*.  
Extraído de:  
<http://www.cnsi.ucla.edu/NanoRegulatoryPolicy/pdfs/bowman.pdf>.
- BRAITHWAITE, J., "Enforced Self-Regulation: A New Strategy for Corporate Crime Control", *Michigan Law Review* 80, 1982.
- BRATTON, W.W., "Enron and the Dark Side of Shareholder Value", *Tulane Law Review*, May 2002, Forthcoming. Extraído de:  
<http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1508&context=facpub>
- BROWN, A.J./ MEYER, D. P./ WHEELER, C./ ZUCKERMAN, J. "Whistleblower support in practice: Towards an integrated research model", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 457 y ss.

- BUCHERT, C./JACOB-HOFBAUER,C "Hinweisgebersysteme des Unternehmens", en *Internal Investigations. Ermittlungen im Unternehmen*, eds. Knierim/Rübenstahl/Tsambikakis, C. F. Müller, Heidelberg et. al. nº 39, 2013.
- BUCY, P. H., "Corporate criminal liability: When does it make sense?", *American Criminal Law Review*, nº 46, 2009, pp. 1437-1457.
- BÜHRER, R., "Einrichtung einer internen Untersuchungsabteilung und deren Prozesse", en AA.VV., *Inteme Untersuchungen. Praxisleitfaden für Untemehmen*, dirs. Moosmayer/Hartwig, edit. C. H. Beck, Munich, 2012, pp. 101 y ss.
- BUSCH, R.J., "Stimulating Corporate Self-Regulation-The Corporate Self Evaluating Privilege", *Northwestern University Review*, nº 87, 1992-1993.
- BUSEKIST, K. /HEIN, O., "Der IDW PS 980 und die allgemeinen rechtlichen Mindestanforderungen an ein wirksames Compliance Management System (1) Grundlagen, Kultur und Ziele", *CCZ*, nº 2, 2012, pp. 41-48.
- BUSH, J.K. y otros, *Antitrust Law Strategies. Leading Lawyers on Best Practices for Compliance, M & A Transactions and Litigation Proceedings*, Aspatore Books, Boston, 2007.
- BUSSMANN, K./SALVENMOSER, S., "Der Wert von Compliance und Unternehmenskultur", *CCZ*, nº 5, 2008.
- CALDERÓN MARTIN, J., "Compliance en la normativa sectorial", AA.VV., *Compliance. Cómo gestionar los riesgos normativos en la empresa*, coord. C.A. Sáiz Peña, Pamplona, 2015, pp. 483 y ss.
- CALDERÓN, R./ FERRERO, I./ REDIN, D., "Ethical Codes and Corporate Responsibility of the Most Admired Companies of the World: Toward a Third Generation Ethics?", *D. Business and Politics*. Vol. 14 (4), 2012, pp. 1-24.
- CALLAHAN, E.S./ DWORKIN, T.M./ FORT, T.L. /SCHIPANI, C.A., "Integrating Trends in Whistleblowing and Corporate Governance: Promoting

- Organizational Effectiveness, Societal Responsibility, and Employee Empowerment", *American Business Law Journal*, vol. 40, 2002, pp. 177-215.
- CALLAHAN, E.S./ MOREHEAD, T., "Do Good and Get Rich: Financial Incentives for Whistleblowing and the False Claim Act", *Villanova Law Review*, 37, 1993.
- CALLAHAN, E.S./ DWORKIN T.M./ LEWIS, D. "Whistleblowing: Australian, U.K., and U.S. Approaches to Disclosure in the Public Interest", *Virginia Journal of International Law*, nº 880, 2003-2004.
- CALVO GALLEGO, F.J., "Códigos de conducta y obligaciones éticas de los trabajadores: Análisis jurídico" en AA.VV., *Ética empresarial y Códigos de conducta*, dir. J.L. Goñi, Madrid, 2011, pp. 263-317.
- CANCIO MELIÁ, M., *Conducta de la víctima e imputación objetiva en Derecho penal*, 2ª ed., Bosch, Barcelona, 2001.
- CARDONA RUBERT, B., "El derecho a la intimidad en la relación laboral", *Ius et Praxis*, año 4, 1998, pp. 107-134.
- CARUSO, A., "Leniency Programmes and Protection of Confidentiality: The Experience of the European Commission" en *Journal of European Competition Law & Practice*, vol. 1, nº 6, 2010, pp. 453-477.
- CASANOVAS YSLA, A., *Legal compliance. Principios de cumplimiento generalmente aceptados*, Madrid, 2012.
- CASTILLO PLAZA, C. A., "Transposición e implementación de la directiva 2009/138/CE (SOLVENCIA II)", en AA.VV., *La reforma del derecho del seguro*, dirs. J. Bataller Grau, M.R. Quintans Eiras y A.B. Veiga Copo, Pamplona 2015, pp. 305 y ss.
- CASTIÑEIRA, Mª T./ LLOBET, M./ MONTANER, R., "Accidentes de trabajo, medidas de seguridad y concurrencia de culpas: criterios jurisprudenciales", *InDret Penal*, 2005.

- CAVICO, F., "Private sector whistleblowing and the employment-at-will doctrine: A comparative legal, ethical and pragmatic analysis" en *South Texas Law Review*, nº 45, 2004, pp. 543-645.
- CHAMBERS, A., *Corporate Governance Handbook*, IDDAS, 5ª ed. 2012.
- CHAN, S. "Sarbanes Oxley". Ed. Risk Books, 2006, p. 1 y ss.
- CHERRY, "Whistling in the Dark? Corporate Fraud, Whistleblowers, and the Implications of the Sarbanes-Oxley Act for Employment Law", *Washington Law Review Association*, nº 79, 2004.
- CLARK, A., "Lehman whistleblower lost his job weeks after raising alarm". *The Guardian*. 2010, March 16, Extraído de <https://www.theguardian.com/business/2010/mar/16/lehman-whistleblower-auditors-matthew-lee>
- CLARK, R., "Los cambios en el Gobierno Corporativo tras la Sarbanes-Oxley Act: una historia con moraleja también para el legislador", en *Gobierno Corporativo y crisis empresariales*. II seminario Harvard-Complutense de Derecho mercantil, edit. Marcial Pons, Madrid, 2006, pp. 16 y ss.
- COFFEE, J. F., *Gatekeepers. The professions and corporate governance*. Oxford, 2006.
- COFFEE, J. C., Jr, "What Caused Enron - A Capsule Social and Economic History of the 1990s", *Cornell Law Review*, vol. 89, Issue, 2004, pp. 268 y ss.
- COFFEE, J. C., Jr, "Beyond the shut-eyed sentry: toward a theoretical view of corporate misconduct and an effective legal response", *Virginia Law Review*, vol. 63, nº 7, pp. 1099-1278.
- CONDE MARIN, E., *La buena fe en el contrato de trabajo. Un estudio de la buena fe como elemento de integración del contrato de trabajo*, 2007.
- CORTINA ORTS, A., "La ética en los negocios", *Auditoría Interna*, nº 105, 2014, pp. 36-37.



- CORTINA, A., *Ética De La Empresa. Claves Para Una Nueva Cultura Empresarial (Estructuras y Procesos. Filosofía)*, 7ª ed., Trotta, Madrid, 2013.
- CRAGG, W., *Ethics Codes, Corporations and the Challenge of Globalization*, Edwar Elgar, Northampton, 2005.
- CRESPO RODRÍGUEZ, M, /ZAFRA JIMÉNEZ, A., *Transparencia y buen gobierno: su regulación en España*, La Ley, Madrid, 2005.
- CULP, "Whistleblowers: Corporate Anarchists or Heroes? Towards a Judicial Perspective", *Hofstra Labor Law Journal*, nº 13 (1995-1996).
- DAHL RENDTARFF, J., *Responsibility Ethics and Legitimacy of Corporations*, Copenhagen Business School Press, 2009.
- D'ARCANGELO, F. "I canoni di accertamento della idoneità del modello organizzativo nella giurisprudenza", en *La responsabilità amministrativa delle società e degli enti*, nº 2, 2011.
- DARNACULLETA 1 GARDELLA, M<sup>a</sup> M., *Autorregulación y Derecho Público: La autorregulación regulada*, Marcial Pons, Madrid, 2005.
- DE CLEYN, SH. "Compliance of Companies with Corporate Governance Codes: Case Study and Listed Belgian SMEs", en *Journal of Business Systems, Governance and Ethics*, nº 1, 2008, pp. 2 y ss.
- DE FELICE, P. *La responsabilità da reato degli enti collettivi*, Cacucci, Bari, 2002.
- DE MAGLIE, C. *L'etica e il mercato. La responsabilità penale delle società*, Giuffré, Milano, 2002.
- DE SIMONE, G. "I profili sostanziali della responsabilità c.d. amministrativa degli enti: la 'parte generale' e la 'parte speciale' del d.lgs. 8 giugno 2001, n. 231", en Garuti (ed.), *Responsabilità degli enti per illeciti amministrativi dipendenti da reato*, Cedam, Padova, 2002.

