universidad de león

Facultad de Derecho
Universidad de León
Curso 2018/2019

BUEN GOBIERNO CORPORATIVO Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: *EL PRINCIPIO DE ACCOUNTABILITY EN EL ÁMBITO DE LAS SOCIEDADES MERCANTILES*

CORPORATE GOVERNANCE AND PERSONAL DATA PROTECTION: *THE ACCOUNTABILITY PRINCIPLE IN THE CONTEXT OF BUSINESS CORPORATIONS*

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y EL ENTORNO DIGITAL

Realizado por el alumno	Tutorizado por la Profesora
D. Jorge Saco Vega	**Dra. Dª Elena Fátima Pérez Carrillo**

SUMARIO

ABREVIATURAS

AEPD	*Agencia Española de Protección de Datos.*
Art./s	*Artículo/s.*
Cap.	*Capítulo.*
CEO	*Chief Executive Officer.*
CIO	*Chief Information Officer.*
CISO	*Chief Information Security Officer.*
CNIL	*Commission Nationale de l'Informatique et des Libertés / Comisión Nacional de Informática y de las Libertades. (FR)*
CNMV	*Comisión Nacional del Mercado de Valores.*
CSO	*Chief Security Officer.*
CTO	*Chief Technology Officer.*
DPO / DPD	*Delegado de Protección de Datos Personales.*
EIPD /PIA	*Evaluación de Impacto / Privacy Impact Assessment.*
ENAC	*Entidad Nacional de Acreditación.*
ERM	*Enterprise Risk Management / Gestión de Riesgos Empresariales.*
IT	*Information Tecnology / Tecnología de la Información.*
LOPD	*Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*
LOPDGDD	*Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales.*
NACD	*National Association of Corporate Directors / Asociación Nacional de Directores Corporativos. (EE.UU.)*
OECD	*Organisation for Economic Co-operation and Development / Organización para la Cooperación y el Desarrollo Económicos.*
Pág. / Págs.	*Página/s.*
RD	*Real Decreto.*
RGDP / GDPR	*Reglamento General de Protección de Datos Personales.*
RSC	*Responsabilidad Social Corporativa.*
Sec.	*Sección.*
TID	*Transferencias Internacionales de Datos.*
VV.AA.	*Varios Autores.*

RESUMEN

El objetivo de este trabajo consiste en ofrecer un acercamiento a la reciente normativa de protección de datos personales en relación con las principales manifestaciones y mecanismos del buen gobierno corporativo en el seno de las sociedades mercantiles. Asimismo, se trata de presentar como interactúan los principales roles encargados de la protección de datos personales dentro de las empresas y como estos pueden llevar a cabo las funciones propias del cumplimiento normativo y del principio de responsabilidad proactiva al mismo tiempo que actúan siguiendo los principios de la gobernanza empresarial.

Palabras clave: protección de datos personales, buen gobierno corporativo, gobernanza empresarial, data governance, cumplimiento normativo, compliance, responsabilidad proactiva, accountability, RGPD, LOPDGDD, soft law, códigos de conducta.

ABSTRACT

This dissertation offers an approach to the recent personal data regulations in regards to the fundamental manifestations and mechanisms of corporate governance within the context of the business sector. The current study also presents how the key data protection roles within the enterprise system interact and how they can conduct their functions to demonstrate compliance by meeting the requirements of the accountability principle, while at the same time they act according to the principles of corporate governance.

Keywords: *Personal data protection, corporate governance, data governance, compliance, accountability, GDPR, governance mechanisms, soft law.*

OBJETO DEL TRABAJO

El presente estudio ofrece una aproximación a la nueva legislación en materia de protección de datos personales desarrollada dentro del marco de la Unión Europea y, específicamente, en el ordenamiento jurídico español. Particularmente, se busca delimitar como esta nueva normativa afecta al funcionamiento y continuidad del sector privado o empresarial, al mismo tiempo que se relaciona dicha materia con el concepto del buen gobierno corporativo.

Durante la primera parte del trabajo, se ofrece una visión general de cómo ha ido evolucionando dentro del marco jurídico español, por un lado, la legislación existente relativa a la protección de datos personales y, por otro lado, el desarrollo de la figura del buen gobierno corporativo o gobernanza empresarial. Asimismo, se trata de realizar una exposición de cuáles son los aspectos formales introducidos por la nueva legislación y cuáles son las actuaciones necesarias para llevar a cabo una implantación responsable de la protección de datos personales dentro de las sociedades mercantiles, respetando y garantizando los principios rectores del buen gobierno corporativo.

Finalmente, se analiza el surgimiento y evolución del principio de responsabilidad proactiva o *accountability*, exponiendo como el mismo constituye una manifestación clave del nuevo régimen de protección de datos personales establecido en la Unión Europea, a la vez que se presenta como un instrumento idóneo a la hora de potenciar y garantizar que el cumplimiento normativo y las previsiones del buen gobierno corporativo se desarrollan correctamente en el seno de las sociedades mercantiles. En este aspecto, se trata de ofrecer una visión práctica de como los distintos roles y responsables en materia de protección de datos dentro la empresa juegan un papel clave a la hora de poder garantizar el cumplimiento normativo sin salirse de los cauces marcados por la gobernanza empresarial.

METODOLOGÍA

En un primer momento, la elección del tema objeto del presente estudio vino motivada en gran medida por ser esta materia una de las principales ramas tratadas en los estudios de máster, ya que la protección de datos de carácter personal ocupa una gran parte del contenido lectivo del título, siendo además una temática de gran actualidad, tanto desde el punto de vista jurídico como social. Posteriormente, se plantearon diversos debates y reuniones con la tutora que dirige el presente estudio con el objetivo de buscar una perspectiva o enfoque mercantilista, tratando de abordar este tema desde el área del derecho que constituye el núcleo profesional y docente de la tutora y sobre la que personalmente estoy más especializado y tengo un mayor interés. A consecuencia de esto, se decidió abordar el tema en conexión con el buen gobierno corporativo, creando de este modo una línea de trabajo que recoge y desarrolla perfectamente ambas materias, especialmente a través del cumplimiento normativo, el *soft law* y el principio de responsabilidad proactiva, los cuales constituyen los tres elementos clave del presente trabajo.

El proceso académico que ha dado como resultado este proyecto se ha desarrollado fundamentalmente en base al análisis y consulta de, por un lado, artículos, manuales y monografías de diversos autores y, por otro, de diversas fuentes legislativas, normas de distinto rango y una pequeña selección de material jurisprudencial. En cuanto al primer grupo de materiales, los diferentes artículos y monografías se han extraído tanto de bases de datos y fuentes informáticas, como de un conjunto de manuales facilitados por la universidad y el departamento de derecho mercantil. En relación con la búsqueda de materiales presentes en bases electrónicas, es importante destacar que gran parte de la bibliografía tiene un marcado carácter internacional y pertenece a doctrina extranjera, ya que la materia tratada en el trabajo posee de manera intrínseca un aspecto globalizado y novedoso, habiendo sido necesario llevar la búsqueda de materiales a publicaciones que abarcan un ámbito supranacional. Por otro lado, y en relación con el estudio de normas jurídicas, se han analizado principalmente aquellas disposiciones relativas a la protección de datos, destacando fundamentalmente la nueva regulación europea y la ley orgánica nacional, así como una serie de documentos y disposiciones de organismos e instituciones nacionales e internacionales. No obstante, también se han consultado y estudiado en gran

medida aquellas disposiciones pertenecientes al llamado *soft law*, destacando principalmente los conocidos códigos de conducta, pues los mecanismos de autorregulación y certificación son una de las principales materias que ha abarcado el presente trabajo. Por su parte, el compendio jurisprudencial examinado es bastante escueto, todo ello a consecuencia de que el enfoque del estudio se plantea desde el punto de vista del *soft law* en su mayor parte, siendo además las dos principales disposiciones legales examinadas de reciente aprobación, circunstancia que supone que la materia no ha sido tratada en gran medida en los tribunales.

Conjuntamente a todo lo anterior, han sido imprescindibles para la realización del trabajo las aportaciones y asistencia de la tutora, así como el seguimiento y discusiones realizados en el departamento de derecho mercantil a lo largo del año. Asimismo, el periodo de prácticas externas en empresa ha constituido un factor esencial para el desarrollo de parte de este estudio, pues haber trabajado con profesionales del sector de la protección de datos y la ciberseguridad ha sido imprescindible a efectos de entender la casuística y la puesta en práctica de esta materia, así como para conocer los aspectos formales de implantación de la misma dentro de las sociedades mercantiles y los roles y responsabilidades existentes en la organización.

EL BUEN GOBIERNO CORPORATIVO Y LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: *EL PRINCIPIO DE ACCOUNTABILITY EN EL ÁMBITO DE LAS SOCIEDADES MERCANTILES*

1. PRIMER CAPÍTULO

PLANTEAMIENTO INICIAL E INTRODUCCIÓN A LA PROTECCIÓN DE DATOS EN EL SECTOR PRIVADO

1.1. Evolución legislativa y enfoque general sobre la protección de datos

Antes de abordar el núcleo del tema objeto de este trabajo, es conveniente realizar un pequeño acercamiento a la materia y a su trasfondo jurídico. El objetivo es ofrecer una visión panorámica de la nueva regulación europea y nacional en materia de protección de datos y su posterior desarrollo dentro de la esfera mercantil y empresarial.

En la actualidad estamos presenciando lo que podíamos llamar una "*avalancha de datos*", donde la cantidad de datos generados, procesados y transferidos por una gran variedad de entidades se incrementa exponencialmente día a día. Los avances tecnológicos y el desarrollo de los sistemas de comunicación e información, junto con la creciente capacidad de los individuos para usar e interactuar con estas tecnologías, se encuentran en la base que justifica este fenómeno.

Más allá de la ubicuidad de los datos, el hecho de que la gran mayoría del *big data*[1] sean datos personales supone que la información generada a partir de ellos se convierta en una moneda de cambio, no sólo en Internet. Asimismo, este aumento en el valor social, económico y político de los datos trae consigo incrementos en la cantidad y gravedad de los riesgos que se derivan de su tratamiento, tanto en el sector público como en el privado, cuya posible materialización tendría consecuencias devastadoras en términos tanto económicos como reputacionales. Por todo lo anterior, a día de hoy

[1] DATOO A. *Legal Data for Banking: Business Optimisation and Regulatory Compliance*. 1 st Ed, 2019: El concepto de *big data* es un término genérico utilizado para referirse a colecciones de datos de tal tamaño y complejidad que su gestión no puede ser llevada a cabo por los métodos tradicionales de procesamiento de datos. De manera generalizada se utilizan cuatro elementos fundamentales para determinar si estamos ante un conjunto de datos calificado como *big data*, estos son el volumen, la variedad, la veracidad y la velocidad de los mismos.

encontramos una creciente necesidad e interés en adoptar medidas necesarias para proporcionar una verdadera protección de los datos personales. [2]

Tras cuatro años de constante preparación y debate en sede de las instituciones comunitarias, se llevó a cabo la aprobación por parte del Parlamento Europeo y el Consejo del *Reglamento (UE) 2016/679 de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* (en adelante, RGPD). Esta nueva normativa europea, de aplicación directa, deroga a la directiva predecesora en la materia, la *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos* (en adelante, Directiva 95/46/CE).

El propio RGPD recoge en su *Considerando 9* que dicha Directiva perseguía objetivos y principios que aun considera válidos, pero que su aplicación se ha llevado a cabo de una manera fragmentada a lo largo del territorio comunitario. Ante esta falta de uniformidad legislativa entre los Estados Miembros, se impulsó desde las instituciones europeas la elaboración de este Reglamento a efectos de garantizar que la protección de datos en la U.E. alcanza un elevado nivel de desarrollo y sigue una serie de principios de coherencia y homogeneidad.[3] El RGPD entró en vigor el 25 de mayo de 2018 y es directamente aplicable en cada Estado miembro y obligatorio en todos sus elementos (Art. 99.2 RGPD).

Desde el punto de vista del Estado español, toda esta evolución legislativa ha ocasionado la necesidad de que la normativa nacional se haya ido adaptando a lo largo de los años a los cambios que se han ido aconteciendo en Europa. En un primer momento [4], se aprobó la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de*

[2] EUROPEAN COMISSION. (Article 29 Data Protection Working Party). *Opinion 3/2010 on the principle of accountability* [En línea]. Bruselas, 2010. [Fecha de consulta: 02/04/19] [Disponible en: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf*]
[3] Considerando 10, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, 27 de abril de 2016, L 119/2.
[4] Todo ello sin perjuicio de la *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*, popularmente conocida como LORTAD, que fue la ley pionera en nuestro país en materia de protección de datos y vino derogada por la LO 15/1999. Además del *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, de 28 de enero de 1981, firmado y ratificado por España en 1985.

Carácter Personal (en adelante, LO 15/1999), la cual trasponía en España el contenido de la *Directiva 95/46/CE* y se fundamentaba en el desarrollo del artículo 18 de la *Constitución Española* relativo al derecho al honor, a la intimidad personal y familiar y a la propia imagen. En relación con esto, es importante destacar que la principal fuente de desarrollo se relaciona con el *apartado 4* del citado artículo 18 CE[5], a raíz del cual se configura la protección de datos -también conocido como *habeas data* o *derecho a la libertad informática*-, como un derecho fundamental [6], circunstancia que implica su desarrollo mediante una ley orgánica.

Con la aprobación del RGPD y la derogación de la *Directiva 95/46/CE*, se propició la elaboración de un nuevo texto normativo que se ajustase a las disposiciones del nuevo reglamento y desarrollase aquellas cuestiones específicas que él mismo encomendaba a los ordenamientos internos de los Estados Miembros. Esto ocasionó la aprobación en España de la reciente *Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales* (en adelante, LOPDGDD). Esta nueva normativa deroga la anterior LO 15/1999 salvo citadas excepciones [7], así como otras disposiciones en materia de protección de datos y su desarrollo.[8]

A este respecto, y una vez expuesto sin ánimo de exhaustividad el trascurso legislativo que se ha llevado a cabo en materia de protección de datos, cabe destacar que el análisis del tema objeto del presente trabajo se va a basar en la concepción actual y previsiones incluidas en el RGPD y la LOPDGDD, así como, en la aplicabilidad de las citadas disposiciones en la esfera del derecho mercantil. Todo ello en conjunción con otros mecanismos de autorregulación voluntaria, como son los códigos de conducta o buen gobierno y los mecanismos de certificación.

[5] Art. 18. 4, Constitución Española, *BOE*, 1978: *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*.
[6] Véanse las *Sentencias del Tribunal Constitucional (STC) 292/2000, de 30 de noviembre*; *la 254/1993, de 20 de julio; la 143/1994, de 9 de mayo y la 11/1998, de 13 de enero*; entre otras.
[7] La disposición derogatoria única de la LOPDGDD nos dice que deroga la anterior normativa en materia de protección de datos sin perjuicio de lo dispuesto en la disposición adicional decimocuarta y transitoria cuarta, relativas al artículo 13 de la Directiva 95/46/CE en materia de excepciones y limitaciones, y al tratamiento de datos personales por las autoridades con fines relativos a la persecución de infracciones penales, respectivamente.
[8] Recoge la derogación *del Real Decreto-ley 5/2018, de 27 de julio, de medias urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos* y todas aquellas disposiciones de igual o inferior rango que se opongan o sean incompatibles con el RGPD y la citada ley orgánica.