- DE SIMONE, G. "Il 'fatto di connessione' tra responsabilità individuale e responsabilità corporativa", en *Rivista trimestrale di diritto penale dell'economia*, 2011.
- ESTEVE PARDO, J. "Autoregulación: Génesis y efectos", Aranzadi. 2012.
- DE VERO, G. "Il progetto di modifica della responsabilità degli enti tra originarie e nuove aporie", en *Diritto penale e processo*, 2010.
- DE VERO, G. "La responsabilità penale delle persone giuridiche", AA.VV., *Trattato di diritto penale*, coords. Grosso/ Padovani/Pagliaro, Giuffré, Milano, 2008.
- DEVINE, T. / MAASSARANI, T.F., *The Corporate Whistleblower's Survival Guide*. Berret-Koehle. 2011.
- DÍAZ RUIZ, E./ RUIZ BACHS, S., "Transposición de MiFID en España", en *Actualidad Jurídica Uría Menéndez*, nº 19, 2008, extraído de <http://www.uria.com/documentos/publicaciones/1924/documento/articuloUM.pdf?id=3171>
- DIEZ RIPOLLÉS, J. L., "La responsabilidad penal de las personas jurídicas. Regulación española", *InDret*, 1/2012.
- DONALDSON, T./DUNFEE, T.W., *Ties that Bind. A Social Contracts Approach to Business Ethics*. Harvard Business School Press. Boston. 1999.
- DOPICO GÓMEZ-ALLER, J., "Posición de garante del *compliance officer* por infracción del deber de control: una aproximación tópica", en AA.VV., *El Derecho penal económico en la era compliance*, Tirant lo Blanch, Valencia, 2013.
- DOPICO GÓMEZ-ALLER, J., "Responsabilidad de personas jurídicas", en AA.VV., *Memento Experto Reforma Penal. LO 5/2010*, coord. Ortiz de Urbina Gimeno, Francis Lefebvre, Madrid 2010, pp. 11-38.
- DREW, K., "Whistleblowing and Corruption". *An Initial and Comparative Review*. Public Services International Research Unit, University of Greenwich, Londres, 2003, pp. 54 y ss.

- DWORKIN, T.M. y CALLAHAN, E. S., "Employee disclosures to the Media: When is a 'source' a 'sourcerer'?" en *Hasting Communication and Entertainment Law Journal*, Vol. 15, 1993, pp. 357-397.
- DWORKIN, T.M. y CALLAHAN, E.S., "Do good and get rich: Financial incentives for whistleblowing and the False Claim Act" en *Villanova Law Review*, Vol. 37, 1992, pp. 273-336.
- ECKENBERGER, W., "Interne Untersuchungen bei Kartellrechtsverstößen" en MOOSMAYER, K. y HARTWIG, N. (Edits.), *Interne Untersuchungen. Praxisleitfaden für Unternehmen*. Múnich, 2012, pp. 139-157.
- EIRANOVA ENCINAS, E., "La responsabilidad penal de la persona jurídica", en AA.VV., *Gobierno corporativo: la estructura del órgano de gobierno y la responsabilidad de los administradores. Adaptado a la Ley 31/2014, de 3 de diciembre*, dir. A. Martínez-Echevarría, Pamplona, 2015, pp. 857 y ss.
- EISELE, J., *Compliance und Datenschutzstrafrecht. Strafrechtliche Grenzen der Arbeitnehmerüberwachung*, Nomos, 2012.
- EMBED IRUJO, J.M./ DEL VAL TALENS, P., *La responsabilidad social corporativa y el Derecho de sociedades de capital: entre la regulación legislativa y el soft law*, Madrid, 2016.
- ESPINO GARCÍA, M.G., "Fundamentos de la Ley Sarbanes-Oxley", Ed. IMCP, 20 de abril de 2017, p. 20
- ESTEVE PARDO, J., *Autorregulación. Génesis y efectos*, Aranzadi, Pamplona, 2002.
- ESTRADA I CUADRAS, A./ LLOBET ANGLI, M., "Derecho de los trabajadores y deberes del empresario: conflicto en las investigaciones empresariales internas", en AA.VV., *Criminalidad de empresa y compliance. Prevención y reacciones corporativas*, dir., J.M. Silva, Barcelona, 2013, pp. 197 y ss.

ETHICS RESOURCE CENTER: "2011 National Business Ethics Survey".

Extraído de: <http://www.ethics.org>.

FASTERLING, B., "Whistleblower protection: A comparative law perspective", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 331 y ss.

FATEH-MOGHADAM, "Criminal Compliance ernstgenommen -zur Garantenstellung des Compliance-Beauftragten", en Steinberg/Valerius/Popp (eds.), *Das Wirtschaftsstrafrecht des StGB*, 2011.

FAUNCE, T./ CROW, K. / NIKOLIC, T./ MORGAN, F. M. Jr., "Because they have evidence: Globalizing financial incentives on for corporate fraud whistleblowers", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 381 y ss.

FEIJOO SANCHEZ, B. J., "El art. 129 como complemento de la responsabilidad penal de las personas jurídicas", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª Ed., adaptada a la Ley 1/2015, de 30 de marzo, por la que se modifica el Código Penal, Pamplona, 2016, pp. 301 y ss.

FEIJOO SANCHEZ, B. J., "La extinción de la responsabilidad penal de las personas jurídicas", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª Ed., adaptada a la Ley 1/2015, de 30 de marzo, por la que se modifica el Código Penal, Pamplona, 2016, pp. 297 y ss.

FEIJOO SANCHEZ, B. J., "La persona jurídica como sujeto de imputación jurídico-penal", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª ed., adaptada a la Ley 1/2015, de 30 de marzo, por la que se modifica el Código Penal, Pamplona, 2016, pp. 55 y ss.

FEIJOO SANCHEZ, B. J., "Las características básicas de la responsabilidad penal de las personas jurídicas en el Código Penal español", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª ed.,

- adaptada a la Ley 1/2015, de 30 de marzo, por la que se modifica el Código Penal, Pamplona, 2016, pp. 67 y ss.
- FEIJOO SANCHEZ, B. J., "Las consecuencias jurídicas del delito", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª ed., adaptada a la Ley 1/2015, de 30 de marzo, por la que se modifica el Código Penal, Pamplona, 2016, pp. 273 y ss.
- FEIJOO SANCHEZ, B. J., "Los requisitos del art. 31 bis 1", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª ed., adaptada a la Ley 1/2015, de 30 de marzo, por la que se modifica el Código Penal, Pamplona, 2016, pp. 75 y ss.
- FERNÁNDEZ RODRÍGUEZ, J.J., De la condicionalidad social y los Acuerdos marco internaciones, sobre la evolución de la responsabilidad social empresarial (Fundación Justicia Social, Thomson Reuters Aranzadi), Navarra, 2012.
- FERNANDEZ-SORDO LLANEZA, E., "El gobierno corporativo de las entidades financieras ante la crisis económica", en AA.VV., Crisis y reforma del sistema financiero, coords. A.J. Recalde Castells, I. Tirado Martí y A. B. Perdices Huetos, Pamplona, 2014, p. 293.
- FIANDACA, G. /MUSCO, E., *Diritto penale, parte generale*, 6ª ed., Zanichelli, Bologna, 2010.
- FIRST, H., "Branch office of the prosecutor: the new role of the corporation in business crime prosecutions", *North Carolina Law Review*, nº 24, 2011, pp. 23-98.
- FLICK, "Le prospettive di modifica del d.lg. n. 231/2001, in materia di responsabilità amministrativa degli enti: un rimedio peggiore del male?", en *Cassazione penale*, 2010.
- FOFFANI, L., "Escándalos económicos y reformas penales: prevención y represión de las infracciones societarias en la era de la globalización", *Revista Penal*, nº 23, 2009, pp. 35 y ss.;

- FORO ASEGURADOR DE CUMPLIMIENTO, *La función de verificación de cumplimiento, Revista Española de Seguros*, nº 7 monográfico, 2016.
- FOX, T., *Best Practices Under the FCPA and Bribery Act*. 2013.
- FRANCÉS, P./ BORREGO, A./ VELAYOS, C., *Códigos éticos en los negocios. Creación y ampliación en empresas e instituciones*, Madrid, 2003.
- FRED ALFORD, C., *Whistleblowers. Broken lives and Organizational Power*. Cornell University Press. 2002.
- FREEMAN, R.E, *Strategic Management: A Stakeholder Approach*, Pitman Press, Boston, 1984.
- FRIEDMAN, A.L./ MILES, S., *Stakeholders: Theory and Practice*, Oxford University Press, 2006.
- FRIEDRICHS, D., "Enron et al.: Paradigmatic White Collar Crime Cases for the New Century", *Critical Criminology*, vol. 12, 2004, pp. 114 y ss.
- FRITZ, H.J./NOLDEN, D., Unterrichtungspflichten und Einsichtrechte des Arbeitnehmers im Rahmen von unternehmensinternen Untersuchungen, CCZ, 5/2010.
- FROTSCHER, *Kommentar zum Einkommensteuergesetz* (Stand: 11/2011), § 4 EStG.
- GARCIA MORENO, B., "Whistleblowing y canales institucionales de denuncia", en AA.VV., *Manual de cumplimiento penal en la empresa*, dir. A. Nieto Martín, Valencia, Tirant lo Blanch, 2015, pp. 206-230.
- GARCIA-NUÑEZ SERRANO, F., "La regulación sobre la protección de datos personales y su incidencia en el ámbito laboral", *Aranzadi Social*, nº. 21, 2001, pp. 1105 y ss.
- GARGANI, "Delitti colposi commessi con violazione delle norme sulla tutela della sicurezza sul lavoro: responsabile 'per definizione' la persona giuridica?", en *Studi in onore di Mario Romano*, Vol. II, Napoli, 2011.

- GARRETT, J., *Antitrust Compliance: A Legal and Business Guide*, Practising Law Institute, New York, 1978.
- GASCÓN INCHAUSTI, F., *Proceso penal y persona jurídica*, Marcial Pons, Madrid, 2012.
- GENTILE, *L'illecito colposo dell'ente collettivo*, Giappichelli, Torino, 2009.
- GERKE/RICHTER, "Die Vertretung von Arbeitsgebern in (Arbeits-) Strafverfahren", en Gerke/Kraft/Richter, *Arbeitsstrafrecht. Strafrechtliche Risiken und Risikomanagement*, C. F. Müller, Heidelberg et. al., 2012, nm. 104.
- GERST, H.J., Unternehmensinteresse und Beschuldigtenrechte bei Internal Investigations, CCZ 1/2012.
- GIARDA/SPANGHER (eds.), *Codice di procedura penale commentato*, Giuffrè, Milano, 2010.
- GILBERT W. J. *Sarbanes-Oxley For Dummies*, 2ª ed., Indianapólis, 2008.
- GIMÉNEZ-SALINAS COLOMER, E. "Delincuencia juvenil y control social". Barcelona, 1981.
- GLAZER, M.P. y GLAZER, P.M., *The whistleblowers. Exposing corruption in Government and industry*. Basic Book, Inc. New York. 1989.
- GLOBAL LEGAL GROUP (edit.), *The International Comparative Legal Guide to Cartels & Leniency 2011. A practical cross-border insight into cartels and leniency*. London, 2010.
- GOBERT, J./ PUNCH, M., "Whistleblowers, the Public Interest, and the Public Interest Disclosure Act 1998" en *The Modern Law Review*, vol. 63, January 2000, pp. 25-54.
- GOMEZ MARTIN, V., "Compliance y derechos de los trabajadores", en AA.VV., *Compliance y teoría del Derecho penal*, eds. L. Kuhlen, J.P. Montiel, I. Ortiz de Urbina, Madrid, 2013, pp. 125-146.
- GOMEZ MARTÍN, V., "Compliance y derechos de los trabajadores", en AA.VV., *Responsabilidad de la Empresa y Compliance. Programas de*

- prevención, detección y reacción penal*, dirs. S. Mir Puig, M. Corcoy y V. Gómez, Madrid, 2014, pp. 421 y ss.
- GÓMEZ POMAR, F./ ORTIZ DE URBINA GIMENO, I., *Chantaje e intimidación: un análisis jurídico-económico*, Civitas, Navarra, 2005.
- GOMEZ TOMILLO, M., *Introducción a la responsabilidad penal de las personas jurídicas en el sistema español*, 2ª ed., Madrid, 2015.
- GOMEZ-JARA DIEZ, C., "Fundamentos de la responsabilidad penal de las personas jurídicas", en AA.VV., *Responsabilidad penal de las personas jurídicas. Aspectos sustantivos y procesales*, Valencia, 2011.
- GÓMEZ-JARA DIEZ, C., "Aspectos sustantivos relativos a la responsabilidad penal de las personas jurídicas", en *Responsabilidad penal de las personas jurídicas: aspectos sustantivos y procesales*, La Ley, 2011.
- GOMEZ-JARA DIEZ, C., "Fundamentos de la responsabilidad penal de las personas jurídicas", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª Ed., adaptada a la Ley 1/2015, de 30 de marzo, por la que se modifica el Código Penal, Pamplona, 2016, pp. 89 y ss.
- GOMEZ-JARA DIEZ, C., "El injusto típico de la persona jurídica (tipicidad)", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª ed., Pamplona, 2016, pp. 121 y ss.
- GOMEZ-JARA DIEZ, C., "La culpabilidad de la persona jurídica", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª ed., Pamplona, 2016, pp. 143 y ss.
- GOMEZ-JARA DIEZ, C., "La atenuación de la responsabilidad penal de las personas jurídicas", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª ed., Pamplona, 2016, pp. 221 y ss.
- GOMEZ-JARA DIEZ, C., "Auditoría y participación en la responsabilidad penal de las personas jurídicas", en AA.VV., *Tratado de responsabilidad penal de las personas jurídicas*, 2ª ed., adaptada a la Ley 1/2015, de 30 de



marzo, por la que se modifica el Código Penal, Pamplona, 2016, pp. 251 y ss.

GÓMEZ-JARA DIEZ, C., "El sistema de responsabilidad penal de las personas jurídicas en el nuevo Código penal español", en AA.VV, *El nuevo Código penal. Comentarios a la reforma*, dir. J.M. Silva Sánchez, La Ley, Madrid, 2012, pp. 43-102.

GÓMEZ-JARA DIEZ, C., "Responsabilidad penal de las personas jurídicas y contratación pública. A propósito de la nueva directiva Europea sobre contratación pública", *La Ley* nº 8175, 2014, pp. 125 y ss.

GÓMEZ-JARA DIEZ, C., *La responsabilidad penal de las empresas en los EE.UU.*, Fundación Ramón Areces, Sevilla, 2006.

GONZALEZ DE LEON BERINI, A., "El criminal compliance en la reforma norteamericana de la Dodd-Frank Act", en AA.VV., *Criminalidad de empresa y compliance. Prevención y reacciones corporativas*, dir. J.M. Silva Sánchez, ed. Atelier, Barcelona, 2013, pp. 131-142.

GONZALEZ DE LEON BERINI, A., "El criminal compliance en la reforma norteamericana de la Dodd-Frank Act", en AA.VV., *Criminalidad de empresa y compliance. Prevención y reacciones corporativas*, dir. J.M. Silva, Barcelona, 2013, pp. 131 y ss.

GOÑI SEIN, J.L., "Sistemas de denuncia interna de irregularidades ("Whistleblowing")", AA.VV., *Ética empresarial y códigos de conducta*, dir. J.L. Goñi, Madrid, 2011, pp. 319 y ss.

GOÑI SEIN, J.L., "Programas de cumplimiento empresarial (Compliance programs): aspectos laborales", en AA.VV., *Responsabilidad de la Empresa y Compliance. Programas de prevención, detección y reacción penal*, dirs. S. Mir, M. Corcoy y V. Gómez, Madrid, 2014, pp. 367 y ss.

GOÑI SEIN, J.L., "Valor Jurídico de los códigos de conducta empresariales", AA.VV., *Ética empresarial y códigos de conducta*, dir. J.L. Goñi, Madrid, 2011, pp. 583 y ss.

- GOÑI SEIN, J.L., "Criminalidad de empresa, mecanismos de denuncia o 'whistleblowing' y protección de datos" AA.VV., *Derecho de la empresa y protección de datos*, dir. A. Recalde, Thomson Aranzadi, Pamplona, 2008, pp. 21-65.
- GOÑI SEIN, J.L., *El respeto a la esfera privada del trabajador: un estudio sobre los límites del poder de control empresarial*, Civitas, Madrid, 1988.
- GORDON, S. D., "Implementation of Effective Compliance and Ethics Programs and the Federal Sentencing Guidelines", AA.VV., *Corporate Compliance Answer Book*, edit. Practising Law Institute, 2016, pp. 29 y ss.
- GRAEFF, P./SCHRÖDER, K./ WOLF, S. (eds.), *Der Korruptionsfall Siemens. Analysen und praxisnahe Folgerungen des wissenschaftlichen Arbeitskreises von Transparency International Deutschland*, 2009.
- GREEN, B./PODGOR, E., Unregulated Internal Investigations: Achieving Fairness For Corporate Constituents, *Boston College Law Review*, vol. 54, 2013.
- GRUNER, R.S. *Corporate Criminal Liability and Prevention*, Law Journal Press, New York, 2010.
- GRUNER, R.S./ BROWN, L.M., "Organizational Justice: Recognizing and Rewarding the Good Citizen Corporation", *The Journal of Corporation Law*, vol. 21, 1996.
- HANNAY, WILLIAM M., *Designing an Effective Antitrust Compliance Program*, Thomson West, Chicago, 1996.
- HASSINK, H./ DE VRIES, M. / BOLLEN, L., "A Content Analysis of Whistleblowing Policies of Leading European Companies", *Journal of Business Ethics*, vol. 75, Issue 1, 2007, pp 25–44.
- HARTMAN, L./ ELM, D. /RADIN, T./ POPE, K.R., "Translating Corporate Culture around the World: A cross-cultural analysis of whistleblowing as an example of how to say and do the right thing" *Politeia: Corporate and*

- Stakeholder Responsibility Theory and Practice*, Vol. Anno XXV Iss. N° 93, 2009, pp. 255-272.
- HAUSCHKA, CH. E. (edit.), *Corporate Compliance. Handbuch der Haftungsvermeidung im Unternehmen*, C.H. Beck, München, 2010.
- HAUSCHKA, CH. E., "Die Voraussetzungen für ein effektives Compliance System i.S. von § 317 Abs. 4 HGB", *Der Betrieb*, n° 21, 2006, pp. 1143-1146.
- HEALTH and SAFETY EXECUTIVE, "Risk assessment, A brief guide to controlling risks in the workplace". Extraído de: [www.hse.gov.uk/pubns/indg163.htm](http://www.hse.gov.uk/pubns/indg163.htm).
- HECHLER BAER, M., "Governing Corporate Compliance", *Boston College Law Review*, vol. 50, 2009, pp. 4 y ss.
- HEFENDEHL, R., "Enron, WorldCom, and the Consequences: Business Criminal Law Between Doctrinal Requirements and the Hopes of Crime Policy", *Buffalo Criminal Law Review*, vol. 8, 2005, pp. 51 y ss.
- HEFENDEHL, R., "Alle lieben Whistleblowing", en BÖSE/STERNEBERG-LIEBEN (eds.), *Grundlagen des Straf-und Strafverfahrensrechts. Festschrift für Knut Amelung*, Berlín, 2009, pp. 617-643.
- HELMER, J., *False Claim Act: Whistleblower Claim Act: Whistleblower Litigation*, 3ª ed. Charlottesville. Lexis Nexis. 2002.
- HEMPHILL, T./CULLARI, F., "Corporate Governance Practices: A Proposed Policy Incentive Regime to Facilitate Internal Investigations and Self-Reporting of Criminal Activities", en *Journal of Business Ethics*, n° 87, 2009, p. 334.
- HERMANNNS, F./KLEIER, U., *Grenzen der Aufsichtspflicht in Betrieben und Unternehmen*, Heymann, Köln-Berlin- Bonn- München, 1987.
- HILLENKAMP, TH., *Vorsatztat und Opferverhalten*, Göttingen, Otto Schwarz, 1981.