A efectos de desarrollar los posteriores apartados sobre esta reciente normativa es conveniente exponer aquellos principios rectores o inspiradores sobre los que se ha cimentado la misma y que constituyen el núcleo legislativo de la materia. [9] Estos seis principios se configuran como un guía de intenciones éticas subyacentes a la propia norma y manifiestan la visión de futuro perseguida por la protección de datos, poniendo de manifiesto el espíritu de la legislación, así como quienes son las personas responsables de garantizar sus valores y obligaciones.[10] Es importante destacar que dentro de estos principios no encontramos ninguno relativo a los derechos de los particulares o personas físicas ni sobre las transferencias internacionales de datos, ya que en el nuevo reglamento estas dos materias se abordan separadamente en los capítulos III y V respectivamente de la citada norma.[11] Los mencionados principios vienen recogidos en el *artículo 5 del RGPD* y son los siguientes[12]:

(a) *Licitud, lealtad y transparencia*. Los datos personales deberán ser procesados de manera legal, justa y transparente en relación con el interesado.
(b) *Limitación de la finalidad*. Los datos deberán ser recopilados en base a fines específicos, explícitos y legítimos, no pudiendo estar sometidos a un tratamiento posterior que sea incompatible con dichos fines. [13]
(c) *Minimización de los datos*. Únicamente se podrán tratar aquellos datos que sean adecuados, pertinentes y limitados a los fines para los que se recogen.

[9] GILBERT, F. "Privacy and Security Legal Issues". En: GENG, H. *Internet of Things and Data Analytics Handbook*. 1st Ed. 2017: Como precedente de estos principios encontramos que en 1973 el Departamento estadounidense en materia de Sanidad, Educación y Bienestar adoptó los llamados *Principios para la práctica legitima de la información* (FIPPs), la cual incluía 7 principios – notificación, elección, exactitud, minimización, seguridad y *accountability* (responsabilidad)-. Estos principios son muy similares a los que elaboró posteriormente la OECD en sus guías para la privacidad y a los incluidos en la Directiva 95/46/CE, así como a los establecidos en la normativa actual.
[10] GOBEO A., FOWLER C. y BUCHANAN W.J. *GDPR and Cyber Security for Business Information Systems*. Gistrup, 2018.
[11] FOULSHAM M., HITCHEN B. y DENLEY A. *GDPR: How To Achieve and Maintain Compliance*. Nueva York, 2019.
[12] Como se dispone en la Sentencia del Tribunal Europeo de Derechos Humanos de 24 de abril de 2018 (*Caso Benedik vs. Slovenia*), debemos considerar que"*los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo".*
[13] El principio de limitación de la finalidad es uno de los principios mas relevantes, pues debido a su naturaleza la existencia de los demás principios está muy vinculada a este. A estos efectos, el Tribunal Constitucional en la *Sentencia de 22 mayo 2019* fundamente que "*Es suficiente con constatar que, al no poderse identificar con la suficiente precisión la finalidad del tratamiento de datos, tampoco puede enjuiciarse el carácter constitucionalmente legítimo de esa finalidad, ni, en su caso, la proporcionalidad de la medida prevista de acuerdo con los principios de idoneidad, necesidad y proporcionalidad en sentido estricto*".

(d) *Exactitud*. Los datos sobre los que se trabaja deberán ser exactos y en su caso actualizados.

(e) *Limitación del plazo de conservación*. Los datos personales podrán estar almacenados de manera que permita la identificación del interesado únicamente el tiempo necesario para el cumplimiento de los fines por los que fueron recopilados.[14]

(f) *Integridad y confidencialidad*. Los datos deberán ser tratados garantizando siempre su seguridad, incluyendo la protección contra un uso ilícito y contra su perdida, destrucción o daño, mediante medidas eficaces de carácter técnico y organizativo.

(g) *Responsabilidad proactiva*. El nuevo principio introducido por el RGPD con respecto a la anterior normativa y el que más nos interesa a efectos de este trabajo. Supone que el responsable del tratamiento es responsable no solo del cumplimento de estos principios, sino que además debe ser capaz de demostrarlo.

Por todo lo anteriormente expuesto, y con la finalidad de poner fin a este pequeño apartado introductorio, encontramos que existe la necesidad critica, especialmente para todas aquellas personas encargadas de llevar a cabo el control de los datos, de aplicar unas reales y efectivas medidas de protección que estén encaminadas a un buen gobierno en materia de datos personales a la vez que se lleva a cabo una minimización de los posibles riesgos legales, económicos y reputacionales que pudieran derivarse de llevar a cabo una ineficiente práctica en esta materia.[15] Ante esto, y como se irá desarrollando a lo largo de las líneas de este trabajo, los mecanismos basados en la responsabilidad proactiva o *accountability* serán los medios más idóneos y congruentes para el logro de estos objetivos.

[14] El RGPD incluye una pequeña dispensa en relación con los principios de limitación de la finalidad y del plazo de conservación de los datos en el *artículo 89, apartado 1*. En el mismo se establece que se podrán excepcionar dichas limitaciones cuando las finalidades del tratamiento sean relativas al archivo en interés público, a la investigación científica o histórica o con propósitos estadísticos.

[15] EUROPEAN COMISSION (Article 29 Data Protection Working Party). *Opinion 3/2010 on the principle of accountability* [en línea]. Bruselas, 2010. [Fecha de consulta: 02/04/19] [Disponible en: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf*]

1.2. Gobernanza empresarial: Introducción al gobierno corporativo responsable.

Cuando hablamos de gobernanza empresarial nos encontramos ante un concepto que goza de una amplia variedad de definiciones en base a la perspectiva que escojamos para delimitarlo. En primer lugar, es preciso destacar que estamos ante una figura que puede ser nombrada de diversas maneras; gobernanza empresarial, gobierno corporativo, buen gobierno corporativo o, simplemente, buen gobierno. Ante esta variedad de términos para referirnos al mismo concepto, podemos utilizar indistintamente cada uno de ellos cuando queramos hacer referencia al mismo. Considerando la naturaleza del presente trabajo, podemos definir al buen gobierno como todas aquellas actuaciones y decisiones realizadas dentro de la organización interna de una sociedad que, en base a la autonomía de la voluntad, al libre mercado y a los principios de solidaridad y responsabilidad, están encaminadas a llevar a cabo una efectiva dirección y ordenación empresarial.[16]

Este fenómeno se ha ido desarrollando de manera desigual en los diferentes países desde su surgimiento en EE.UU. y Reino Unido. Dentro del ámbito de la Unión Europea su perfeccionamiento no ha sido distinto, pues a pesar del derecho comunitario y la jurisprudencia sigue existiendo una falta de homogeneidad en todo lo relativo al derecho privado, la estructura empresarial, las especificidades nacionales y la diversidad de las estructuras económicas de los diferentes países.[17] Por ello, las técnicas de derecho "blando" u orientaciones incorporadas en Códigos de Buen Gobierno han resultado especialmente útiles para incorporar en la actividad global, pero también europea y española, las mejores prácticas en relación con la gestión y dirección de empresas.

Cuando hablamos del movimiento de gobernanza empresarial en España debemos remontarnos a 1997, momento en el cual se elabora el primer código de conducta relativo al buen gobierno corporativo, el Código Olivencia. Con este documento se buscaba poner solución a los diversos problemas que existían sobre los Consejos de Administración de las sociedades cotizadas españolas, estableciendo para ello una serie de recomendaciones relativas a la composición, intervención, delegación, etc., de los mismos. A partir de este

[16] PÉREZ CARRILLO, E.F. "Gobierno corporativo comparado". En: *Gobierno corporativo y responsabilidad social de las empresas*. Madrid, 2009. Págs. 49-75.
[17] *Ibíd.*

momento, y con el surgimiento de otros documentos similares con el paso del tiempo [18], se ha venido configurando en España nuestro modelo de gobierno corporativo. [19]

A efectos de hacer una correspondencia de este fenómeno con el objeto del presente trabajo, encontramos como el buen gobierno desarrollado en el seno de los Consejos de Administración se relaciona muy a menudo con el llamado *compliance* empresarial.[20] En primer lugar, encontramos que ambas poseen la misma naturaleza autorregulativa, donde a pesar de nacer con un ánimo voluntario pueden llegar a desarrollar un carácter vinculante para la organización que se vea sometida a su ámbito de aplicación. Otro de los espacios fundamentales donde convergen los caminos de estas dos figuras, especialmente relacionado con la protección de datos y la ciberseguridad, es en la gestión de riesgos. El *Código de buen gobierno de las sociedades cotizadas* elaborado por la CNMV, cuya actual versión data de 2015, establece que esta gestión de riesgos deberá estar directamente ejercida por el consejo, ya sea a través de una comisión de auditoria u otra análoga. [21] En relación con esto último, debemos considerar que dicho código alude a los potenciales riesgos generales y/o económicos que puede enfrentar una sociedad cotizada, no haciendo mención explícita a los posibles riesgos en la privacidad de los datos o relacionados con la ciberseguridad. No obstante, todas las estrategias operativas y actuaciones recomendadas por este código de buen gobierno pueden aplicarse y adaptarse a estos últimos. [22]

Es importante destacar que al igual que ocurre con los planes de *compliance*, los códigos de buen gobierno pueden ser una herramienta idónea para evitar que se produzcan conductas delictivas en el seno de la organización empresarial.[23] Por lo que, ante la nueva regulación existente tanto en materia de protección de datos como en ciberseguridad, y

[18] Véase el Informe Aldama de 2002 para el Fomento de la Transparencia y la Seguridad de los Mercados Financieros y Sociedades Cotizadas.
[19] GARCÍA COTO, D.J. y BLANCO DIEGO, R. "Códigos de buen gobierno en Europa y Estado Unidos. Especial referencia a los códigos de Olivencia y Aldama en España". En: *Análisis financiero. Número extraordinario sobre "Corporate Governance".* Nº 90. 2010. Págs. 49-63.
[20] Entendiendo este *compliance* empresarial desde una perspectiva amplia que abarcar el cumplimiento normativo en todas las materias que pueden afectar a la gestión diaria de una sociedad mercantil, no solo el llamado *compliance* penal, como se fundamenta a lo largo del presente trabajo.
[21] CNMV (COMISIÓN NACIONAL DEL MERCADO DE VALORES). *Código de buen gobierno de las sociedades cotizadas*. [en línea]. Madrid, 2015. [Fecha de consulta: 24/04/19]. [Disponible en: *https://www.cnmv.es/docportal/publicaciones/codigogov/codigo_buen_gobierno.pdf*]
[22] CAZORLA GONZÁLEZ-SERRANO, L. "El deber de diligencia del administrador social y los programas de cumplimiento o "compliance" penal". En: *Lex Mercatoria* Nº 1, 2015.
[23] A modo ejemplificativo, el *Código de buen gobierno de las sociedades cotizadas* anteriormente citado, recoge una serie de recomendaciones y actuaciones encaminadas a la prevención y resolución de los posibles conflictos de intereses que puedan presentarse en el entorno societario.

como se irá desarrollando a lo largo del presente trabajo, no es descabellado pensar que estos mecanismos de autorregulación supondrán un activo muy importante y efectivo para las empresas que quieran desarrollar políticas internas de seguridad y protección sobre datos personales y activos de la información, como ya se está empezando a ver en ciertas organizaciones.

Por otra parte, la posición de las sociedades ante una legislación cada vez más prolija y variada es lo que ha ocasionado que exista una predisposición de las organizaciones empresariales hacia la figura de la autorregulación o *soft law*, donde son las propias empresas las que actúan como garantes de la legalidad, procediendo de una manera preventiva, investigadora y correctiva con el objetivo de evitar posibles sanciones normativas. Además, la implementación y aplicación de estos mecanismos de autorregulación supone un tipo de actuación en aras de la Responsabilidad Social Corporativa (RSC) y una mejoría de la imagen y reputación de la organización. Es importante evidenciar que esta tendencia supone un cambio al modelo tradicional, pues el coste que supone garantizar este cumplimiento normativo es trasladado hacia las empresas.[24]

Pero el problema aquí no radica solamente en que la legislación en materia de protección de datos sea cada vez más amplia y compleja, sino que además nos encontramos con el hecho de que la misma tiene cierto carácter volátil que puede suponer que se encuentre constantemente bajo nuevas reformas y modificaciones. Esto viene motivado de la naturaleza de los propios datos, los cuales tienden a ser inconsistentes y residen en una gran diversidad de sistemas, provocando que las tecnologías actuales de procesamiento de datos sean difícilmente escalables y sostenibles, haciendo que el uso de las mismas sea cada vez más complicado. Todo ello comporta que la normativa y leyes sobre esta materia padezcan un nivel acorde de complejidad que además se ve constantemente matizado o modificado con el objetivo de adaptarse a la realidad cambiante de los datos. [25] Como decía el Profesor Hernández Gil [26] en relación con la naturaleza y carácter del Derecho, "*no se trata de que el Derecho vaya a ordenar nuevas*

[24] GIMENO BEVIÁ, V. "Los programas de «*impact*» como manifestación del deber de diligencia de los administradores*"*. En*: Revista de Derecho de Sociedades*. 2019. Núm.55/2019, pág. 2.
[25] DATOO A. *Legal Data for Banking: Business Optimisation and Regulatory Compliance*. 1 st Ed, 2019
[26] HERNÁNDEZ GIL, A. *Problemas socio culturales de la Informática Jurídica, Ponencia en la Mesa redonda sobre Teleinformática Jurídica*, Fundación para el desarrollo social de las comunicaciones (FUNDESCO). Madrid, 1973.

realidades, sino que el Derecho mismo va a experimentar, en cuanto objeto del conocimiento, una mutación derivada de un modo distinto de ser elaborado, tratado y conocido".[27]

Como consecuencia de esto, la solución idónea que se nos presenta ante esta realidad tan compleja es el buen gobierno corporativo, específicamente, el llamado *Data Governance* o buen gobierno de los datos, una figura que desarrollaremos más profundamente en los puntos posteriores y que en palabras de John Ladley [28] "*constituyen un conjunto de buenas prácticas que optimizan, protegen y aprovechan la información como un activo empresarial al alinear los objetivos de múltiples funciones*".