- HOLDER, E., memorándum sobre *Bringing Criminal Charges Against Corporations*, de 16 de junio 1999. Extraído de: <http://www.justice.gov/criminal/fraud/documents/reports/1999/char-ging-corps.PDF>.
- HUFF, K. "*The Role of Corporate Compliance Programs in Determining Corporate Criminal Liability: A Suggested Approach*", *Columbia Law Review*, vol. 96, 1996.
- HUTTER, B. "*Compliance Regulation and environment*". Clarendon Press, 1997.
- INFORME COSO, *Los nuevos conceptos del control interno (Informe Coso)*, Coopers & Lyband, 1997.
- JAHN, M. "*Ermittlungen in Sachen Siemens/ SEC*", en *StV*; n° 1, 2009, pp. 45 y ss.
- JAKOBS, G., *Estudios de Derecho penal*, Civitas, Madrid, 1997.
- JAREÑO LEAL, A., *Las amenazas y el chantaje en el Código Penal de 1995*, Tirant lo Blanch, Valencia, 1997.
- JOHNSON, R. A., *Whistleblowing. When it Works and why*, London, 2003.
- JORGE BARREIRO, A., "Del descubrimiento y revelación de secretos", en AA.VV., *Comentarios al Código penal*, dir. Cobo del Rosal, Edersa, Madrid, 1999, pp. 109 y ss.
- JUBB, P., "Whistleblowing: A restrictive Definition and Interpretation", *Journal of Business Ethics*. n° 74.
- KAHLWNBURG, H./ SCHWINN, H., "Amnestieprogramme bei Compliance Untersuchungen in Unternehmen", *CCZ*, 3/2012.
- KAISER, G./ METZGER-PREGIZER, G. (eds.), *Betriebsjustiz*, 1976.
- KANZENBACH, K., *Die Implementierung und Ausgestaltung eines "best-practice" Hinweisgeberbzw. Whistleblower-Systems unter arbeitsrechtlichen Gesichtspunkten – Eine Handlungsempfehlung für Unternehmen*; Shaker Verlag, 2013.

- KAPLAN, S., "The words of Risk Analysis", *Risk Analysis an International Journal*, vol. 17, Issue 4, ed. Wiley Online Library, 1997, pp. 401- 523.
- KARBAUM, C., *Kartellrechtliche Compliance Rechtsgrundlagen und Umsetzung*, Peter Lang Verlag, Frankfurt am Main, 2010.
- KARST, A., "Kartellrechtscompliance im Konzern" en *Wirtschaft und Wettbewerb*, nº 2, 2012, pp. 150-156.
- KASTEN, B., "Kartellrechtscompliance" en MÄGER, T. (edit.), *Europäisches Kartellrecht*, Baden-Baden, 2011, pp. 81-142.
- KELLY, J., "The Year of the Whistle-Blowers", *Time*, nº 30, 2002.
- KINDHÄUSER, U., *Strafprozessrecht*, Nomos, Baden-Baden, 2006 (2ª ed.), § 1, nº 9; VOLK, *Grundkurs StPO*, 7ª ed., § 3, nm. 1, C. H. Beck, München, 2010.
- KNAUER, C."Interne Ermittlungen (Teil I)-Grundlagen", en *ZWH*, nº 2, p. 41, 2012.
- KNIERIM, T."Erfordernisse und Grenzen der Internal Investigations", en Rotsch (ed.), *Wissenschaftliche und praktische Aspekte der nationalen und internationalen Compliance-Diskussion*, pp. 85 y ss.
- KOCH, A., "Korruptionsbekämpfung durch Geheimnisverrat? Strafrechtliche Aspekte des Whistleblowing", *ZIS*, 2008, pp. 500-505.
- KOHN, S. M., *Concepts and Procedures in Whistleblowers Law*. Quorum Books, London, 2001.
- KOHN, S. M., *The Whistleblower's handbook. A step by step to Doing What's Right and Protecting Your Self*. Lyons Press. 2011.
- KOTZ, H. D., *Financial Regulation and Compliance. How to manage Competing and Overlapping Regulatory Oversight*, Edit. John Wiley & Sons, Inc, New York, 2015.
- KUHLEN. L., "Grundfragen von Compliance und Strafrecht", en Kuhlen, Kudlich y Ortiz de Urbina (coords.), *Compliance und Strafrecht*, C.F.

- Müller, Heidelberg-München-Landsberg-Frechen-Hamburg, 2013, pp. 1-25.
- KUHLEN, L., "Grundfragen von Compliance und Strafrecht", AA.VV., *Compliance und Strafrecht*, coords. Kuhlen, Kudlich y Ortiz de Urbina, C. F. Müller, Heidelberg, 2012, pp. 9 y ss..
- KUHLEN, L./ MONTIEL, J. P./ ORTIZ DE URBINA GIMENO, I., *Compliance y Teoría del Derecho Penal*. Marcial Pons. 2013.
- KUHLEN, L. "Compliance y derecho penal en Alemania", AA.VV., *Responsabilidad de la Empresa y Compliance. Programas de prevención, detección y reacción penal*, dirs. S. Mir Puig, M. Corcoy y V. Gómez, Madrid, 2014, pp. 89 y ss.
- KÜHNE, H., *Strafprozessrecht. Eine systematische Darstellung des deutschen und europäischen Strafverfahrensrechts*, 8ª ed., C. F. Müller, Heidelberg, 2010.
- LAHMAN LARRY, D., "Bad Mules, a primer of the Federal False Claim Act", *Oklahoma Bar Journal*, vol. 76, nº 12, 2005.
- LASCURAIN SÁNCHEZ, J. A., "Compliance, debido control y unos refrescos", en *El Derecho penal económico en la era compliance*, Tirant lo Blanch, Valencia, 2013.
- LAUFER, "Corporate Liability, Risk Shifting, and the Paradox of Compliance", *Vanderbilt Law Review*, vol. 52, 1999.
- LEWIS Y KENDER, "A Survey of Whistleblowing/Confidential Reporting Procedures in the Top 250 FTSE Firms". Manuscrito.
- LEWIS, D.S., *Compliance: A concise guide to the role of the Compliance Function in financial services firms*, Ed. Create Space Independent Publishing Platform, 2016.
- LEWIS, D. / BROWN, A.J./ MOBERLY, R., "Whistleblowing, its importance and the state of the research", en AA.VV., *International Handbook on*

- Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 1 y ss.
- LEWIS, D./ DEVINE, T./ HARPUR, P. "The key to protection: Civil and employment law remedies", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 350 y ss.
- LEYS, J. / VANDEKERCKHOVE, W., "Whistleblowing duties", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 115 y ss.
- LIÑAN LAFUENTE, A., "El control preventivo de la responsabilidad penal de las personas jurídicas", en AA.VV., *Cumplimiento normativo. Compliance*, Cuadernos de Derecho para Ingenieros, nº 14, dirs. M.A. Agúndez, J. Martínez-Simancas, Madrid, 2012, pp. 43 y ss.
- LOMAS, P. / KRAMER, J. D., *Corporate Internal Investigations. An International Guide*, 2ª ed., 2013.
- LÓPEZ BARJA DE QUIROGA, J., "Las escuchas telefónicas y la prueba ilegalmente obtenida". AKAL. 1989.
- LÓPEZ BARJA DE QUIROGA, J: "*Tratado de Derecho Penal*". Civitas Ediciones. 2010.
- LOUGHMAN, B.P. /SIBERY, R.A., *Bribery and Corruption. Navigating the Global Risks*, Wiley Corporate F&A, Kindle Edition, 2012.
- LOYENS, K. / MAESSCHALCK, J., "Whistleblowing and power", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 154 y ss.
- LOZANO AGUILAR, J. F., *Códigos éticos para el mundo empresarial*, Madrid, 2004.
- LUJAN ALCARAZ, J., "Uso y control en la empresa de los medios informáticos de comunicación", *Aranzadi Social*, nº 5, 2001, pp. 55 y ss.