Fuera de las posibles connotaciones legales que pueden derivarse de una deficiente gestión societaria, encontramos como el gobierno corporativo tiene un enfoque muy vinculado al concepto de valor empresarial. En muchas ocasiones los problemas con el gobierno corporativo surgen como resultado de una serie de cambios en la estructura del capital y organización de las propias empresas, las cuales no son capaces de adaptarse a estos nuevos cambios y acaba suponiendo que las mismas tengan que soportar una serie de cargas económicas importantes.[29]

Ante esta realidad encontramos como el gobierno corporativo o gobernanza empresarial se constituye como un activo fundamental dentro del ámbito de la gestión empresarial, el cual debe ser considerado a efectos de asegurar un correcto desarrollo de las sociedades.[30] Pues bien, si nos adentramos en la esencia y naturaleza del gobierno corporativo encontramos como el mismo se caracteriza por ser una especie de vínculo de unión entre los accionistas y la dirección de la sociedad. Desde este enfoque, el desarrollo del escenario del gobierno corporativo afecta fundamentalmente al ámbito de actuación del consejo de administración, de los directivos y de los consejeros delegados. Por esta razón, numerosos autores sugieren que es conveniente que el buen gobierno abarque todos aquellos procesos y mecanismo que afectan la toma de decisiones desde la alta

[27] DAVARA RODRÍGUEZ, M.A. *Manual de Derecho Informático*.10ª Ed. Pamplona, 2008.
[28] LADLEY, J. *Data Governance: How to Design, Deply and Sustain an Effective Data Governance Program*. Boston, 2012.
[29] VERNIMMEN P., QUIRY P., DALLOCCHIO M., LE FUR Y y SALVI A. *Corporate Finance: Theory and Practice, Fifth Edition.* Págs. 783-795.
[30] CLARKE T. *International Corporate Governance: A Comparative Approach*. 2nd Ed. Routlede, 2011. Págs. 33-83

dirección.[31] La propia OCDE recomienda que los mecanismos y técnicas del gobierno corporativo actúen sobre las decisiones que suponen la creación de valor e intercambio dentro de las empresas y destaca cuatro áreas principales al respecto, siendo una de ellas la transparencia y la información.[32]

En conclusión, en este apartado vemos como el modelo de actuación del gobierno corporativo no solo se conforma como un instrumento idóneo dentro del ámbito de la gestión empresarial, sino que además podemos comprobar como su naturaleza guarda una estrecha similitud con la concepción del *compliance* empresarial o cumplimiento normativo. Ante esto, podemos deducir que este buen gobierno puede actuar como un garante idóneo del cumplimiento normativo en materia protección de datos personales, garantizando al mismo tiempo la participación activa del órgano de administración y de altos mandos sociales en la gestión de las políticas de protección de datos de una sociedad mercantil.

[31] HEIDIRCK & STRUGGLES. *Towards Dynamic Governance 2014: European Corporate Governance Report*. 2014. Pág. 16.
[32] VERNIMMEN P., QUIRY P., DALLOCCHIO M., LE FUR Y. y SALVI A. *Corporate Finance: Theory and Practice, Fifth Edition.* Págs. 783-795.

2. SEGUNDO CAPÍTULO

LA IMPLANTACIÓN RESPONSABLE DE LA PROTECCIÓN DE DATOS EN LA EMPRESA

2.1. El ordenamiento de protección de datos a la luz de las recientes reformas

Habiendo trazado una pequeña introducción sobre cómo se configura la legislación en materia de protección de datos, no hay duda en como esta materia goza de una naturaleza trasversal que afecta a una amplia variedad de sectores. Uno de los que más afectación sufre a consecuencia de la propia naturaleza de la normativa es el sector privado o empresarial, por ello es conveniente realizar un pequeño acercamiento a aquellas novedades que esta normativa ha introducido en este campo y que pueden ser de interés en relación con el presente trabajo.

El RGPD tiene el objetivo de llevar a cabo una reducción de ciertas trabas que existían con la normativa anterior para los responsables y encargados de las empresas, a la vez que garantiza que la protección de datos personales de las personas físicas que sean objeto de tratamiento están correctamente asegurados.[33] Por ejemplo, una de las novedades más destacables la encontramos motivada en su *Considerando 89*, el cual nos habla de la antigua obligación exigida por la *Directiva 95/46/CE* relativa a que se debía notificar con carácter previo el tratamiento de datos a la autoridad de control. Dicho considerando argumenta como esa "*notificación indiscriminada*", que suponía unas amplias cargas administrativas y financieras, no implicaba realmente una mayor protección de los datos. De hecho, esto se demostró en la práctica, y se llegó a determinar que la solución radica en la aplicación e implementación de mecanismos más eficaces y menos gravosos en las organizaciones. [34]

Conjuntamente, el RGPD incluye una serie de previsiones y principios rectores que, pese a no haber sido desarrollado ampliamente por ahora, entiendo que guardan una

[33] EUROPEAN COMISSION. *The GDPR: New opportunities, new obligations*. [En línea] [Fecha de consulta: 26/03/19] [Disponible en: *https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf*]

[34] Considerando 89, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, 27 de abril de 2016, L 119/2.

vinculación muy intensa, incluso directa, con el buen gobierno o gobernanza empresarial, el cumplimiento normativo y los planes de gestión de riesgos.

Por otro lado, tanto el RGPD como la LOPDGDD introducen nuevas previsiones relativas al derecho a la información y a la transparencia para con los interesados a la hora de poder iniciar el tratamiento de los datos. El artículo 13 del RGPD[35] estandariza ciertas obligaciones para el responsable del tratamiento en materia de información que surgen a la hora de iniciar la recolección de datos personales sobre el interesado. La previsión establecida en el artículo viene dividida en cuatro párrafos, los dos primeros regulan el campo de aplicación de la obligación de información en el momento en el que inicia la obtención de los datos personales. Seguidamente, el tercer párrafo estandariza el requerimiento de transmitir la información en caso de un ulterior tratamiento y el cuarto dispone una dispensa del deber de información recogido en los dos primero párrafos en el caso de que el interesado ya este en posesión de dicha información.[36] Esta previsión viene completada con los dispuesto en el artículo 14 en el caso de que los datos personales no sean obtenidos directamente de la persona interesada.

Otra de las novedades más notorias introducidas por esta nueva regulación es la aparición del Delegado de Protección de Datos (DPO en adelante),[37] una figura que deberá ser designada de manera imperativa en las organizaciones cuando ser den ciertas características.[38] Esta obligación viene motivada por los buenos resultados que ha planteado en países de la UE donde ya existía [39] , ya que este rol se plantea como uno de los elementos y activos necesarios para garantizar el cumplimiento normativo dentro de la esfera del RGPD. [40]A su vez, este reglamento también promociona, como se venía

[35] En la *LOPDGDD* encontramos esta obligación dentro del Cap. I, Titulo III, específicamente dentro del *artículo 11*.
[36] KAZEMI, R. *General Data Protection Regulation (GDPR)*. Hamburg, 2018.
[37] Si bien es cierto, el *Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000*, ya incluía y regulaba esta figura. No obstante, recogía la designación y establecimiento de la misma únicamente en sede de instituciones y cuerpos de la Unión Europea, no afectando al sector privado ni publico de los estados miembros.
[38] Véase art. 37.1 *Reglamento (UE) 2016/679 de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* y art. 34 *Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales.*
[39] La legislación de protección de datos alemana reconoce la figura del Delegado de Protección de Datos (*Datenschutzbeauftragte*r) desde hace más de 30 años, donde ha demostrado ser uno de los elementos clave para el cumplimiento de esta normativa0 . Del mismo modo, ciertos países establecían en sus ordenamientos la posibilidad de designar de manera voluntaria un DPO, como es el caso de Polonia, Francia y Suecia.
[40] VOIGT P. y VON DEM BUSSCHE A. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham, 2017.

haciendo con la normativa precedente, la adhesión a códigos de conducta y la adscripción a mecanismos de certificación como recoge la Sección V del Cap. IV.[41]

El *Considerando 81* del RGPD reconoce que la adhesión a estos instrumentos por parte del encargado puede servir como un dispositivo valido para demostrar el cumplimiento por parte del responsable siendo, por tanto, un método idóneo para cumplir con el principio de responsabilidad proactiva o *accountability*.

Asimismo, se puede ver como existe un aire incentivador en toda esta reciente regulación hacia la implementación de este tipo de códigos y mecanismos en el interior de las organizaciones, dejando entre ver como el legislador europeo apuesta cada vez más por una potenciación del *soft law* como instrumentos de autorregulación. En este sentido, se reconoce del mismo modo que estos podrán establecer obligaciones para ambas partes del tratamiento, por lo que encontramos como la naturaleza vinculante e imperativa de este *soft law* va ganando fuerza en perjuicio de la voluntariedad que le caracterizaba. Además, esta inclusión dentro de la norma europea no ha sido pequeña, pues en la Sección V del Capítulo IV encontramos cuatro amplios artículos relativos a la materia (arts. 40 al 43), contenido que se ve reflejado del mismo modo en la normativa española que desarrolla esta temática dentro de los artículos 38 y 39 del Capítulo V de la LOPDGDD.

La implementación de estos instrumentos dentro de una sociedad mercantil supone una serie de ventajas prácticas en cuanto al desarrollo de la gestión empresarial. En primer lugar, y la más conveniente, es que la adhesión o certificación por parte de los mismos suponen la adecuación a la norma de protección de datos por parte de la sociedad, evitando de este modo las potenciales sanciones que prevé la ley. Por otro lado, la implantación de las medidas seguridad requeridas por estos mecanismos hace que dicho nivel de seguridad y control se puede extender a otras áreas dentro de la estructura empresarial, suponiendo de este modo una optimización de los procesos y la continuidad del negocio.

Del mismo modo, estos mecanismos tienen un alto impacto positivo en la imagen y reputación de la empresa, satisfaciendo de este modo las demandas de todos los sujetos

[41] MARTÍNEZ-MARTÍNEZ, D.F. *Unification of personal data protection in the European Union: Challenges and implications.* El profesional de la información, v. 29, n. 1, pp. 185-194. 2018, enero-febrero. [Fecha de consulta: 26/03/19] [Disponible en: *https://doi.org/10.3145/epi.2018.ene.17*]

interesados de la sociedad.[42] Igualmente, se pueden evitar auditorias constantes por parte de los proveedores a efectos de verificar que la empresa cumple con lo dispuesto en la ley, pues al estar certificados solo tendremos que pasar por dicha evaluación en el momento de cumplir con los dispuesto en el código de conducta, sello o certificación correspondiente.[43]

2.2. Requisitos de implantación formal del RGPD / LOPDGDD

Uno de los mayores retos a los que se enfrentan las organizaciones y empresas sometidas al ámbito de aplicación del RGPD es transformar los requerimientos legales exigidos por esta normativa en actuaciones u operaciones de carácter responsable y sostenible. Esta necesidad goza de cierta dificultad a la hora de llevarla a la práctica, pues además nos hallamos ante un escenario marcado por una naturaleza desigual en base al tipo de sociedad o empresa ante la que nos encontremos. Mientras que algunas organizaciones, por ejemplo, de servicios financieros o del sector sanitario, están en gran medida acostumbradas a lidiar con exigencias y obligaciones legales, otras se están viendo en una posición en la que nunca habían estado, pues están experimentando por primera vez con el RGPD la necesidad de implantar dentro o de su estructura empresarial una serie de estrictas medidas en materia de protección de datos.[44]

El perfeccionamiento de una cultura empresarial preocupada por la gestión de los datos personales radica en que la seguridad de los mismos se conciba como un elemento integral en todos los niveles de la empresa. Para ello, las sociedades deben asegurar la protección de los activos de información de la organización y mostrar una actitud diligente con el cumplimiento normativo en materia de protección de datos. Una vez que la estructura empresarial haya implementado políticas que revelen un nivel de riesgo

[42] YÁÑEZ, J. "Las nuevas certificaciones oficiales a la luz del RGPD". En: *Actualidad Jurídica Aranzadi*. Núm. 933/2017, 2017.
[43] *Reglamento (UE) 2016/679 de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*: El art. 28 relativo al encargado del tratamiento establece que este "*pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable*".
[44] VV.AA. (META COMPLIANCE). *GDPR Best Practices Implementation Guide: Transforming GDPR Requirements into Compliant Operational Behaviours*.

aceptable es cuando podemos hablar de que la administración de la empresa ha actuado con diligencia a la hora de establecer un nivel adecuado en sus prácticas de seguridad.[45]

Con el objetivo de llevar a cabo una efectiva implantación de los requisitos formales que recoge la normativa, tanto la europea como la nacional, en materia de protección de datos, las empresas deben considerar previamente cuales son las implicaciones que plantea el cumplimiento normativo en materia de protección de datos.

En primer lugar, las sociedades tienen que vincular la privacidad y la protección de datos al más alto nivel dentro de la actividad empresarial. En este sentido, la OCDE aboga por que el consejo de administración de las sociedades efectúe una participación activa y una alta implicación en estos asuntos, designado roles y responsabilidades en la materia, garantizando de este modo una integración plena de la protección de datos en todos los estratos de la empresa. [46] Las cuestiones relativas a este aspecto y sus especificidades se detallan en los puntos posteriores del presente trabajo.

Por otro lado, la empresa tiene que llevar a cabo una clasificación de los datos personales que posee y sobre los que realiza el tratamiento. Esta gestión permite a las organizaciones conocer si trabaja con datos personales especialmente sensibles, además de que esto posibilita llevar a cabo el cumplimiento de las obligaciones relativas a la conservación y supresión de los datos. Tener una constancia cierta de estas dos previsiones es muy importante, pues puede suponer la existencia de nuevas obligaciones para la sociedad, como la elaboración de una Evaluación de Impacto de Protección de Datos (EIPD).[47]

Es importante a su vez evaluar si existen contratos o convenios con terceras partes interesadas de la empresa con las cuales la misma comparte información. La normativa de protección de datos requiere que las empresas pongan en orden sus acuerdos relativos a la privacidad y a la seguridad de los datos para cada uno de los tratamientos que lleve a cabo con dichos terceros. Esta previsión viene intensificada en el supuesto de que estemos

[45] WARSINKE, J. "Security and Risk Management". En: *CISSP: Certified Information Systems Security Professional.* 2019
[46] OECD. *Principles of Corporate Governance*. [En línea] [Fecha de consulta: 06/06/19] [Disponible en: *https://www.oecd.org/daf/ca/Corporate-Governance-Principles-ENG.pdf*].
[47] HERAS CARRASCO, R. "Evaluaciones de Impacto". En: *I+S*: *Revista de la Sociedad Española de Informática y Salud*. Núm. 127, 2018. Págs. 24-27. [En línea] [Fecha de consulta: 06/06/19] [Disponible en: *https://dialnet.unirioja.es/servlet/autor?codigo=4444603#ArticulosRevistas*].

hablando de Transferencias Internacionales de Datos (TID), donde además se deberán de atender una serie de requisitos especiales y estar a los dispuesto por la Comisión Europea y el *Privacy Shield*[48]- con EE. UU- sobre los países y entidades que reúnen las condiciones necesarias de seguridad. [49]

En lo relativo a las medidas de seguridad, la participación activa de la empresa es muy importante a la hora de establecer procedimientos que se anticipen adecuadamente a las potenciales brechas de seguridad que puedan afectar a los datos personales.[50] Asimismo, fomentar la sensibilización de los trabajadores de la organización en materia de protección de datos es esencial a la hora de garantizar el cumplimiento normativo en todos los niveles de la organización. El establecimiento de actividades de formación y concienciación de los empleados que impliquen una participación activa de estos constituye a su vez un mecanismo satisfactorio para cumplir con el principio de responsabilidad proactiva, pues se presenta como un activo idóneo para la empresa a la hora de demostrar el cumplimiento e implicación con el RGPD y la LOPDGDD.[51] No obstante, conseguir que se cree una cultura de la seguridad dentro de la empresa es uno de objetivos que más dificultad plantean, pues no solo exige una un gran inversión de

[48] KOSSEFF, J. *Cibersecurity Law*. 2017. Págs. 340-346: De carácter previo al *Privacy Shield*, las compañías en Estados Unidos estaban adheridas a un programa de certificación conocido como *Safe Harbour*, negociado entre EE. UU y la Unión Europea, el cual requería a las sociedades mercantiles estadounidenses reunir una serie de principios relativos a la protección de datos para poder realizar transferencias internacionales. No obstante, en octubre de 2015, el Tribunal de Justicia de la UE (*Caso Schrems vs. Autoridad Europea de Protección de Datos*) canceló dicho programa a consecuencia de que las filtraciones sobre la inteligencia estadounidense reveladas por Edward Snowden demostraban que este no reunía las condiciones de seguridad que afirmaba el gobierno estadounidense. A raíz de esto, se iniciaron de nuevo las negociaciones para reestablecer un marco que permitiese el intercambio de datos entre EE. UU y la UE, dando lugar al actual *Privacy Shield*.

[49] COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo y al Consejo relativa al Intercambio y protección de los datos personales en un mundo globalizado. 2017. [En línea] [Fecha de consulta: 06/06/19]. [Disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017DC0007&from=EN*].

[50] EUROPEAN PARLIAMENT. *A Governance Framework for Algorithmic Accountability and Transparency*. 2019. [En línea] [Fecha de consulta: 07/06/19]. [Disponible en: *http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf*]: En este punto no está de más destacar un estudio reciente elaborado por el Parlamento Europeo que menciona la llamada "auto-organización de las empresas", un concepto que hace referencia a aquellas medidas adoptadas por las sociedades a efectos de reducir los riesgos mediante la implantación en la empresa de principios y normas reflejen el interés público, la evaluación interna de la calidad en relación con determinados riesgos, etc. Esta "auto-organización" suele integrarse generalmente dentro de las estrategias de responsabilidad social corporativa de la empresa y sirve para aumentar la reputación o imagen de la sociedad, o para evitar dañar la misma.

[51] OUWERKERK, E. "The Value Chain: Beware of GDPR – Take your Cyber Risk Responsability More Seriously". En: CHISHTI, S. *The InsurTech Book*. 2018. Págs. 175-178 [En línea] [Fecha de consulta: 06/06/19]. [Disponible en: *https://onlinelibrary.wiley.com/doi/10.1002/9781119444565.ch40#*].

tiempo, sino que además supone la necesidad de que exista una voluntad y participación conjunta de todos los sujetos de la organización.[52]

Además de todo lo anteriormente expuesto, es esencial para garantizar la continuidad y efectividad del cumplimiento a lo largo del tiempo que la empresa establezca una serie de políticas y planes de actuación en materia de privacidad y protección de los datos. Para ello, una de las fórmulas más eficaces y, a la larga, más sencilla es el seguimiento de códigos de conducta o la adhesión a mecanismos de certificación o sellos de garantía. Esta previsión se ha ido desarrollando a lo largo del presente trabajo y se especificara en el punto siguiente aquellas cuestiones más específicas del mismo, así como, la justificación de por qué estas medidas se constituyen como un gran aliado de cumplimiento normativo en la esfera empresarial.[53]

Para poner fin a esta exposición sobre las necesarias formalidades de implantación del RGPD y de la LOPD dentro de la empresa es necesario referirse a la figura del Delegado de Protección de Datos (DPO/DPD). El nombramiento de esta figura es una obligación para aquellas entidades que reúnan, de manera general, alguna de las condiciones del art. 37. 1 del RGPD y, de manera específica, aquellas recogidas en el art. 34.1 de la LOPDGDD. Esta figura no exige que se implante en la organización interna de la empresa pues se puede suplir el cumplimiento de esta necesidad mediante la formalización de un contrato mercantil con un tercero externo a la misma, tal como recoge el propio reglamento.[54] No obstante, su vinculación dentro de la estructura de la organización empresarial es un método más idóneo, especialmente en relación con el cumplimiento normativo y el buen gobierno como se verá en los puntos posteriores.

En resumen, los asuntos legales y en materia de cumplimiento normativo relacionados con la ciberseguridad y la protección de datos que deben afrontar las sociedades vienen predefinidos en términos de aceptación, razonabilidad y preparación. Las sociedades deben trabajar para asegurar que cada previsión aplicable en materia de

[52] INCIBE. *Desarrollar cultura en seguridad*. [En línea] [Fecha de consulta: 07/06/19]. [Disponible en: *https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_desarrollar-cultura-en-seguridad.pdf*].
[53] FOULSHAM, M.; HITCHEN, B. y DENLEY, A. GDPR: *How To Achieve and Maintain Compliance. Nueva York*, 2019.
[54] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea, 27 de abril de 2016, L 119/2.*

protección de datos se cumple siguiendo los estándares establecidos. Asimismo, los miembros del consejo de administración deben estar al tanto sobre todos estos procesos pues se garantiza de este modo su implicación en relación con los deberes fiduciarios que les son propios, además de servir como apoyo a la hora de probar a los interesados y autoridades que han actuado con la diligencia y lealtad debida en caso de un potencial evento que perjudique la confidencialidad, integridad y disponibilidad de los datos que trata la sociedad.[55]

2.3. El buen gobierno de los datos y su vinculación con el principio de responsabilidad proactiva o accountability

El principio de responsabilidad proactiva o *accountability* es una de las grandes novedades introducidas a la luz de la nueva regulación europea en materia de protección de datos personales. Si acudimos al RGPD encontramos en su *Considerando 74* que una de las principales motivaciones de esta regulación busca establecer y garantizar que la persona responsable del tratamiento está sometida a un correcto régimen de responsabilidad. Dicho considerando también nos habla de que el responsable deberá implementar una serie de medidas eficaces que demuestren su cumplimiento en esta materia y que lo está haciendo de una manera diligente, pues las medidas que se adopten deberán considerar en todo caso cual es *"la naturaleza, el ámbito, el contexto y los fines del tratamiento".* [56] Del mismo modo, este principio de responsabilidad se concibe como un mecanismo de cooperación entre el responsable del tratamiento y la autoridad de control, con el principal objetivo de garantizar las operaciones de supervisión del tratamiento. [57] Esto ha supuesto que el rol de las empresas en materia de protección de datos que existía hasta ahora haya dado un vuelco de 180 grados, pasando de un estado pasivo a la obligación de tener que adoptar una posición marcadamente activa.

[55] RISHIKOF, H. & SULLIVAN, C. "Legal and Compliance". En: ANTONUCCI, D. *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. 2017. Págs. 255 – 270.
[56] Considerando 74, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, 27 de abril de 2016, L 119/2.
[57] Considerando 82, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, 27 de abril de 2016, L 119/2.

El concepto de responsabilidad proactiva o *accountability* en materia de protección de datos apareció formalmente durante la década de 1980 de la mano de la OECD (*Organisation for Economic Co-operation and Development / Organización para la Cooperación y el Desarrollo Económicos*). El 23 de septiembre de 1980 dicha organización publicó las llamadas *Guías para la protección de la privacidad y los flujos transfronterizos de datos personales,* las cuales eran un tipo de código de conducta que instaba a que los responsables del tratamiento de los datos debían ser los responsables de cumplir las medidas necesarias que garantizasen una serie de principios fundamentales en materia de privacidad y protección de datos. [58] Una previsión muy importante que a su vez incluía este código de conducta es que la responsabilidad del cumplimiento de las normas y las decisiones relativas a la protección de los datos debe recaer siempre en la figura del responsable del tratamiento, con independencia de que en dicho tratamiento existan terceras partes u encargados que a su vez realicen actividades de tratamiento.[59]

Posteriormente, el Grupo de Trabajo del artículo 29 de la Comisión Europea (GT Art. 29, en adelante) [60] adoptó el 13 de julio de 2010 la *Opinión 3/2010 relativa al principio de responsabilidad proactiva o accountability,* la cual se elaboró con el objetivo de asegurar que con ese principio se garantiza un nivel mínimo de certeza jurídica a la vez que se permite que la escalabilidad tiene un grado eficiente de actuación dentro de cada una de las entidades.

Del mismo modo, se discute en el documento como el citado principio puede afectar a otras áreas como las transferencias internacionales de datos, los requerimientos de las notificaciones, las sanciones y el desarrollo de los programas de certificación y de los sellos. No obstante, la apreciación más importante que encontramos dentro este documento es que el GT Art. 29 afirma que el marco jurídico de la UE necesita una serie de herramientas adicionales para promover la puesta en práctica de la protección de datos y por ello anima a la Comisión a enmendar la Directiva 95/46/CE (la por entonces

[58] OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* [En línea] [Fecha de consulta: 22/05/19] [Disponible en: *https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#preface*].

[59] A pesar de esta afirmación, las propias directrices incluidas en dicha guía no impedían en ningún momento que esas otras partes que pueden llevar a cabo ciertas actividades de tratamiento rindieran también cuentas en base a sus actuaciones. A este respecto, se decía que las sanciones por incumplimiento en materia de confidencialidad podían dirigirse a todos los sujetos que formaran parte del tratamiento de los datos.

[60] Es un grupo de trabajo de carácter independiente dentro del ámbito de la UE que se ha encargado de llevar a cabo todos aquellos asuntos relativos a la protección de los datos personales y la privacidad hasta la entrada en vigor del RGPD el 25 de mayo de 2018.

normativa en vigor) a estos efectos. Específicamente se habla de proponer un principio de responsabilidad proactiva o *accountability* que requiera que los responsables del tratamiento pongan sobre la mesa una serie de apropiadas y efectivas medidas que aseguren que los principios y obligaciones recogidos en la normativa europea de protección de datos son respetados. Pero esto no acaba ahí, sino que además se habla de poder demostrar que se está cumpliendo de manera diligente con la normativa siempre que las autoridades de control y supervisión lo soliciten.[61]

En consideración con lo anteriormente expuesto, la Autoridad de Control Francesa o CNIL (*Commission Nationale de l'Informatique et des Libertés*) quiso llevar a la práctica lo dispuesto en la Opinión 3/2010 sobre responsabilidad proactiva en el año 2015, antes de la entrada en vigor del RGPD. A consecuencia de esto, se aprobó una norma de cumplimiento en materia de protección de datos [62] que recogió entre su articulado una serie de disposiciones relacionadas con el principio de responsabilidad proactiva, las cuales disponían para los responsables y encargados del tratamiento una serie de obligaciones de carácter "*proactivo y sistemático*". Con esta normativa se establecía un sistema mediante el cual todas aquellas organizaciones que cumplieran lo establecido en dicha disposición y fueran capaces de demostrarlo obtendrían un *sello de cumplimiento del principio de accountability* de la CNIL. [63] Es decir, con este sistema la CNIL creaba una especie de sistema de certificación o sello para aquellas empresas que cumplían con estas disposiciones, actuando como una especie de entidad certificadora.

Como es lógico, este tipo de manifestaciones podemos encontrarlas en la realidad actual, pues una de las medidas más efectivas a la hora de garantizar el cumplimiento relativo a la protección de datos y poder avalar las medidas de seguridad que exige la normativa es mediante la adhesión a códigos de conducta o mecanismos de certificación.[64] El RGPD establece una serie previsiones en las que dispone como la vinculación a este tipo de *soft law* puede considerarse como un medio de prueba de que la empresa está cumpliendo con lo dispuesto en el ordenamiento jurídico. No obstante,

[61] EUROPEAN COMISSION (Article 29 Data Protection Working Party). *Opinion 3/2010 on the principle of accountability* [en línea]. Bruselas, 2010. [Fecha de consulta: 02/04/19] [Disponible en: *https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2010/wp173_en.pdf*]
[62] Véase *Privacy seals on privacy governance procedures, CNIL.* Disponible en: https://www.cnil.fr/sites/default/files/typo/document/CNIL_Privacy_Seal-Governance-EN.pdf
[63] RAMOS F. *El principio de Accountability o de Responsabilidad Proactiva*. [en línea] [Disponible en *http://www.dpoitlaw.com/el-principio-de-accountability-o-de-responsabilidad-proactiva/]*
[64] ALBERTO GONZALEX, P. "Responsabilidad proactiva en los tratamientos masivos de datos". En: *Dilemata, Revista Internacional de Éticas Aplicadas*. 2017, Nº24, págs. 115-129.

esta inclusión en la norma no es un *numerus clausus* y, por lo tanto, no impide al responsable del tratamiento acreditar el cumplimiento de la misma ante la autoridad de control mediante otros medios.[65] En este sentido como se ha dado pie en apartados anteriores del presente trabajo, uno de los aspectos más importantes que debemos considerar en este ámbito es la vinculación de estas exigencias legales con la figura del gobierno corporativo, que nos permite no solo garantizar un cumplimento en esta materia sino que además se vincula al órgano de dirección y a los altos directivos de la empresa en la toma de decisiones directas y en el control de las políticas de protección de datos personales.[66]

Si bien es cierto, dentro de la normativa encontramos otros instrumentos garantes del principio de responsabilidad proactiva que permiten no solo cumplir con la norma con una mayor facilidad, sino también poder demostrar de manera fehaciente dicho cumplimiento. A estos efectos, la Evaluación de Impacto (PIA) [67] se prevé como un sistema idóneo para garantizar un cumplimiento diligente y demostrable especialmente cuando hablamos de los tratamientos que implican un alto riesgo. Lo interesante de esa materia, especialmente en relación con los mecanismos de certificación y los sellos de garantía es que estas evaluaciones de impacto pueden ser desarrolladas en las mismas organizaciones mediante un método propio, pero también se puede adoptar un método desarrollado por terceros, como bien serían los organismos de estandarización y diferentes asociaciones de garantía.[68]

En consideración con todo lo anterior podemos deducir que dentro de la estructura organizativa de una sociedad mercantil es necesario que existan una serie de políticas o instrumentos que garanticen la protección de datos personales o, dicho de otro modo, establecer un sistema de buen gobierno sobre los datos. Algunos autores se refieren a esta

[65] THOMPSON REUTERS ARANZADI. *Sector Retail. Guía Corporate Compliance y Protección de Datos*. Pamplona, 2018.
[66] A modo ejemplificativo, uno de los métodos más eficientes para proteger los activos de información de una empresa consiste en la implantación de un SGSI (Sistema de Seguridad de la Información) mediante la implementación de la norma ISO que lo regula (UNE-ISO 27000:2009 y ss.). Según dispone la UNE-ISO 27000:2009, el SGSI garantiza el apoyo visible y compromiso de la alta dirección, constituye un programa efectivo de formación, concienciación y educación sobre la seguridad de la información y permite la alineación de la misma con los objetivos de la sociedad. Además, es evidente que la existencia de esta figura dentro de las organizaciones es uno de los principales mecanismos para demostrar el cumplimiento normativo, específicamente la UNE-ISO 27002:2005, relativa a las buenas prácticas para la gestión de la sociedad de la información.
[67] *Véanse artículos 35 y 36 del RGPD.*
[68] AUTORITAT CATALANA DE PROTECCIÓ DE DADES. *Guía práctica. Evaluación de impacto relativa a la protección de datos.* 2018.

gestión como el llamado *Data Governance* o *Buen Gobierno de los Datos,* el cual consiste en delegar, implementar y encomendar dentro de organización societaria la autoridad, control y dirección de la administración de los activos de la información, es decir, de los datos que posee y trata la empresa.[69] Debemos distinguir este concepto de otros similares como son *Information Governance* y *IT Governance.* El primero de ellos hace referencia a aquellas políticas o procedimientos que se llevan a cabo dentro de una organización con el objetivo de optimizar y aprovechar la información a la vez que esta se mantiene actualizada y segura, cumpliendo con las posibles obligaciones legales existentes y con los objetivos perseguidos por la sociedad. Por otro lado, el *IT Governance* consiste en establecer una serie de objetivos y buenas prácticas encaminadas a conseguir el máximo aprovechamiento de las inversiones que haya realizado la sociedad en tecnologías de la información y la comunicación. Es decir, busca alinear los objetivos de la sociedad con la estrategia IT para obtener valor de negocio.[70] Para nuestro interés en relación con el tema del presente trabajo y para evitar excederse en la materia vamos a limitarnos a exponer únicamente las especificidades relativas al *Data Governance*.