- LUTTERBACH, C., "Die Strafrechtliche Würdigung des Whistleblowings", disertación (tesis doctoral) defendida en la Facultad de Derecho de la Universidad de Bremen (Alemania), el 27 de junio de 2011. Extraído de: <http://elib.suub.uni-bremen.de/edocs/00102123-1.pdf>.
- MARKOPOLOS, H., *No one would listen: A True Financial Thriller*, Wiley, 2010
- MARTIN BERNAL, J. M., *El abuso del Derecho*, Madrid, 1982.
- MARTIN, B. "Research that whistleblowers want and what they need", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 497 y ss.
- MARTÍNEZ, R. "*El Delegado de Prevención de Riesgos Ambientales*". Trabajo original de investigación para la oposición a Profesor Titular de Derecho Administrativo UAB, convocada por la Resolución de 8 de noviembre de 2001 (BOE 26 de noviembre de 2001).
- MARINEZ, R. "Armas: ¿Libertad americana o prevención europea?. Ariel 2002.
- MARTÍNEZ, R. "La intervención administrativa en el derecho a llevar armas". UAB, 2000.
- MARTÍNEZ ECHEVARRÍA/ GARCÍA DE DUEÑAS, A., *La propiedad de la empresa y el gobierno corporativo*, ed. CEU, 2009.
- MARTÍNEZ FONS, D., *El poder de control del empresario en la relación laboral*, 2002.
- MARTÍNEZ-CARANDE CORRAL, J. L., "La conservación de documentos en el nuevo reglamento de prevención del blanqueo de capitales. El artículo 29 del Real Decreto 304/2014, una puerta al caos documental", *Diario La Ley*, nº 8354, Sección Tribuna, 2014.
- MASCHMANN, F. "Vermeidung von Korruptionsrisiken aus Unternehmenssicht -Arbeits-und Zivilrecht, Corporate Governance-", en



- Benz/Dieners/Dölling *et. al.* (eds.), *Handbuch der Korruptionsprävention*, C. H. Beck, München, 2007, pp. 154 y ss.
- MATEU DE ROS CEREZO, R., *El Nuevo Código Unificado de Gobierno Corporativo*, Thomson-Aranzadi, Pamplona, 2007.
- MATHEWS, A. F., "Internal corporate investigations", *Ohio State Law Journal*, nº 45, 1984, pp. 655-702.
- MCDONALD, L. / ROBINSON, P., *A Colossal Failure of Common Sense: The Inside Story of the Collapse of Lehman Brothers*. Ebury press. 2009.
- McKENDALL, M./DEMARR, B./ RIKKERS, J. "Ethical Compliance Programs and Corporate Illegality: Testing the Assumptions of the Corporate Sentencing Guidelines", en *Journal of Business Ethics*, nº 37, 2002, p. 369.
- MCLEAN, B. / ELKIND, P., *The smartest guys in the room. The amazing rise and scandals fall of Enron*, New York, 2004.
- MCNULTY, P. J., memorándum on *Bringing Criminal Charges Against Corporations*, de 12 de diciembre de 2006, Extraído de: [http://www.justice.gov/dag/speeches/2006/mcnulty\\_memo.pdf](http://www.justice.gov/dag/speeches/2006/mcnulty_memo.pdf).
- MESIA MARTÍNEZ, C., "El procedimiento de denuncia interna o whistleblowing en los códigos de conducta", en AA.VV., *Gobierno corporativo: La estructura del órgano de gobierno y la responsabilidad de los administradores (Adaptado a la Ley 31/2014, de 3 de diciembre)*, obra colectiva dirigida por Alfonso Martínez- Echevarria y García de Dueñas, Navarra, 2015, pp. 1209-1252.
- MICELI, M./ NEAR, J./ POLLEX, J./ MOREHEAD, T., *Whistle-blowing in organizations*. Edit. Routledge. New York, 2008.
- MICELI, M. / DREYFUS, S. / NEAR, J., "Outsider 'whistleblowers': Conceptualizing and distinguishing 'bell-ringing' behavior", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 71 y ss.

- MICHELS, K., "Internal Corporate Investigations and the Truth", en *Seton Hall Law Review*, nº 40, 2010, pp. 84 y ss.
- MIR PUIG, S., "El principio de proporcionalidad como fundamento constitucional de límites materiales del Derecho penal", en *LH-Vives Anton*, II, 2009.
- MIR PUIG, S., *Derecho penal. Parte general*, 9ª ed., Barcelona, 2011.
- MIR PUIG/GOMEZ MARTIN, V., "Comentario al art. 20 CP", en Mir Puig/ Carcoy Bidasolo, *Comentarios al Código penal, LO 5/2010*, 2011.
- MIRÓ MORROS, D. " Los trabajadores como 'delatores': la importancia de la Sentencia del Tribunal Supremo de 17 de septiembre de 2015", *Actualidad Jurídica Aranzadi* nº 913, 2015, pp. 12 y ss.
- MOBERLY, R. / WYLIE, L., "An Empirical Study of Whistleblower Policies in United States Corporate Code of Ethics". Extraído de: <http://ssrn.com/>.
- MOBERLY, R., "To persons or organizations that may be able to effect action": Whistleblowing recipients", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 273 y ss.
- MOBERLY, R., "Sarbanes-Oxley's Structural Model to Encourage Corporate Whistleblower's". *BYU Law Review*. 2006.
- MOBLEY, S. /DENTON, R., *Global Leniency Manual*, Oxford, 2010.
- MOELLER, R., *Coso Enterprise Risk: Establishing Effective Governance, Risk, and Compliance Processes*, 2ª ed., Wiley Corporate F&A, 2011.
- MOLINA FERNÁNDEZ, F., "El estado de necesidad como ley general. (Aproximación a un sistema de causas de justificación)", *Revista de Derecho Penal y Criminología*, nº extraordinario 1º, 2000, pp. 199-260.
- MOMSEN, C., "Internal Investigations zwischen Mitwirkungspflicht und strafprozessuale Selbstbelastungsfreiheit", en *ZIS*, nº 6, 2011, p. 510.
- MONEREO PÉREZ, J.L., *Los derechos de información de los representantes de los trabajadores*, Civitas, Madrid, 1992.

- MONTANER FERNANDEZ, R., "La estandarización alemana de los sistemas de gestión de cumplimiento: implicaciones jurídico-penales", en AA.VV., *Criminalidad de empresa y Compliance. Prevención y reacciones corporativas*, dir. J.M<sup>a</sup> Silva Sanchez, Barcelona, 2013, pp. 143 y ss.
- MONTANER FERNÁNDEZ, R., *Gestión empresarial y atribución de responsabilidad penal. A propósito de la gestión medioambiental*, Atelier, Barcelona, 2008.
- MONTIEL, J. P., "Sentido y alcance de la investigaciones internas en la empresa", en AA.VV., *Responsabilidad de la Empresa y Compliance. Programas de prevención, detección y reacción penal*, dirs. S. Mir Puig, M. Corcoy y V. Gómez, Madrid, 2014, pp. 487 y ss.
- MONTOYA MELGAR, A., "Comentario al artículo 20", en AA.VV., *Comentarios al Estatuto de los Trabajadores*, dir. A.V. Sempere, 9<sup>a</sup> ed., Pamplona, 2013, pp. 220 y ss.
- MOOSMAYER, K., *Compliance. Praxisleitfaden für Unternehmen*, C.H. Beck, München, 2009.
- MOOSMAYER, K./ HARTWIG, N., *Interne Untersuchungen: Praxisleitfaden für Unternehmen*, Beck; München, 2012.
- MORALES PLAZA, A., *La regulación nuclear globalizada*, Madrid, 2009.
- MORALES PRATS, F., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en AA.VV., *Comentarios al Código Penal Español*, dir. Quintero Olivares, 6<sup>a</sup> ed., Aranzadi, Pamplona, 2011, pp. 1281-1356.
- MORALES PRATS, F., *La nueva responsabilidad penal de las personas jurídicas en la reforma del Código penal*, Estudios jurídicos, 2011.
- MORATO GARCIA, R. M., "Incumplimiento de los códigos de conducta y potestad disciplinaria del empresario", en AA.VV., *Ética empresarial y códigos de conducta*, dir. J.L. Goñi, Madrid, 2011 pp. 413-456.

- NORDBERG, D., *Corporate Governance: Principles and Issues*, SAGE Publications Ltd, London, 2011
- MORÓN LERMA, E., "El compliance officer: régimen y responsabilidad", en AA.VV., *Cumplimiento normativo. Compliance*, Cuadernos de Derecho para Ingenieros, nº 14, dirs. M.A. Agúndez, J. Martínez-Simancas, Madrid, 2012, pp. 68 y ss.
- MUCCIARELLI, F., "Una progettata modifica a1 D.Lgs. nº 231/01: la certificazione del modello come causa di esclusione della responsabilità", en *Le societa*, 2010.
- MUÑOZ, P. "Reforma Código Penal de 2015: planes de cumplimiento corporativo". Extraído de: <http://www.legaltoday.com/practica-juridica/penal/economico/reforma-codigo-penal-de-2015-planes-de-cumplimiento-corporativo>.
- MURPHY, D., "The Federal Sentencing Guidelines for Organizations: A Decade of Promoting Compliance and Ethics", *Iowa Law Review*, nº 87, 2002, pp. 697-719.
- MYERS, A., "Whistleblowing- The UK Experince", en AA.VV., *Whistleblowing Around The World: Law, Culture and Practice*, dirs. R. Calland y G. Dehn, London, 2004 pp. 101-118.
- NAVARRO GARCÍA, F., "Responsabilidad Social Corporativa: Teoría y práctica", ESIC Editorial, 17 de febrero de 2012, pp. 2 y ss.
- NEAR, J. y DWORKIN, T.M., "Responses to legislative changes: corporate whistleblowing policies" en *Journal of Business Ethics*, Vol. 17, Issue 14, 1998, pp. 1551-1561.
- NESTLER, N., "Internal Investigations: Definition und rechtstatsächliche Erkenntnisse zu internen Ermittlung in Unternehmen", en Knierim/ Rübenstahl/ Tsambikakis (eds.), *Internal Investigations. Ermittlungen im Unternehmen*, C. F. Müller, Heidelberg et. al., 2013, nm. 16 y ss.