Ahora bien, debemos dejar claro que el buen gobierno de los datos no es simplemente un proceso de gestión rutinario que pueda satisfacerse por medio de la actuación de los técnicos o responsables de IT de una empresa. El *Data Governance* debe plantearse desde un enfoque más amplio que asegure la implicación del conjunto de la organización llegando incluso hasta el órgano de administración de la sociedad. Es decir, es necesario que exista dentro la empresa un marco estructurado con diferentes roles y niveles que asegure la correcta gestión de los datos y, por lo tanto, garantice la protección de los mismos y vele por el cumplimiento normativo en esta materia.[71]

En resumen, para poder garantizar que el buen gobierno de los datos se desarrolla en un correcto marco de actuación dentro de la empresa debemos determinar, como mínimo, (1) una serie de políticas que establezcan como la sociedad lleva a cabo la gestión

[69] DATOO A. *Legal Data for Banking: Business Optimisation and Regulatory Compliance*. 1 st Ed, 2019: Todo esto entendido dentro de un marco de responsabilidad (*accountability*) y procesos organizativos.
[70] SMALLWOOD, R. *Information Governance: Concepts, Strategies and Best Practices*. 2014. Págs.15-22: Debemos destacar que estas tres figuras forman un subconjunto que se encuentra dentro del Buen Gobierno Corporativo, no conformando como tal una figura propia e independiente de este concepto.
[71] LADLEY, J. *Data Governance: How to Design, Deply and Sustain an Effective Data Governance Program*. Boston, 2012: Todo esto sin perjuicio de que, como es lógico, aquellas personas encargadas de la gestión técnica y al cargo de las tecnologías de la información dentro de la empresa deban asumir funciones propias de su cargo que garanticen la protección de los activos de información y de los datos.

y medidas de protección de los datos; (2) los roles y responsabilidades de aquellos que estén al mando de la gestión de los mismos y, por último, (3) una serie de procedimientos básicos que garanticen la claridad, consistencia y coordinación entre las medidas y agentes involucrados.[72]

[72] GORDON, K. *Principles of Data Management: Facilitating Information Sharing.* London, 2014.

3. TERCER CAPÍTULO

GOBERNANZA DE SOCIEDADES MERCANTILES Y COMPETENCIAS EN MATERIA DE PROTECCIÓN DE DATOS

Una vez analizado a lo largo del presente trabajo como el buen gobierno de los datos o *Data Governance* se integra dentro de un marco de trabajo en relación directa con el principio de responsabilidad proactiva o *accountability*, quedaría por dilucidar cuales son -o deberían ser- las relaciones entre competencias funcionales relativas a la protección de datos y el sistema de distribución de competencias y responsabilidades propio del derecho de sociedades, conforme también, a los principios de buen gobierno societario y a la distribución legal de funciones de los órganos de sociedades mercantiles. Dejamos ya indicado que, a la luz de lo dispuesto en la Ley de Sociedades de Capital, nos centramos en el órgano de administración, con especial alusión al Consejo dado que es sobre este órgano sobre el que recae la competencia de administrar la persona jurídica.

La desconexión entre la ciberseguridad y la protección de datos con los objetivos principales de la sociedad, así como la omisión de dichas materias en los planes estratégicos y la falta de vinculación con el órgano de administración constituyen un conjunto de actuaciones que no solo son contrarias a la naturaleza del buen gobierno corporativo, sino que además son desencadenantes de una serie de riesgos que pueden afectar de manera muy negativa al cumplimiento normativo por parte de la empresa.

3.1. El órgano de administración: Especial referencia al Consejo

Por su especial sofisticación organizativa nos vamos a centrar en la configuración de este órgano como Consejo. El Consejo de Administración de las sociedades va a marcar aquellas pautas y estrategias por las que la persona jurídica se rija, todo ello sin perjuicio de las leyes o normas existentes que le sean de aplicación y de los Estatutos sociales. Además, y a modo de fuente complementaria, dicho órgano deberá actuar conforme a las previsiones del buen gobierno corporativo, el cual se concentra principalmente en establecer las condiciones necesarias para que la empresa actúe atendiendo al interés de los accionistas y demás interesados, al mismo tiempo que dirige la actuación de la sociedad, en términos de ética, legalidad y justicia, hacia el interés

perseguido por esta.[73] En la actualidad, la delimitación legal explícita del papel del órgano de administración, ya sea en su configuración como consejo o en cualquier otra, son apenas existentes, y es por ello que debemos recurrir a las grandes declaraciones sobre gobierno corporativo para orientar esta investigación y para poder aportar sugerencias.

El Consejo de Administración se configura como un órgano colegiado, es decir, las decisiones que vayan a afectar a la gestión empresarial deberán tomarse de una forma unitaria por todos los miembros del consejo, ya que de carácter individual cada uno de sus miembros no posee facultades de actuación salvo que se le hayan delegado por acuerdo de dicho órgano.[74] Es decir, aquellas decisiones fundamentales que vayan a marcar la dirección y funcionamiento de la sociedad deberán ser resultado de un acuerdo conjunto aprobado en sede del Consejo de Administración por sus miembros, no pudiendo actuar de manera independiente cada uno de ellos, salvo que se hayan delegado en él ciertas funciones.[75] A este respecto, la delegación de una serie de funciones ejecutivas en uno de los miembros del consejo es una práctica habitual y necesaria para conseguir una gestión eficiente de la sociedad. Ese miembro del consejo sobre el que se delegarán las funciones que estime el propio órgano, es el conocido como Consejero Delegado (CEO, por sus siglas en inglés), que de carácter general será el encargado de celebrar y ejecutar contratos en nombre de la sociedad, así como demás funciones generales de tipo ejecutivo.[76] Asimismo, estas funciones también podrán ser delegadas en una varias comisiones ejecutivas siempre y cuando se establezca el contenido, los límites y las modalidades de dicha delegación. [77]

En relación con las responsabilidades del Consejo de Administración y el buen gobierno corporativo, una de las principales previsiones que plantea la OCDE es la asunción de funciones clave por parte de dicho órgano. En su *Guía relativa a los principios de gobernanza corporativa* se plantea que es conveniente que el consejo sea el

[73] WARSINKE, J. "Security and Risk Management". En: *CISSP: Certified Information Systems Security Professional*. 2019
[74] Art. 249 *Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital.*
[75] La LSC establece en el *articulo 249 bis* una serie de funciones que son indelegables y que, por lo tanto, deberán estar siempre en manos del consejo de administración en su conjunto,
[76] En este sentido, es muy importante no confundir la delegación de funciones o mandatos que realiza el consejo de administración sobre el CEO con los actos de apoderamiento, los cuales se pueden conferir sobre cualquier persona o tercero no siendo necesario que este forme parte del propio órgano colegiado.
[77] Art. 249 *Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital*

responsable de guiar y revisar los principales planes de acción de la empresa, los procedimientos y políticas de gestión de riesgos y la monitorización de la implementación de las actuaciones corporativas. Asimismo, se especifica que este órgano debe asegurar que existen los sistemas de control necesarios dentro de la sociedad que aseguren el control de los sistemas de gestión de riesgos y el cumplimiento normativo. [78] Con este trasfondo, podemos presumir que la gestión de la ciberseguridad y la protección de datos dentro en las sociedades corresponde implementarla a través de una implicación activa del Consejo de Administración.

Conforme a la premisa establecida, el órgano de administración debería ser el encargado de establecer las directrices principales y llevar a cabo un seguimiento de las mismas. No porque exista una obligación legal establecida para las sociedades, sino por razón de la coherencia interpretativa entre las funciones del órgano y las exigencias de la gestión de la ciberseguridad y la protección de datos, conforme a los principios del buen gobierno corporativo. Esta interpretación es acorde con el principio de responsabilidad proactiva o *accountability*, al que nos referíamos, ya que la implicación del órgano máximo de la gestión societaria contribuiría a demostrar el cumplimiento de la persona jurídica en relación con la normativa de protección de datos y ciberseguridad.[79]

Dentro de las grandes declaraciones sobre gobernanza ya se van conociendo los primeros ejemplos en los que se apunta a esta interrelación. Así, la *National Association of Corporate Directors* (NACD, en adelante) de los EE.UU. ha elaborado una guía a efectos de garantizar que esta participación e implicación activa por parte del Consejo de Administración en materia de ciberseguridad y protección de datos se lleva a cabo de una manera eficiente. En la misma afirman que dicho órgano directivo deberá centrarse en cinco núcleos fundamentales. [80] En primer lugar, se establece la necesidad de que los miembros del consejo entiendan y enfoquen la ciberseguridad como parte de la gestión

[78] OECD. *Principles of Corporate Governance*. [En línea] [Fecha de consulta: 07/06/19] [Disponible en: *https://www.oecd.org/daf/ca/Corporate-Governance-Principles-ENG.pdf*].
[79] RSA CONFERENCE. *Survey: 82% of boards are concerned about cybersecurity* [En línea] [Fecha de consulta: 07/06/19] [Disponible en: *https://www.rsaconference.com/press/53/survey-82-of-boards-are-concerned-about*]: En 2016, durante una conferencia de ISACA (*International Systemns Audit and Control Association*) / RSA, se realizó una encuesta global a 461 responsables de ciberseguridad. En la misma se mostraba como el número de ciberataques y brechas de datos a las empresas estaba sufriendo un crecimiento exponencial en la cantidad y sofisticación de los mismos. Del mismo modo, se reveló que el 82 por ciento de los responsables de ciberseguridad afirmaba en los órganos de administración estaban preocupados o muy preocupados sobre la ciberseguridad.
[80] LEECH T., HANLON L. "Board Cyber Risk Oversight: What needs to change?" En: ANTONUCCI, D. *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. 2017.

de riesgos empresariales (ERM) y no como un riesgo especifico de las tecnologías de información. Es decir, los administradores deben entender las implicaciones legales de los ciber-riesgos pues se relacionan con las circunstancias específicas de su organización. Del mismo modo, los órganos de administración deberán tener un acceso adecuado a expertos en ciberseguridad y protección de datos, así como a conversaciones regulares sobre la gestión de los ciber-riesgos incluso dentro del orden del día de las reuniones con la Junta Directiva. [81]

3.2. El Compliance Officer

Venimos destacando la importancia que tiene la implicación activa del Consejo de Administración en los temas relacionados con el cumplimiento normativo en materia de protección de datos y ciberseguridad, participación que se proyecta también hacia otras materias, provocando que dichos administradores tengan que reunir un perfil cada vez más multidisciplinar para poder cumplir con sus deberes fiduciarios [82], y que surjan figuras específicas como es el caso del *Compliance Officer*.

Esta figura nació con una naturaleza puramente penal, cuya principal función era asegurar que las sociedades no incurrían en actuaciones que pudieran generar responsabilidad penal para los socios, administradores o incluso para la persona jurídica en sí misma, especialmente en materias fiscales, de blanqueamiento de capitales y de corrupción.[83] No obstante, en la actualidad esta figura ha ido evolucionando hacia un modelo con un enfoque más amplio en el que no solo actúa dentro de ese ámbito penalista, sino que además asegura el cumplimiento normativo de la empresa en una amplia variedad de áreas. En relación con esto, la *Asociación Española de Compliance* publicó un Libro Blanco donde se incluyen una serie de previsiones relativas a las funciones y configuración de esta figura dentro de las empresas. En el mismo se destaca como la función principal del *compliance* consiste en asumir tareas de prevención, detección y gestión de riesgos a través de la realización de programas de *compliance*, impulsando de

[81] NACD. *Director's Handbook on Cyber-Risk Oversight.* 2017. [En línea] [Fecha de consulta: 07/06/19] [Disponible en: *https://www.nacdonline.org/insights/publications.cfm?itemnumber=10687*].
[82] Podemos encontrar los deberes y responsabilidades propios de los administradores sociales entre los artículos de la Ley de Sociedades de Capital, siendo estos el deber de diligencia, lealtad, administración y gestión, control y supervisión; entre otras previsiones y responsabilidades específicas.
[83] DE ROS RAVENTÓS, I. "El órgano de prevención penal o "Compliance Officer". En: *Delito Fiscal y Tax Compliance*. 2018. BIB 2018/13552

este modo la cultura del cumplimiento normativo.[84] Es decir, vemos como en el mismo no se especifica la naturaleza penal de los posibles riesgos ni de sus planes de actuación, sino que vela por el cumplimiento normativo en general.

Asimismo, el Comité de Supervisión Bancaria de Basilea nos aclara esta cuestión - específicamente en relación con las entidades financieras pero extrapolable a cualquier tipo de sociedad mercantil - en una de sus publicaciones. En primer lugar, la citada organización mundial se refiere a los riesgos del *compliance* como aquellos que puedan implicar no solo sanciones legales, sino además aquellos que puedan suponer pedidas económicas y reputacionales derivadas del incumplimiento de leyes, normas, mecanismos de estandarización y códigos de conducta aplicables.[85] Como vemos, hace referencia directa a aquellas obligaciones asumidas de manera voluntaria por las entidades mediante sistemas de autorregulación o *soft law*, encontrando una relación directa con el buen gobierno corporativo.

Además de esto, se establecen una serie de previsiones que vinculan el *compliance* con las más altas esferas de la organización, destacando que el *compliance* deber ser parte de la cultura corporativa de la organización y que tiene que verse como una parte integral de las actividades de negocio. De nuevo, apreciamos una relación clara del *compliance* con la gobernanza empresarial, pues además destaca entre sus principios que el Consejo de Administración debe ser responsable de supervisar y controlar la gestión de los potenciales riesgos de *compliance* y la implementación de sus políticas. [86]

En virtud de todo lo expuesto, podemos determinar que el *Compliance Officer* es una figura importante para las sociedades, no solo en atención a sus funciones en aras del cumplimiento normativo, sino que también juega un papel fundamental a la hora de garantizar el correcto desarrollo del buen gobierno corporativo. [87] Es por ello que esta

[84] ASCOM (ASOCIACIÓN ESPAÑOLA DE COMPLIANCE). Libro blanco sobre la función de Compliance. 2017.
[85] BASEL COMMITTEE ON BANKING SUPERVISION. *Compliance and the compliance function in banks*. 2005. [En línea] [Fecha de consulta: 10/06/19] [Disponible en: *https://www.bis.org/publ/bcbs113.pdf*].
[86] *Ibid.*
[87] PÉREZ PALACI, J.E. "¿Debe ser interna o externa o externa la figura del *compliance officer*?" En: *Actualidad Jurídica Aranzadi*. Núm. 938/2018. 2018. BIB. 2018/7008: Es habitual en la práctica empresarial que surjan ciertas dudas sobre si es más conveniente que la figura del *compliance officer* sea interna o externa. No existen previsiones legales expresas sobre esta cuestión, no obstante, se considera que durante las primeras fases de implantación y hasta que la sociedad haya adquirido una cultura de *compliance* solida esta figura este externalizada a efectos de garantizar una mayor independencia y autonomía.

figura debe trabajar con una vinculación muy estrecha y periódica con el Consejo de Administración. No obstante, es importante garantizar la independencia de este agente en el desempeño de sus funciones de control y supervisión con el principal objetivo de evitar la sucesión de potenciales conflictos de intereses, así como la falta de imparcialidad que puede afectar a la correcta realización de las labores de detección y control de riesgos e incumplimientos. [88]

Ahora bien, podemos afirmar que el *Compliance Officer* es una figura con una naturaleza flexible que ha sabido adaptarse a las demandas de las sociedades mercantiles en las que desempeña sus funciones, evolucionando de un origen esencialmente penal hacia una naturaleza multidisciplinar y custodiando el cumplimiento normativo en su sentido más extenso. Sin embargo, ¿es esta una figura idónea a efectos de garantizar el cumplimiento normativo en materia de protección de datos a luz de la reciente normativa? Desde mi punto de vista no, por una simple cuestión, el Delegado de Protección de Datos; la nueva figura introducida por el RGPD a la cual se encomiendan en una serie de funciones que respaldan la protección de datos dentro de las organizaciones. Si acudimos al artículo 39 del citado reglamento encontramos que las funciones que tiene encomendadas este agente son las propias de un *Compliance Officer,* pero para el caso concreto de la protección de datos.

3.3. El Delegado de Protección de Datos (DPO)

El Delegado de Protección de Datos (DPD o DPO por sus siglas en inglés) es la nueva figura clave en aquellas cuestiones relativas a la protección de datos que puedan darse dentro de las diferentes entidades. Tiene encomendada la tarea de llevar a cabo las labores de información, asesoramiento y supervisión del responsable o encargado en relación con el tratamiento de datos personales. A su vez, es el nexo de unión entre estos dos sujetos y la autoridad de control, llevando a cabo las labores de notificación y cooperación con la misma. [89] La existencia de este sujeto dentro de las empresas no es siempre obligatoria,

[88] MORENO DE LA SANTA GARCÍA, E. "La función de apoyo del *compliance officer* a los administradores de sociedades de capital: Distribución de deberes y capital." En: *Revista de Derecho Bancario y Bursátil*. Núm. 151/2018. 2018. BIB 2018/10829.

[89] Art. 39. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE . *Diario Oficial de la Unión Europea*, 27 de abril de 2016, L 119/2.

pues solo se exige cuando se den ciertas características particulares por parte de la empresa, las cuales se recogen en la normativa europea y nacional de aplicación. [90]

A pesar de que la designación de este profesional solo es imperativa en una serie de supuestos, la normativa europea no descarta la posibilidad de nombrar un DPO de carácter voluntario en el seno de cualquier empresa. Para las sociedades mercantiles, el hecho de contar con una figura de este tipo dentro de su organización supone una garantía del cumplimiento de la normativa en materia de protección de datos, actuando por lo tanto como un mecanismo muy eficaz a la hora de salvaguardar el principio de responsabilidad proactiva o *accountability*. A su vez, el Delegado de Protección de Datos se presenta de alguna manera como una especie de doble garante del buen gobierno y del cumplimiento normativo en materia de protección de datos, pues la AEPD, con la ayuda de un Comité Técnico de Expertos, ha establecido la creación de un esquema de certificación de esta figura.[91] Este esquema de certificación busca aportar seguridad y fiabilidad tanto a los propios profesionales como a las empresas que vayan a incluir un DPO dentro de su organización. [92]

El citado esquema de certificación se basa en lo dispuesto en la normativa europea y nacional en materia de protección de datos, así como en normas internacionales de estandarización y certificación. Asimismo, se establece que aquellas entidades que pretendan conceder este tipo de certificaciones deberán estar acreditadas previamente por la Entidad Nacional de Acreditación (ENAC).[93] Por otro lado, el DPO deberá realizar las funciones propias de su cargo de la manera más exclusiva posible, siendo aceptable el desempeño de otras funciones, siempre y cuando no den lugar a un conflicto de intereses. Al mismo tiempo, el RGPD afirma que este cargo deberá ostentarlo un profesional con la

[90] En el caso del sector privado, la normativa europea recoge su obligatoriedad para aquellas empresas que realizan operaciones de tratamiento mediante una observación habitual y sistemática de personas a gran escala, o de tratamientos de datos de categorías especiales, también a gran escala. Por su parte, la ley española, además de referirse a los supuestos anteriores, establece en su art. 34 una lista con 16 supuestos en los que será necesario asignar un DPO.

[91] Es importante destacar que la certificación de DPO no constituye un mandato imperativo por la ley, sino que se trata de un método para garantizar que esta figura se ajusta a ciertos criterios de idoneidad y profesionalidad. No obstante, aunque no sea necesaria esta certificación para designar a alguien DPO, en la práctica se muestra una tendencia favorable hacia la acreditación, pues no solo constituye un mayor atractivo para la entidad que vaya a contar con ese DPO, sino también para el propio profesional, pues esta certificación va a suponer una ventaja competitiva para él en el ámbito profesional.

[92] LOZANO GODOY, S. *Delegado de Protección de Datos, el profesional más buscado*. En: AENOR: Revista de la normalización y la certificación. Nº 338, 2018. Págs. 20-23:

[93] AEPD. *Esquema de certificación de delegados de protección de datos de la agencia española de protección de datos (Esquema AEPD-DPD).* 2018. [En línea] [Fecha de consulta: 11/06/19] [Disponible en: *https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf*].

capacidad y cualidad necesarias que, además, deberá poseer conocimientos especializados de la legislación sobre protección de datos.[94]

El RGPD destaca en su artículo 37.6 que el DPO podrá ser tanto una figura interna de la propia empresa como desempeñar sus funciones en el marco de un contrato de servicios. Sin embargo, y al igual que se dijo en relación con el *Compliance Officer*, la inclusión de esta figura dentro de la plantilla de la organización supone una mayor garantía, especialmente en beneficio del buen gobierno corporativo, aunque la implantación y primeros pasos se lleven de una manera externalizada a efectos de guardar el carácter independiente de dicha figura. Es decir, es más idóneo que, aunque los primeros pasos de la adecuación a esta nueva normativa se lleven a cabo mediante un servicio de DPO externalizado, posteriormente se pase a incluir esta figura en la estructura interna de la sociedad. Esto es así a consecuencia de que existe la necesidad de que el DPO desarrolle su actividad con la mayor relación posible con el órgano de administración de la sociedad (art. 38.3 RGPD), todo ello sin perjuicio de salvaguardar su naturaleza autónoma e independiente.[95] Por lo que, podemos incluso destacar que, a efectos del buen gobierno corporativo, esta figura debería incluirse en un puesto de alto rango dentro de la organización societaria.

Este tipo de previsiones constituyen una prueba más de lo que hemos ido exponiendo a lo largo del presente trabajo, y es que toda la regulación en materia de protección de datos guarda una estrecha vinculación con las diferentes manifestaciones del *soft law*. Es evidente como esta normativa incentiva y promueve la utilización de esta autorregulación, certificación y estandarización, pues lo ve como una herramienta útil para ayudar a los sujetos y entidades obligadas a cumplir con la norma. Del mismo modo, estos instrumentos de "*derecho blando*" se constituyen como una manifestación importante del buen gobierno corporativo, pues son materiales idóneos para garantizar una actuación responsable por parte de la empresa, así como, para vincular e incentivar la participación

[94] SIERRA BENITEZ, E. "El delegado de protección de daos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico". En: *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*. Vol. 6, Núm. 1, 2018. Págs. 237-253

[95] Además de esta individualidad y autonomía del DPO en el desarrollo de sus funciones, encontramos que la ley le otorga una exención de responsabilidad personal ante el suceso de potenciales sanciones e infracciones. Es decir, en el supuesto de que acontezca algún tipo de evento que vulnere la normativa en materia de protección de datos, los únicos responsables de la misma serán el responsable y el encargado del tratamiento.

de los altos mandos y del consejo de administración de la sociedad en los asuntos sobre la protección de datos.

3.4. Previsión sobre una potencial Comisión Interna del Consejo en materia de protección de datos y ciberseguridad

En línea con las pioneras previsiones sobre la gobernanza de la ciberseguridad y la protección de datos en las sociedades mercantiles, podemos plantearnos si es idóneo crear una comisión interna en materia de ciberseguridad, privacidad y protección de datos dentro del Consejo. Sus funciones abarcarían no solo las relativas a la información e implicación del órgano de administración, sino que también se delegaría sobre la misma una serie de actuaciones relativas a la gestión e implementación de estas materias dentro de la empresa como la formulación de estrategias al respecto, la supervisión de la contratación de personal y equipos relativos a su competencia, etc. Al igual que sucede con otras comisiones delegadas del consejo, esta deberá reportar al órgano de administración sobre todas sus actividades.[96]

Como se destacó en puntos anteriores del presente trabajo, el consejo de administración puede delegar una serie de funciones, ya sea de carácter temporal o permanente, a consejeros delegados o a comisiones ejecutivas. Pues bien, aunque en la actualidad no existe en la ley ningún tipo de referencia o previsión legal a esta comisión y, a pesar de que los distintos textos de *soft law* que hacen mención a ello no son abundantes, entiendo que mediante la creación de una comisión interna de esta categoría se conseguiría establecer un control al más alto nivel sobre la protección de datos y la ciberseguridad, actuando en coherencia con el sistema de reparto de competencias en la sociedad acorde con los objetivos de seguridad que subyacen tanto al RGPD como a la LOPDGDD.

Para la configuración de esta comisión, encuentro posible dos alternativas. Por un lado, podría estar constituida por aquellos agentes que tengan roles relacionados con la ciberseguridad, las IT y la protección de datos, como pueden ser el CISO (*Chief Information Security Officer*), CSO (*Chief Security Officer*), CIO (*Chief Information Officer*), CTO (*Chief Technology Officer*), *Compliance Officer* y DPO (*Data Protection*

[96] Art. 249 *Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital.*

Officer)[97], junto con la participación de alguno de los miembros del consejo de administración o incluso del CEO (*Chief Executive Officer*). Implícitamente, ello implicaría que las figuras mencionadas anteriormente serían miembros del consejo, dado que los miembros de las comisiones delegadas, al menos en derecho español, deben ser todos ellos consejeros. Pero, por otro lado, y posiblemente en una dirección más factible, cabría exigir competencias en materia de ciberseguridad y datos a los consejeros que formasen parte de esta comisión, dejando a los agentes encargados de la seguridad de la información y de los datos personales en el ámbito de las relaciones laborales de alta dirección, eso sí, con una vinculación directa con la comisión delegada del consejo.

Volviendo con las disposiciones establecidas por la NACD, encontramos entre las mismas la exigencia de que los administradores deberán establecer previsiones relativas al establecimiento de un marco de gestión en materia de riesgos cibernéticos para toda la organización, haciendo que la dirección que la empresa sea conforme a esto y se disponga de un personal y presupuesto adecuado que asegure el correcto funcionamiento del mismo.[98] Además, las conversaciones regulares en materia de ciberseguridad y protección de datos deben incluir a su vez la identificación de los riesgos que deben evitarse, aceptarse, mitigarse o transferirse a través de la contratación de ciberseguros [99], así como de los planes concretos que puedan existir en cada materia especifica.

[97] INCIBE. *CEO, CISO, CIO... ¿Roles en ciberseguridad?* [En línea] [Fecha de consulta: 07/06/19] [Disponible en: *https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad*].
[98] NACD. *Director's Handbook on Cyber-Risk Oversight.* 2017. [En línea] [Fecha de consulta: 07/06/19] [Disponible en: *https://www.nacdonline.org/insights/publications.cfm?itemnumber=10687*].
[99] EIOPA. *Keynote speech by Gabriel Bernardino, Chairman, European Insurance and Occupational Pensions Authority (EIOPA) at the 3rd Annual FinTech and Regulation Conference on "Taking innovation to the next level" on 26 February 2019 in Brussels*. [En línea] [Fecha de consulta: 07/06/19] [Disponible en: *https://eiopa.europa.eu/Publications/Speeches%20and%20presentations/2019-02-26%20ThirdAnnual FinTechRegulationConferenceAforeConsultingSpeechGabrielBernardino.pdf*]: En relación con este tema, es importante destacar como Gabriel Bernardino, el presidente de la autoridad europea en materia de seguros, afirmó recientemente que desde la EIOPA están estudiando la posibilidad de establecer la obligatoriedad para las empresas de contratar este tipo de *ciber-pólizas*, especialmente desde la aprobación del RGPD en la Unión Europea.

4. APORTACIONES, RECAPITULACIONES Y CONCLUSIONES

Tras la exposición sistemática del contenido y de los elementos principales relativos a la protección de datos personales y su vinculación con el buen gobierno corporativo, a modo de conclusión, y donde desarrollo del mismo modo mi opinión sobre la materia, encuentro que:

PRIMERA: El conjunto de datos que es transferido y procesado a través de los sistemas de la información y comunicación se está viendo sometido a un incremento sistemático día a día. La cantidad de información que es manipulada a diario y la complejidad de su tratamiento hace que los sistemas que operan los datos tengan cada vez una dimensión más amplia y compleja. Por tanto, el derecho positivo en estas materias está conociendo una creciente complejidad, como lo es en su aplicación y desarrollo. Sobre esta base, las iniciativas para generar un cuerpo coherente de recomendaciones en materia de seguridad de datos (*soft law)* resultan importantes y son acogidas favorablemente por las empresas, especialmente las grandes, que las asumen dentro del margen de autorregulación del que gozan. Las recomendaciones asumidas o seguidas por las empresas facilitan el cumplimiento normativo por lo que sus efectos son preventivos, supervisores e incluso correctores: al contener pautas de comportamiento orientativo contribuyen al buen gobierno cibernético, a evitar el acontecimiento de daños e incluso la imposición de sanciones derivadas de una mala comprensión de la ley. Con sus beneficios, las recomendaciones y estándares han trasformado los modelos tradicionales de gobernanza en distintos ámbitos -ambiental, contable, laboral, entre otros -y creemos que tienen un papel muy importante que cumplir en materia de protección de datos personales y ciberseguridad.

SEGUNDA: La implantación y adaptación de la actividad empresarial a mecanismos de autorregulación y certificación implica, no solo una garantía en base al cumplimiento normativo, sino también un tipo de actuación en aras del buen gobierno, de la Responsabilidad Social Corporativa (RSC) y un perfeccionamiento de la imagen empresarial y reputacional de la sociedad mercantil. Por lo que, si la actuación o gestión empresarial se desarrolla con la ayuda de estos instrumentos, no solo se estará consiguiendo el objetivo principal que se persigue con los mismos, ya que además se

generarán una serie de ventajas complementarias que son beneficiosas para la actividad de negocio de la sociedad.

TERCERA: A pesar de que la amplitud y detalle de esta regulación -derecho positivo- aporta complejidad a su aplicación, las principales novedades introducidas por el RGPD se han incluido por el legislador con el principal objetivo de eliminar o reducir ciertas dificultades y limitaciones que existían previamente para los responsables y encargados de las empresas, todo ello sin dejar de lado las medidas de seguridad necesarias que aseguren que la protección de datos personales de las personas físicas que sean objeto de tratamiento están correctamente asegurados. Las modificaciones y previsiones que han sido incorporadas en el conjunto de la normativa de protección de datos dejan entrever como una de las principales motivaciones del legislador a la hora de implantar esta ley era la promoción y fomento de mecanismos de certificación, códigos de conducta y, de carácter general, instrumentos de autorregulación o *soft law*. Es decir, desde Europa se apuesta por esta tipología de mecanismos como medios idóneos que garantizan una correcta gestión del tratamiento de los datos personales y, por lo tanto, ayudan a cumplir con las previsiones legales en esta materia.