- NIETO MARTIN, A., "¿Americanización o europeización del Derecho penal económico europeo?", en *Revista Penal*, nº 19, 2007.
- NIETO MARTIN, A., "Cumplimiento normativo", en AA.VV., *Manual de cumplimiento penal en la empresa*, dir. A. Nieto Martin, Valencia, 2015, pp. 25 y ss.
- NIETO MARTIN, A., "Investigaciones internas", en AA.VV., *Manual de cumplimiento penal en la empresa*, dir. A. Nieto Martin, Valencia, 2015, pp. 231 y ss.
- NIETO MARTÍN, A., "Investigaciones internas, whistleblowing y cooperación: la lucha por la información en el proceso penal", en *La Ley*, nº 8120, 2013.
- NIETO MARTÍN, A., "Problemas fundamentales del cumplimiento normativo en el Derecho penal", en *Compliance y teoría del Derecho penal*, Marcial Pons, 2013, pp. 21 y ss.
- NIETO MARTÍN, A., "Responsabilidad social, gobierno corporativo y autorregulación: sus influencias en el derecho penal de la empresa", *Política Criminal*, 5, 2008, pp. 1-18, Extraído de: [http://www.politicacrimina1.cl/n\\_05/a\\_3\\_5.pdf](http://www.politicacrimina1.cl/n_05/a_3_5.pdf).
- NIETO MARTIN, A., *La responsabilidad penal de las personas jurídicas: un modelo legislativo*, Valencia, 2008.
- NIETO MARTIN, A., "El cumplimiento normativo", en AA.VV., *Manual de cumplimiento penal en la empresa*, Valencia, p. 27.
- NWEBERG, J. A., "Corporate Codes of Ethics, Mandatory Disclosure, and the Market for Ethical Conduct". *Vermont Law Review* nº 29, 2005, pp. 253-295.
- ODENTHAL, R., *Korruption und Mitarbeiterkriminalität*, 2 Aufl., Gabler, Wiesbaden, 2009.
- OHRTMANN, N., *Compliance. Anforderungen an rechtskonformes Verhalten öffentlicher Unternehmen*, Wolters Kluwer, Köln, 2009.

- OLCESE SANTOJA, A. /BROWING, R./ WEIL, S., "Burden of Doubt: Stock of Doubt: Stocks take a beating as accounting worries spread beyond Enron", *Wall Street Journal*, 30 de enero de 2002.
- OLCESE SANTONJA, A., *El capitalismo humanista*, Marcial Pons, Barcelona, 2009.
- OLSEN, J., "Reporting versus inaction: How much is there, what explains the differences and what to measure", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, 2014, pp. 177 y ss.
- OMAROVA, S. T., "Rethinking the Future of Self-Regulation in the Financial Industry", *Brooklyn Journal of International Law* 35, 2010, pp. 665-706.
- ORTIZ DE URBINA GIMENO, I., "Responsabilidad penal de las personas jurídicas y programas de cumplimiento empresarial ("compliance programs")", en AA.VV., *Ética empresarial y códigos de conducta*, dir. J.L. Goñi, Madrid, 2011, pp. 95-135.
- ORTIZ DE URBINA GIMENO, I, en *Ética empresarial*, 2011, pp. 128-129.
- OTERO GONZALEZ, P., "Delitos contra la intimidad, derecho a la propia imagen, inviolabilidad del domicilio de personas jurídicas y establecimientos abiertos al público", en AA.VV., *Memento Penal Económico y de la Empresa*, coord., Ortiz de Urbina Gimeno, Francis Lefebvre, Madrid, 2011.
- OTERO SALGADO, L.D., "Prevención del blanqueo de capitales", AA.VV., *Compliance. Cómo gestionar los riesgos normativos en la empresa*, coord. C.A. Sáiz Peña, Pamplona, 2015, pp. 176 y ss.
- PAGE WEST, R., *Advising the Qui Tam Whistleblower: From Identifying a Case to Filing Under the False Claims Act*, edit. American Bar Association, 2009.
- PANAGIA, S., "Rilievi critici sulla responsabilità punitiva degli enti", en *Rivista trimestrale diritto penale dell'economia*, 2008.

- PASCUAL CADENA, A., *El plan de prevención de riesgos penales y responsabilidad corporativa*, Madrid, 2016.
- PASTOR MUÑOZ, N., "La respuesta adecuada a la criminalidad de los directivos contra la propia empresa: ¿Derecho penal o autorregulación empresarial?", *InDret* 4/2006.
- PASTOR MUÑOZ, N., "¿Organizaciones culpables? Recensión a Carlos Gómez-Jara, 'La culpabilidad penal de la empresa', *InDret*, nº 2, 2006.
- PASTORE, B., "Soft law, gradi di normatività, teoría delle fonti", *Lavoro e Diritto*, nº1, 2003, p. 5.
- PAUTHNER-SEIDEL, S., "§ 27: Compliance-Managementsysteme für Unternehmensrisiken im Bereich des Wirtschaftsstrafrechts", en Hauschka, ed. *Corporate Compliance*, C. H. Beck, München, 2ª ed., nº. 50, 2010.
- PÉREZ FERNÁNDEZ, P., "La importancia de los programas de cumplimiento (compliance programmes) en las políticas sancionadoras de las autoridades de competencia" en *Revista de Derecho Mercantil*, nº 292, 2014, pp. 297-332.
- PERRINI, F. "Corporate Social Responsibility: Un nuovo approccio strategico alla gestione d'impresa (Cultura di impresa)". ed. Egea, pp. 1-2, 11 de enero de 2011.
- PICKETT, S., *Internal Investigations: A Basic Guide Anyone Can Use*, Wiley, Southern Gate, p. 27, 2008.
- PIETH, M. "Co-Regulierung im Wirtschaftsstrafrecht", en Herzog/ Neumann eds., *Festschrift für W: Hassemer*, 2010.
- POLLACK, B. J., "Time to stop living vicariously: a better approach to corporate criminal liability", *American Criminal Law Review*, nº 46, pp. 1393-1415, 2009.
- PONS, P. M. "Comentarios al proyecto de ley de prevención del blanqueo de capitales y de la financiación del terrorismo: nuevas obligaciones para

- entidades financieras y otros sujetos obligados”, *Actualidad Jurídica Uribe Menéndez*, nº 25, pp. 61-73, 2010.
- POTINECKE, H. / BLOCK, F., "Gesellschaftliche Rahmenbedingungen und Beratung der Unternehmensführung", en Knierim/Rübenstahl/Tsambikakis eds., *Internal Investigations. Ermittlungen im Unternehmen*, C. F. Müller, Heidelberg et. al., nº 168 y ss., 2013.
- PROPPER, E., *Corporate Fraud Investigations and Compliance Programs*, Oceana Publications, New York, 2000, pp. 52 y ss.
- PULITANO, D., "La responsabilità 'da reato' degli enti nell'ordinamento italiano", en *Responsabilità degli enti per i reati commessi nel loro interesse*, Giuffrè, Milano, 2003.
- PULITANO, D., "La responsabilità 'da reato' degli enti: i criteri di imputazione", en *Rivista italiana di diritto e procedura penale*, 2002.
- QUIGLEY, S. K., "Whistleblower Tug-Of-War: Corporate attempts to secure internal reporting procedures in the face of external monetary incentives provided by the Dodd-Frank act", *Santa Clara Law Review*, nº 52, 2012, pp. 255-296.
- QUINTERO OLIVARES, G., "Personas jurídicas, entes, grupos y sus individuos: su responsabilidad penal tras la reforma de la Ley Orgánica 5/2010", *El Cronista del Estado Social y democrático de Derecho*, nº 22, 2011.
- RAGUÉS I VALLÈS, R., *La ignorancia deliberada en Derecho penal*, Atelier, Barcelona. STRACK, G., "Whistleblowing in Germany", 2007, Extraído de: [http://www.drasuszodis.lt/usermes/WB\\_in\\_Germany\(I\).pdf](http://www.drasuszodis.lt/usermes/WB_in_Germany(I).pdf).
- RAGUÉS I VALLÈS, R., "¿Héroes o traidores?. La protección de los informantes internos (whistleblowers) como estrategia político criminal", *InDret* nº 3, 2006, pp. 7 y ss.



- RAGUÉS I VALLÈS, R., "El fomento de la denuncias como instrumento de política criminal contra la criminalidad corporativa: whistleblowing interno vs. whistleblowing externo" en AA.VV., *Responsabilidad de la empresa y compliance. Programas de prevención, detección y reacción penal*, dir. S. Mir, M. Corcoy, V. Gomez, pp. 459-486, Madrid, 2014.
- RAGUÉS I VALLÈS, R., "Los procedimientos internos de denuncia como medida de prevención de delitos en la empresa" en AA.VV., *Criminalidad de empresa y compliance. Prevención y reacciones corporativas*, dir. J.M. Silva Sánchez, Ed. Atelier, pp. 161-196, Barcelona, 2013.
- RAGUÉS I VALLÈS, R., "Delitos contra la libertad", en AA.VV., *Lecciones de Derecho Penal. Parte Especial*, dir. Silva Sánchez, 3ª ed., Atelier, pp. 85-103, Barcelona, 2011.
- RAGUÉS I VALLÈS, R., *Whistleblowing. Una aproximación desde el Derecho penal*. Marcial Pons, 2013.
- RALLO LOMBARTE, A. "Whistleblowing" (sistemas internos de denuncia) y protección de datos", *Cuadernos de derecho para ingenieros*, vol. 14, Cumplimiento normativo. Compliance, coord. M. A. Agúndez, J. Martínez-Simancas Sánchez, pp. 97-118, Cuadernos de Derecho para mecanismos de denuncia o Whistleblowing y protección de datos", en AA.VV. (dir. A. J. Reclade Castells), *Derecho de la Empresa y protección de datos*, Thomson/Aranzadi, AEPD, Navarra, 2008, pp. 21 y ss.; "Sistema de denuncia interna de irregularidades (Whistleblowing)", AA.VV. (dir.: J.L. Goñi Sein), *Ética empresarial y códigos de conducta*, La Ley- Grupo Wolters Kluwer, Madrid, 2011, pp. 319-355; "Los sistemas de denuncia privada de conductas ilícitas: Whistleblowing", en AA.VV. (dirs.: Agúndez, M.A., Martínez-Simancas; coord.: Albañana, C) *Cumplimiento normativo. Compliance. Cuadernos de Derecho para Ingenieros*, pp. 81 y ss.
- RATHGEBER, C., *Criminal Compliance*, 2012.