CUARTA: A la hora de llevar a cabo la implantación formal de la protección de datos dentro de la empresa, una de las previsiones más importantes que debe considerarse es que los miembros del consejo de administración y altos directivos deben tener conocimiento y vinculación directa sobre todos los procesos la misma. De esta forma, se asegura su implicación en relación con los deberes fiduciarios que les son propios, además de servir como soporte a la hora de probar a los interesados y autoridades que han actuado con la diligencia y lealtad debida en caso de un potencial evento que perjudique la confidencialidad, integridad y disponibilidad de los datos que trata la sociedad. Por lo que, a pesar de que no constituya una obligación legal que el consejo de administración tenga una implicación activa en estos temas, es la única forma de que la sociedad actúe siguiendo los dogmas y principios del buen gobierno corporativo al mismo tiempo que puede garantizar su cumplimiento normativo en la materia, cumpliendo con el principio de responsabilidad proactiva o *accountability*.

QUINTA: El acercamiento de posiciones entre las exigencias legales en materia de protección de datos y ciberseguridad con la figura del buen gobierno corporativo da lugar a un conjunto de medidas que no solo posibilitan el cumplimiento normativo por

parte de la empresa con altos niveles de éxito, sino que además se garantiza la intervención del órgano de administración y de los altos directivos de la empresa en la toma de decisiones directas y en el control de las políticas de protección de datos personales.

SEXTA: Para llevar a cabo una correcta gestión del buen gobierno de los datos dentro de la empresa, o dicho de otro modo, para implementar de manera óptima un modelo de *Data Governance*, es necesario que existan y se desarrollen un conjunto de políticas internas relativas a la gestión y medios de protección de los datos; que se determinen los roles y las responsabilidades de cada uno de los agentes que van a dirigir y controlar dicha gestión y, por último, que se implementes una serie de procesos básicos que aseguren la claridad, consistencia y coordinación entre las medidas de seguridad previstas y los agentes implicados.

SÉPTIMA: Dentro de las medidas organizativas y materiales que pueden tomarse en el seno de una sociedad mercantil a efectos de garantizar la normativa de protección de datos y de la ciberseguridad, así como para cumplir con los principios del buen gobierno corporativo, consiste en la creación de una comisión interna en la materia. Este órgano tendría una serie de funciones asignadas en lo relativo a la información y comunicación con el órgano de administración, además de asumir un conjunto de tareas referentes a la gestión e implementación de medidas de seguridad y control sobre datos personales y ciberseguridad de los activos de la información. Como potenciales miembros de la misma entiendo que existen dos alternativas, por un lado, se podría incluir a aquellos sujetos y agentes que reúnan funciones y perfiles relacionados con la ciberseguridad y la protección de datos dentro de dicha comisión. No obstante, esto supondría que los mismos deberían estar a su vez dentro del propio Consejo de Administración, haciendo que esta opción resulte más compleja. Pero, por otro lado, se podrían exigir competencias y conocimientos en materia de protección de datos y ciberseguridad a los propios consejeros que fuesen miembros de dicha comisión, dejando que los agentes mencionados continúen realizando sus funciones propias, eso sí, siempre en el ámbito de la alta dirección y con una vinculación directa con la comisión delegada. Esto permitirá una mayor coordinación y acercamiento con el Consejo, asegurando una significativa implicación del mismo en estos asuntos y consiguiendo la implantación integral de estas dos materias en todos los niveles o estratos empresariales.

OCTAVA: La figura del *Compliance Officer*, que nació con el principal objetivo de gestionar la actuación empresarial para que la misma no incurriese en actuaciones que pudieran constituir un ilícito penal, se ha ido desarrollando y transformando con el tiempo para convertirse en un agente con un carácter multidisciplinar que vela por salvaguardar el cumplimiento normativo en su sentido más amplio dentro de la empresa. No obstante, y en base a la reciente normativa en materia de protección de datos, podemos afirmar que esta figura carece de protagonismo y competencia en dicha materia. Con la previsión de la nueva figura del Delegado de Protección de Datos, así como una serie de nuevas exigencias que deben cumplir los responsables y encargados del tratamiento de los datos, el *Compliance Officer* no encuentra cabida a la hora de gestionar las actuaciones empresariales en lo relativo a la protección de datos, a pesar de que un incumplimiento de la normativa acarrearía una serie de importantes sanciones para la mercantil. Esto es así a consecuencia de que todas aquellas funciones y tareas asignadas al *Compliance Officer* en lo relativo a los planes de prevención de delitos y demás medidas aseguradoras del cumplimiento normativo, vienen encomendadas al DPO, al responsable y al encargado en el nuevo RGPD para todas aquellas cuestiones en relación con la protección de datos personales.

NOVENA: La ley deja clara la posibilidad de que tanto la figura del *Compliance Officer* como la del Delegado de Protección de Datos puedan ser internas a la propia empresa o, por el contrario, profesionales externos que actúan mediante un contrato de servicios. Sin embargo, y considerando una postura que se ajuste a las previsiones del buen gobierno corporativo, la inserción de ambos agentes en el seno de la organización empresarial supone una mayor garantía para la sociedad mercantil, todo ello sin perjuicio de que en un primer momento de implantación ambas figuras se encuentren realizando sus funciones de manera externa a la empresa, previsión que también se recomienda a efectos de garantizar la autonomía e independencia de estos sujetos en la ejecución de sus tareas. Es decir, se pueden dar mejores resultados y una gestión más eficiente de las labores que realizan ambos sujetos cuando en el momento de iniciar su actividad se encuentren efectuando sus funciones de manera externalizada mediante un contrato de servicios, pasando posteriormente a formar parte del organigrama empresarial. Esta previsión se justifica a consecuencia de que es necesario que tanto *Compliance Officer* como DPO actúen con la mayor proximidad posible a órgano de administración y a los altos directivos, asegurando así la una mayor implicación de la empresa para con el buen

gobierno corporativo y con el cumplimiento normativo, a la vez que salvaguardan la independencia y autonomía exigida en sus actuaciones.

DÉCIMA: Tras la exposición sistemática del contenido de este trabajo hemos visto como en esta materia juega un papel muy importante el *soft law*, el cual avanza por delante de la normativa y legislación en la materia, pues su naturaleza le permite adecuarse más rápidamente a la realidad y al avance tecnológico que caracterizan a un ámbito tan cambiante como es el de la protección de datos y la ciberseguridad. Esto nos lleva a pensar si cabe la posibilidad de que en algún momento de la evolución normativa de esta materia nos encontremos con que el legislador encuentra en estas disposiciones de derecho blando un modelo o figura sobre la que basarse a la hora de redactar las posteriores normas o disposiciones con fuerza de ley y, consecuentemente, acabe adoptado aquello que en un primer momento vino recogido en los instrumentos del *soft law.*

UNDÉCIMA: Como colofón de este trabajo, concluimos que el cumplimiento del principio de *accountability* en las sociedades mercantiles -especialmente en relación con los datos personales y el entorno digital- puede ser potenciado mediante la implantación progresiva de instrumentos de *soft law* propios del buen gobierno corporativo. Estos mecanismos de autorregulación deberán seguir una orientación material dirigida hacia la tutela y protección de los datos de carácter personal en el marco del derecho positivo, facilitando su cumplimento, e incluso abriendo vías para nuevos desarrollos de normas y políticas de seguridad de la información de las propias empresas y posiblemente, del legislador.

5. BIBLIOGRAFÍA

AEPD (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS). *Esquema de certificación de delegados de protección de datos de la agencia española de protección de datos (Esquema AEPD-DPD).* 2018. [En línea] [Fecha de consulta: 11/06/19] [Disponible en: *https://www.aepd.es/reglamento/cumplimiento /common/esquema-aepd-dpd.pdf*].

ALBERTO GONZALEX, P. "Responsabilidad proactiva en los tratamientos masivos de datos". En: *Dilemata, Revista Internacional de Éticas Aplicadas*. 2017, Nº24.

ASCOM (ASOCIACIÓN ESPAÑOLA DE COMPLIANCE). *Libro blanco sobre la función de Compliance.* 2017.

BASEL COMMITTEE ON BANKING SUPERVISION. *Compliance and the compliance function in banks*. 2005. [En línea] [Fecha de consulta: 10/06/19] [Disponible en: *https://www.bis.org/publ/ bcbs113.pdf*].

CAZORLA GONZÁLEZ-SERRANO, L. "El deber de diligencia del administrador social y los programas de cumplimiento o "compliance" penal". En: *Lex Mercatoria* Nº 1, 2015.

CLARKE T. *International Corporate Governance: A Comparative Approach*. 2nd Ed. Routlede, 2011.

CNIL (COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS). *Privacy seals on privacy governance procedures,* 2014.

CNMV (COMISIÓN NACIONAL DEL MERCADO DE VALORES). *Código de buen gobierno de las sociedades cotizadas*. [en línea]. Madrid, 2015. [Fecha de consulta: 24/04/19]. [Disponible en: *https://www.cnmv.es/docportal/ publicaciones/codigogov/codigo_buen_gobierno .pdf*].

CNMV (COMISIÓN NACIONAL DEL MERCADO DE VALORES). *Informe de la Comisión Especial para el Fomento de la Transparencia y la Seguridad de los*

Mercados Financieros y Sociedades Cotizadas. [en línea]. Madrid, 2003. [Fecha de consulta: 24/04/19] [Disponible en: *https://www.cnmv.es/DocPortal/ Publicaciones/CodigoGov/INFORMEFINAL.PDF*].

COMISIÓN EUROPEA. *Comunicación de la Comisión al Parlamento Europeo y al Consejo relativa al Intercambio y protección de los datos personales en un mundo globalizado*. 2017. [En línea] [Fecha de consulta: 06/06/19]. [Disponible en:*https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017DC0007&from=EN*].

DATOO A. *Legal Data for Banking: Business Optimisation and Regulatory Compliance*. 1 st Ed, 2019.

DAVARA RODRÍGUEZ, M.A. *Manual de Derecho Informático*. 10ª Ed. Pamplona, 2008.

DE ROS RAVENTÓS, I. "El órgano de prevención penal o "Compliance Officer". En: *Delito Fiscal y Tax Compliance*. 2018. BIB 2018/13552.

EDPS (EUROPEAN DATA PROTECTION SUPERVISOR). *Annual Report 2018*. Luxemburgo, 2019.

EIOPA (EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY). *Keynote speech by Gabriel Bernardino, Chairman, European Insurance and Occupational Pensions Authority (EIOPA) at the 3rd Annual FinTech and Regulation Conference on "Taking innovation to the next level" on 26 February 2019 in Brussels.*

EUROPEAN COMISSION. (Article 29 Data Protection Working Party). *Opinion 3/2010 on the principle of accountability* [En línea]. Bruselas, 2010. [Fecha de consulta: 02/04/19] [Disponible en: *https://ec.europa.eu/justice/article-29/documentation /opinion-recommendation/files/2010/wp173_en.pdf*].

EUROPEAN COMISSION. *The GDPR: New opportunities, new obligations*. [En línea] [Fecha de consulta: 26/03/19] [Disponible en: *https://ec.europa.eu/ commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_ en .pdf*].

EUROPEAN PARLIAMENT. *A Governance Framework for Algorithmic Accountability and Transparency*. 2019. [En línea] [Fecha de consulta: 07/06/19]. [Disponible en: *http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf*].

FOULSHAM M., HITCHEN B. y DENLEY A. *GDPR: How To Achieve and Maintain Compliance*. Nueva York, 2019.

GARCÍA COTO, D.J. y BLANCO DIEGO, R. "Códigos de buen gobierno en Europa y Estado Unidos. Especial referencia a los códigos de Olivencia y Aldama en España". En: *Análisis financiero. Número extraordinario sobre "Corporate Governance".* Nº 90. 2010.

GILBERT, F. "Privacy and Security Legal Issues". En: GENG, H. *Internet of Things and Data Analytics Handbook*. 1st Ed. 2017.

GIMENO BEVIÁ, V. "Los programas de «*compliance*» como manifestación del deber de diligencia de los administradores*"*. En*: Revista de Derecho de Sociedades*. 2019. Núm.55/2019.

GOBEO A., FOWLER C. y BUCHANAN W.J. *GDPR and Cyber Security for Business Information Systems*. Gistrup, 2018.

GORDON, K. *Principles of Data Management: Facilitating Information Sharing.* London, 2014.

HEIDIRCK & STRUGGLES. *Towards Dynamic Governance 2014: European Corporate Governance Report*. 2014.

HERAS CARRASCO, R. "Evaluaciones de Impacto". En: *I+S*: *Revista de la Sociedad Española de Informática y Salud*. Núm. 127, 2018. Págs. 24-27. [En línea] [Fecha de consulta: 06/06/19] [Disponible en: *https://dialnet.unirioja.es/servlet/autor?codigo=4444603#ArticulosRevistas*].

HERNÁNDEZ GIL, A. *Problemas socio culturales de la Informática Jurídica, Ponencia en la Mesa redonda sobre Teleinformática Jurídica*. Fundación para el desarrollo social de las comunicaciones (FUNDESCO). Madrid, 1973.

INCIBE. *CEO, CISO, CIO... ¿Roles en ciberseguridad?* [En línea] [Fecha de consulta: 07/06/19] [Disponible en: *https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad*].

INCIBE. *Desarrollar cultura en seguridad*. [En línea] [Fecha de consulta: 07/06/19]. [Disponible en: *https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_desarrollar-cultura-en-seguridad.pdf*].

KAZEMI, R. *General Data Protection Regulation (GDPR)*. Hamburg, 2018.

LADLEY, J. *Data Governance: How to Design, Deply and Sustain an Effective Data Governance Program*. Boston, 2012

LEECH T., HANLON L. "Board Cyber Risk Oversight: What needs to change?" En: ANTONUCCI, D. *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. 2017.

MARTÍNEZ-MARTÍNEZ, D.F. *Unification of personal data protection in the European Union: Challenges and implications.* El profesional de la información, v. 29, n. 1, pp. 185-194. 2018, enero-febrero. [Fecha de consulta: 26/03/19] [Disponible en: *https://doi.org/10.3145/epi.2018.ene.17*]

MCDERMOTT WILL & EMERY LLP AND PONEMON INSTITUTE LLC. *The Race to GDPD: A Study of Companies in the United States & Europe*, 2018.

MORENO DE LA SANTA GARCÍA, E. "La función de apoyo del *compliance officer* a los administradores de sociedades de capital: Distribución de deberes y capital." En: *Revista de Derecho Bancario y Bursátil*. Núm. 151/2018. 2018. BIB 2018/10829.

NACD. *Director's Handbook on Cyber-Risk Oversight*. 2017. [En línea] [Fecha de consulta: 07/06/19] [Disponible en: *https://www.nacdonline.org/insights/publications.cfm?itemnumber=10687*].

OECD (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT)

- *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. [En línea] [Fecha de consulta: 22/05/19] [Disponible en: *https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#preface*].
- *Principles of Corporate Governance*. [En línea] [Fecha de consulta: 06/06/19] [Disponible en: *https://www.oecd.org/daf/ca/Corporate-Governance-Principles-ENG.pdf*].