- RAUSAND, M. *Risk Assessment: Theory, Methods, and Applications (Statistics in Practice)*, ed. Wiley, New Jersey, 2011.
- REB, P., *Internal Investigations, Schriftenreihe des Mas Planck Institut. Band 127*, Freiburg, 2011.
- REEB, P., *Internal Investigations. Neue Tendenzen privater Ermittlungen*, Duncker & Humblot, Berlin, 2011.
- REMACHA, M. "Compliance, ética y RSC", Cuadernos de la Cátedra "la Caixa" de Responsabilidad Social de la Empresa y Gobierno Corporativo, p. 6 y ss., Julio 2016, Extraído de: [http://www.iese.edu/es/multimedia/catedralaciixa\\_31\\_tcm42-230724.pdf](http://www.iese.edu/es/multimedia/catedralaciixa_31_tcm42-230724.pdf).
- ROBERTS, P., "Motivations for whistleblowing: Personal, private and public interests", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, pp. 207 y ss., 2014.
- ROBLES PLANAS, R., "Pena y persona jurídica: crítica del art. 31 bis CP", *La Ley*, nº 7705, 2011.
- RÖDIGER, K., *Strafverfolgung von Unternehmen, Internal Investigations und strafrechtliche Verwertbarkeit von "Mitarbeitergeständnissen" - Untersuchung am Beispiel der Siemens-Korruptionsaffäre*, Peter Lang Verlag, Frankfurt, 2012.
- RODRIGUEZ YAGÜE, C., "La protección de los *Whistleblowers* por el ordenamiento español: aspectos sustantivos y procesales", en AA.VV., *Fraude y Corrupción en el Derecho penal económico europeo. Eurodelitos de corrupción*, coords. L. Arroyo y A. Nieto Martín, edit. Universidad de Castilla-La Mancha, Cuenca, 2006, pp. 447 y ss.
- RODRIGUEZ, G., "Recepción de denuncias, investigación interna y obtención de evidencias", AA.VV., *Compliance. Cómo gestionar los riesgos normativos en la empresa*, coord. C.A. Sáiz Peña, pp. 657 y ss., Pamplona, 2015.

- RODRÍGUEZ-PIÑERO, M. / BRAVO-FERRER, M., "Derecho a la intimidad del trabajador y contrato de trabajo", *Diario La Ley*, nº 6033, 2004.
- ROHDE LIEBENAU, B. Whistleblowers Rules: Best practice. Assessment and Revision of rules existing in EU Institutions. Estudio solicitado por el Parlamento de la Unión Europea, comisión de control presupuestario, p. 29, Bruselas, 2006.
- ROMEO CASABONA, C.M., *Los delitos de descubrimiento y revelación de secretos*, Valencia, 2005.
- ROTSCH, T. (dir.), *Wissenschaftliche und praktische Aspekte der nationalen und internationalen Compliance-Diskussion*, 2012.
- ROTSCH, T., "Criminal Compliance", en Achenbach/Ransiek (eds.), *Handbuch Wirtschaftsstrafrecht*, 3<sup>a</sup> ed., 2012.
- ROXIN, C., *Strafrecht. Allgemeiner Teil*, 4<sup>a</sup> ed., Beck, München, 2006.
- RUGGIERO, G., *Capacità penale e responsabilità degli enti*, Giappichelli, Torino, 2004.
- SAHAN, S. "Unternehmensinterne Untersuchungen aus rechtsanwaltlicher Perspektive", en AA.VV., *Compliance und Strafrecht*, coords. Kuhlen/Kudlich/Ortiz de Urbina, edit. C. F. Müller, Heidelberg, pp. 171, 2012.
- SALAFIA, V., "Costituzionalità del D.Lgs. nº 231/01 e il disegno di legge per la sua parziale riforma", en *Le società*, 2010.
- SALOMON Y SALOMON, *Corporate Governance and accountability*, Londres, 2004.
- SALVADOR CODERCH, P./GOMEZ LIGÜERRE, C.I., "Respondeat Superior II. De la responsabilidad por hecho de otro a la responsabilidad de la organización", *InDret*, nº 3, 2002, pp. 1 y 22. Extraído de [http://www.indret.com/pdf/088\\_es.pdf](http://www.indret.com/pdf/088_es.pdf)
- SAN MARTÍN MAZZUCCONI, C. /SEMPERE NAVARRO, A. V., "Sobre el control empresarial de los ordenadores", *Aranzadi Social* nº 3, 2012.

- SANTORIELLO, "Riflessioni sulla possibile responsabilità degli enti collettivi in presenza dei reati colposi", en *La responsabilità amministrativa delle società e degli enti*, nº 4, 2011.
- SARACIBAR, E. / GONZALEZ, C. "Privacidad y protección de datos", en AA.VV., *Compliance. Cómo gestionar los riesgos normativos en la empresa*, coord. C.A. Sáiz Peña, pp. 211 y ss., Pamplona, 2015.
- SCHEBEN, B./KLOS, C., "Analyse von Chatprotokollen und E-Mails –Wie ist erlaubt? Was ist verwertbar?" CCZ nº 3, 2013.
- SCHEMMEL, A./ RUHMANNSEDER, F./WITZIGMANN, T., *Hinweisgebersysteme*, C.F. Müller, 2012.
- SCHÜNEMANN, B., "The Sarbanes-Oxley Act of 2002: A German Perspective", *Buffalo Criminal Law Review*, Vol. 8, 2004.
- SCHÜNEMANN, B., "Sistema de Derecho penal y victimodogmática", en DÍEZ RIPOLLÉS *et al.* (ed.), *La ciencia del Derecho penal ante el nuevo siglo: libro homenaje al profesor doctor Don José Cerezo Mir*, Tecnos, pp. 159-172, Madrid, 2002.
- SCHÜRRLER, T./ OLBERS, L.A.M., *Praktische Hinweise zu Rechtsfragen bei eigenen Untersuchungen im Unternehmen*, CCZ 5/2010.
- SCHWARTZ, M. / WATKINS, S. *Power Failure: The Inside Story of the Collapse of Enron*, New York, 2003.
- SEMINARA, S., "Compliance y Derecho Penal: la experiencia italiana", en AA.VV., *Responsabilidad de la Empresa y Compliance. Programas de prevención, detección y reacción penal*, dirs. S. Mir Puig, M. Corcoy y V. Gómez, pp. 127 y ss., Madrid, 2014.
- SERRANO SORDO, T., "Las normas de conducta en la prestación de servicios de inversión. El reglamento interno de conducta como instrumento para asegurar el cumplimiento normativo: especial referencia a las obligaciones en materia de abuso de mercado", en AA.VV., *Gobierno corporativo: La estructura del órgano de gobierno y la*

- responsabilidad de los administradores (Adaptado a la Ley 31/2014, de 3 de diciembre)*, dirs. Alfonso Martínez- Echevarria y García de Dueñas, pp. 687 y ss., Pamplona, 2015.
- SHARP PAINE, L., "Managing for Organizational Integrity", *Harvard Business Review*, marzo-abril, 1994.
- SHORT J. L./ TOFFEL, M. W., "Making Self-Regulation More than Merely Symbolic. The Critical Role of the Legal Environment", *Administrative Science Quarterly* 55, pp. 361-396, 2010.
- SIEBER, U., "Programas de *compliance* en el Derecho penal de la empresa. Una nueva concepción para controlar la criminalidad de empresa", en AA.VV., *Dogmática penal de derecho penal económico y política criminal homenaje a Klaus Tiedeman*, coords. N. Salazar Sánchez y otros, Vol. 2, Universidad de San Martín de Porres (USMP), pp. 206 y ss., Lima, 2011.
- SILVA SÁNCHEZ, J. M., "Hacia el Derecho penal del "Estado de la prevención". La protección penal de las agencias administrativas de control en la evolución de la política criminal", en *¿Libertad económica o fraudes punibles? Riesgos penalmente relevantes e irrelevantes en la actividad económico-empresarial*, coord. J.M. Silva Sánchez, pp. 307-332, Madrid, 2003.
- SILVA SÁNCHEZ, J. M., "La consideración del comportamiento de la víctima en la teoría jurídica del delito. Observaciones doctrinales y jurisprudenciales sobre la "víctimo-dogmática", en CGPJ (ed.), *La victimología*, CGPJ, pp. 13-52, Madrid, 1993.
- SILVA SÁNCHEZ, J. M., *Criminalidad de empresa y Compliance*. 2013.
- SILVA SANCHEZ, J.M., "La responsabilidad penal de las personas jurídicas y las consecuencias accesorias del art. 129 del Código penal", en AA.VV., *Derecho penal económico*, CGPJ, 2001.
- SILVA SÁNCHEZ, J.M., *Aproximación al Derecho penal contemporáneo*, BdeF, Montevideo-Madrid, 2010.

- SINGLETON, S., *Competition Law Compliance 2008*, Thorogood, London, 2008.
- SMITH, R., Whistleblowers and suffering", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, pp. 230 y ss. 2014.
- SNIFFEN, M., *Government's False Claims Recoveries Rise*. Associated Press. Febrero de 2000.
- SOLOMON, J./ SOLOMON, A., *Corporate Governance and Accountability*, Londres, 2004.
- SPANHEIMER, R., "Justification for creating an Ombudsman Privilege in today's society" en *Market Law Review*, Vol. 96, Issue 2, pp. 659-688, 2012.
- SPEHL/GRÜTZNER, *Corporate Internal Investigations*, BECK C. H., MÜNCHEN, *passim*, 2012.
- SPENCER, M. / SPENCER, J. "When it all goes bad: Criminal remedies", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, pp. 405 y ss., 2014.
- SPINDLER, G., "Reformas en el gobierno corporativo al nivel de los órganos de Risk Management Recent reforms in corporate governance of banks according to the CRD IV-Directive", en AA.VV., *Crisis y reforma del sistema financiero*, coords. A.J. Recalde Castells, I. Tirado Martí y A.B. Perdices Huetos, p. 235, Pamplona, 2014.
- STRACK, "Whistleblowing in Germany", p. 5.
- TALADRIZ, C. "Mercados de Capitales. Whistleblowers en los mercados financieros", 21 de noviembre de 2011, Extraído de: <http://mercapuc.blogspot.com.es/2011/11/whistleblowers-en-los-mercados.html>.

- TAMARIT SUMALLA, J. T., *La Víctima en el Derecho Penal. De la víctimodogmática a una dogmática de la víctima*, Aranzadi, Pamplona 1998.
- TAPIA HERMIDA, A.J., "El sistema de gobierno de las entidades aseguradoras", en AA.VV., *Estudios Jurídicos en memoria del profesor Emilio Beltrán. Liber Amicorum*, T. I, pp. 990 y ss., Valencia, 2015.
- TAPIA HERMIDA, A.J., "Los puntos críticos del proceso de implantación del sistema de gobierno en las entidades aseguradoras", *Revista Española de Seguros*, nº 167, pp. 331 y ss., 2016.
- TAPIA HERMIDA, A.J., "Sistema de Gobierno de las Entidades Aseguradoras y Reaseguradoras", en AA.VV., *Supervisión en Seguros Privados. Hacia Solvencia II. Actas del Congreso de Ordenación y Supervisión en Seguros Privados*, dirs. V. Cuñat Edo, J. Bataller Grau, Colección Homenajes y Congresos, pp. 283 y ss. Valencia, 2013.
- TAPIA HERMIDA, A.J., *Manual de Derecho del Mercado Financiero*, Madrid, 2015.
- TARANTINO, A., *Governance, Risk, and Compliance Handbook*. Wiley, 2008.
- TAYLOR, PAUL M., *E.C. & U.K. Competition Law & Compliance: A Practical Guide*, Sweet & Maxwell, London, 1999.
- THOMAS, S., "Guilty of a Fault that one has not Committed. The Limits of the Group-Based Sanction Policy Carried out by the Commission and the European Courts in EU-Antitrust Law" en *Journal of European Competition Law & Practice*, Vol. 3, nº 1, pp. 11-28, 2012.
- THOMPSON, L. D., memorándum on Bringing Criminal Charges Against Corporations, de 20 de enero, 2003, Extraído de: [http://www.justice.gov/dag/cftf/corporate\\_guidelines.htm](http://www.justice.gov/dag/cftf/corporate_guidelines.htm).
- TIPPETT, E., "The promise of compelled whistleblowing: what the corporate governance provisions of Sarbanes Oxley mean for employment law "en

- Employee rights and employment policy Journal*, Vol. 11, nº 1, pp. 1-43, 2007.
- TREVIÑO, L.K./WEAVER, G.R., *Managing Ethics in Business Organizations*, Stanford Business Books, Stanford University Press, California, 2003.
- TROIANO, V. / MOTRONI, R., *La MiFID II: Rapporti con la clientela - regole di governance – mercati*, Milano, 2016.
- TSAHURIDU, E. y VANDEKERCKHOVE, W., “Organizational whistleblowing policies: Making employees responsible or liable?” en *Journal of Business Ethics*. Vol. 82, Issue 1, pp. 107-118, 2008.
- UNITED STATES ATTORNEY'S, *Manual de agosto de 2008*, Extraído de: [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usam/title9/28mcr m.htm](http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/28mcr m.htm).
- UNITED STATES SENTENCING GUIDELINES, *Manual de 2011*, Extraído de: [http://www.ussc.gov/Guidelines/2011\\_Guidelines/Manual\\_PDF/Chapter\\_8.pdf](http://www.ussc.gov/Guidelines/2011_Guidelines/Manual_PDF/Chapter_8.pdf).
- UNITED STATES CONGRESS HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES, *Sarbanes-oxley: Two Years Of Market And Investor Recovery*”, Ulan Press, 2011
- PELCHRZIM, V., "Whistleblowing und der strafrechtliche Geheimnisschutz nach § 17 UWG", CCZ, 2009.
- PEREGRINE, M.W., “Another View: Sarbanes-Oxley and the Legacy of Enron”, November 25, 2011, NY, Extraído de: [https://dealbook.nytimes.com/2011/11/25/another-view-sarbanes-oxley-and-the-legacy-of-enron/?\\_r=0](https://dealbook.nytimes.com/2011/11/25/another-view-sarbanes-oxley-and-the-legacy-of-enron/?_r=0)
- VANDEKERCKHOVE, W. y LEWIS, D., “The content of whistleblowing procedures. A critical review of recent official guidelines” en *Journal of Business Ethics*, Vol. 108, Issue 2, pp. 253-264, 2012.
- VANDEKERCKHOVE, W./ BROWN, A.J. / TSAHURIDU, E., "Managerial responsiveness to whistleblowing: Expanding the research horizon", en



- AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, pp. 298 y ss., 2014.
- VANDEKERCKHOVE, W./ UYS, T./ REHG A., MICHAEL T./ BROWN, J., "Understandings of whistle blowing: Dilemmas of societal culture", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, pp. 37 y ss., 2014.
- VANDEKERCKHOVE, W./ BROWN, A.J./ MOBERLY, R./ LEWIS, D., "Strategic issues in whistleblowing research", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, pp. 522 y ss., 2014.
- VAUGHN, R. *Whistleblowing Law*, Hardback, 2015.
- VAUGHN, R., *The successes and failures of whistleblower laws*, Edward Elgar Publishing, 2012.
- VELASCO NUÑEZ, E./ SAURA ALBERDI, B., *Cuestiones prácticas sobre responsabilidad penal de la persona jurídica. 86 preguntas y respuestas*, Pamplona, 2016.
- VILLEGAS GARCIA, M.A., ENCINAR, M.A. "Compliance Programs y DPA: Una nueva etapa en el camino hacía un derecho anticorrupción sin fronteras", 2016.
- WALDEN, S./ EDWARDS, B. "Whistleblower protection in international governmental m organizations", en AA.VV., *International Handbook on Whistleblowing Research*, dirs. A. J. Brown, D. Lewis, R. Moberly, pp. 430 y ss. 2014.
- WALSH, C.J. /PYRICH, A., "Corporate Compliance Programs as a Defense to Criminal Liability: Can a Corporation Save its Soul?", *Rutgers Law Review*, vol. 47, 1994-1995, pp. 645 y ss.
- WARNER, J.C., *Corporate Ethics (Rapid Skill Builder Series)*, Ed. Ready To Manage Inc, 2012.

- WAUSCHKUHN, "Sanktionierung nach Abschluss der Untersuchungen", en Moosmayer/Hartwig (eds.), *Interne Untersuchungen. Praxisleitfaden für Unternehmen*, Beck, München, pp. 67 y ss., 2012.
- WEBB, D./TARUN, R./MOLO, S., *Corporate Internal Investigation*, Law Journal Press, 2008.
- WEISSE, "Ausgewählte arbeitsrechtliche Aspekte und Amnistie", en Moosmayer/ Hartwig (eds.), *Interne Untersuchungen. Praxisleitfaden für Unternehmen*, C. H. Beck, pp. 58 y ss., Munich, 2012.
- WELLNER, P.A., "Effective Compliance Programs and Corporate Criminal Prosecutions", *Cardozo Law Review*, vol. 27, 2005, pp. 497 y ss.
- WEWERKA, F., *Internal Investigations. Private Ermittlungen im Spannungsfeld von strafprozessualen Grundsätzen und Anforderungen eines globalisierten Wirtschaftsstrafverfahrens; eine Problemanalyse unter besonderer Berücksichtigung des Falles Siemens*, Peter Lang Verlag, Frankfurt a.M. et. al., 2012.
- ZUCKOFF, M., *Ponzi's Scheme: The True Story of a Financial Legend*, Random House: New York, 2005.
- ZUGALDÍA ESPINAR, J. M., " *Societas delinquere potest* (análisis de la reforma operada en el Código penal español por la LO 5/2010 de 22 de junio", *La Ley Penal: revista de derecho penal, procesal y penitenciario*, nº 76, 2010.
- ZYSMAN BERNALDO DE QUIRÓS, D., *Castigo y determinación de la pena en los Estados Unidos: Un estudio sobre las United States Sentencing Guidelines*", edt. Marcial Pons Ediciones Jurídicas y Sociales, S.A., Madrid, 2013.