OUWERKERK, E. "The Value Chain: Beware of GDPR – Take your Cyber Risk Responsability More Seriously". En: CHISHTI, S. *The InsurTech Book*. 2018. Págs. 175-178 [En línea] [Fecha de consulta: 06/06/19]. [Disponible en: *https://onlinelibrary.wiley.com/doi/10.1002/9781119444565.ch40#*]

PÉREZ CARRILLO, E.F. "Gobierno corporativo comparado". En: *Gobierno corporativo y responsabilidad social de las empresas*. Madrid, 2009.

PÉREZ PALACI, J.E. "¿Debe ser interna o externa o externa la figura del *compliance officer*?" En: *Actualidad Jurídica Aranzadi*. Núm. 938/2018. 2018. BIB. 2018/7008.

RAMOS F. *El principio de Accountability o de Responsabilidad Proactiva*. [en línea] [Disponible en *http://www.dpoitlaw.com/el-principio-de-accountability-o-de-responsabilidad-proactiva/]*

RISHIKOF, H. & SULLIVAN, C. "Legal and Compliance". En: ANTONUCCI, D. *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. 2017.

RSA CONFERENCE. *Survey: 82% of boards are concerned about cybersecurity* [En línea] [Fecha de consulta: 07/06/19] [Disponible en: *https://www.rsaconference.com/press/53/survey-82-of-boards-are-concerned-about*].

SIERRA BENITEZ, E. "El delegado de protección de daos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico". En: *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*. Vol. 6, Núm. 1, 2018.

SMALLWOOD, R. *Information Governance: Concepts, Strategies and Best Practices*. 2014.

THOMPSON REUTERS ARANZADI. *Sector Retail. Guía Corporate Compliance y Protección de Datos*. Pamplona, 2018.

VERNIMMEN P., QUIRY P., DALLOCCHIO M., LE FUR Y y SALVI A. *Corporate Finance: Theory and Practice, Fifth Edition.*

VOIGT P. y VON DEM BUSSCHE A. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham, 2017.

VV.AA. (META COMPLIANCE). *GDPR Best Practices Implementation Guide: Transforming GDPR Requirements into Compliant Operational Behaviours*.

WARSINKE, J. "Security and Risk Management". En: *CISSP: Certified Information Systems Security Professional.* 2019

YÁÑEZ, J. "Las nuevas certificaciones oficiales a la luz del RGPD". En: Actualidad Jurídica Aranzadi. Núm. 933/2017, 2017.

6. LEGISLACIÓN Y NORMAS

Constitución Española, *BOE*, 1978

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos, *DOUE*, 1995.

ISO/IEC 27000:2009 Sistemas de Gestión de Seguridad de la Información. Visión de conjunto y vocabulario.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, *BOE*, 1999.

Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales, *BOE*, 2018.

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, *BOE*, 1992.

Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital.

Real Decreto-ley 5/2018, de 27 de julio, de medias urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, *BOE*, 2018.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, *DOUE*, 2016.

7. SENTENCIAS Y JURISPRUDENCIA

Sentencia del Tribunal Constitucional 11/1998, de 13 de enero de 1998. (ECLI:ES:TC: 1998:11)

Sentencia del Tribunal Constitucional 143/1994, de 9 de mayo de 1994. (ECLI:ES:TC: 1994:143)

Sentencia del Tribunal Constitucional 254/1993, de 20 de julio de 1993. (ECLI:ES:TC: 1993:254)

Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2001. (ECLI:ES:TC: 2000:292)

Sentencia del Tribunal Constitucional 76/2019, de 22 mayo de 2019. (ECLI:ES:TC: 2019:76).

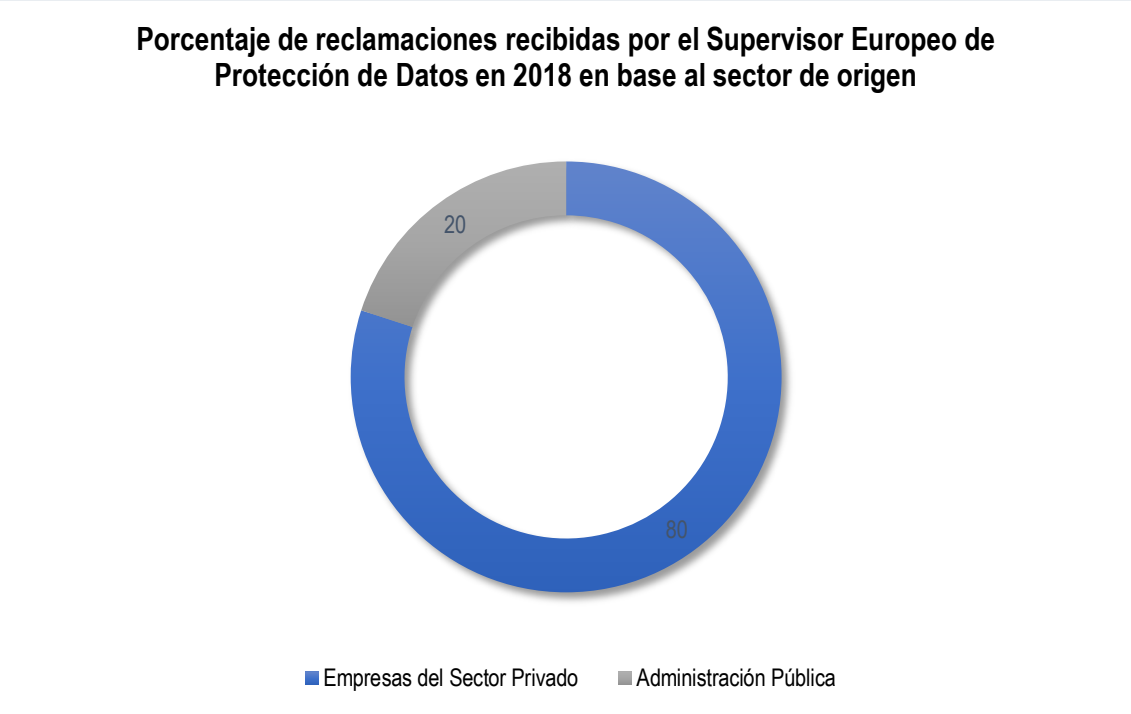
Sentencia del Tribunal de Justicia de la Unión Europea C-362/14, de 6 de octubre de 2015 (*Caso Schrems v. Autoridad Europea de Protección de Datos*). (ECLI:EU:C: 2015:650)

Sentencia del Tribunal Europeo de Derechos Humanos (Sección 4ª) 62357/14, de 24 de abril de 2018 (*Caso Benedik v. Slovenia*).

ANEXO I

GRÁFICOS DE ELABORACIÓN PROPIA Y DATOS COMPLEMENTARIOS SOBRE LA IMPLANTACIÓN DE POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES Y BUEN GOBIERNO DE LOS DATOS EN EMPRESAS EUROPEAS Y ESTADOUNIDENSES

Gráfico 1

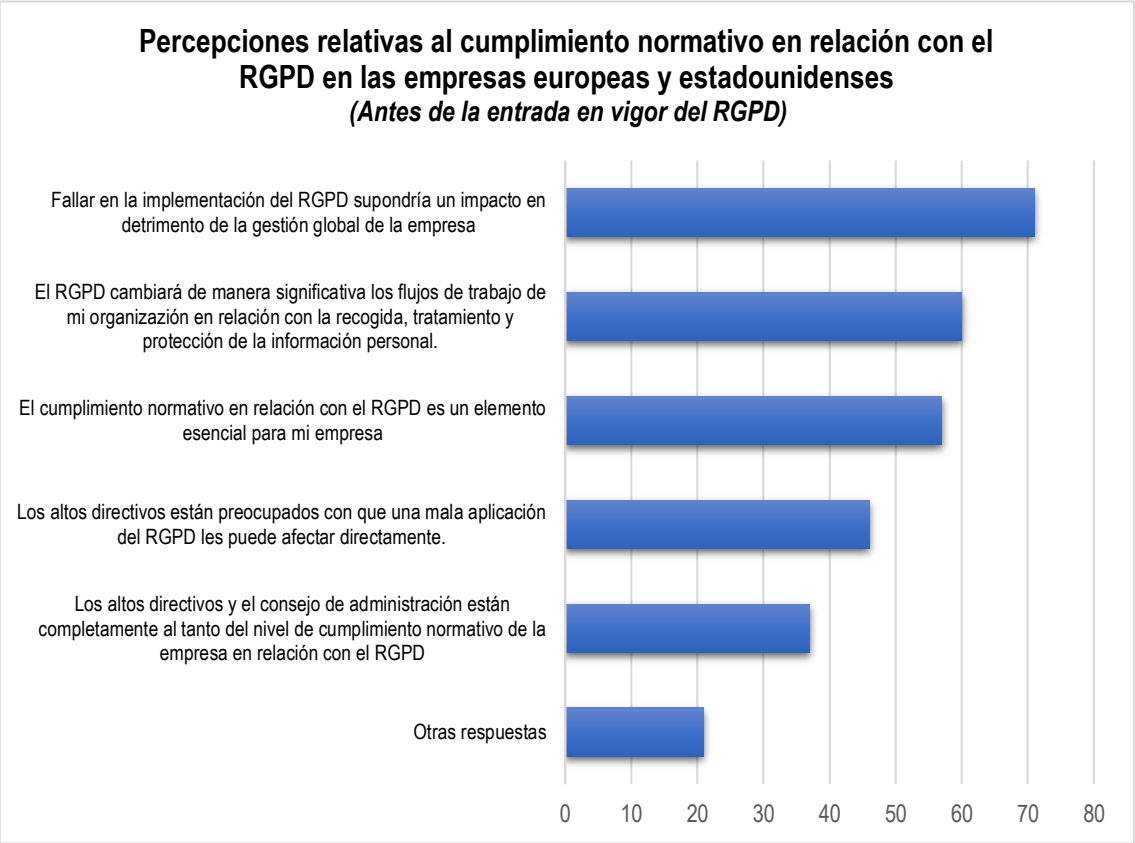


Fuente: *Annual Report 2018*. European Data Protection Supervisor.

Gráfico 2

Fuente: *Annual Report 2018*. European Data Protection Supervisor.

Gráfico 3

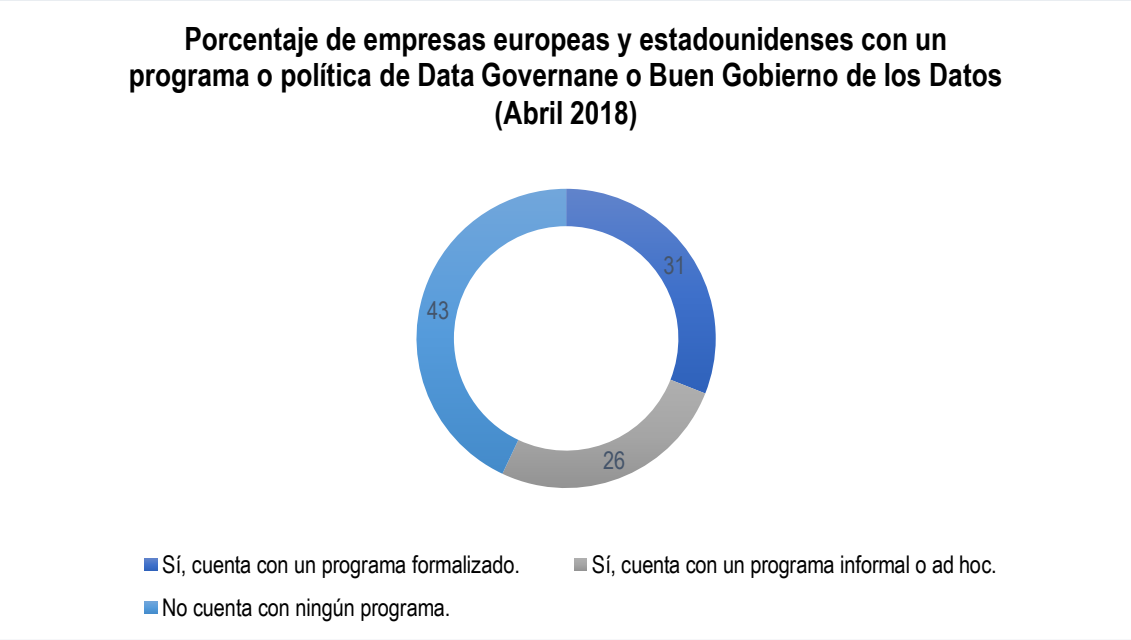


Fuente: *The Race to GDPR: A Study of Companies in the United States & Europe*. McDermott Will & Emery LLP and Ponemon Institute LLC. April 2018.

Gráfico 4

Fuente: *The Race to GDPR: A Study of Companies in the United States & Europe*. McDermott Will & Emery LLP and Ponemon Institute LLC. April 2018.

Gráfico 5.A.

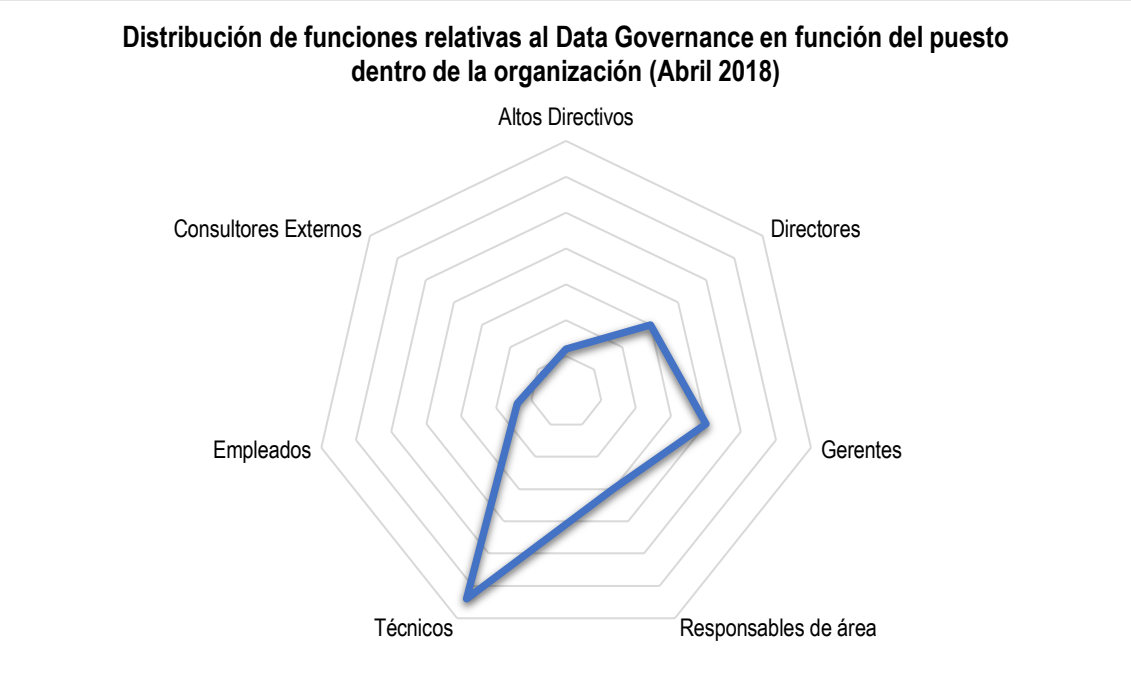


Fuente: *The Race to GDPR: A Study of Companies in the United States & Europe*. McDermott Will & Emery LLP and Ponemon Institute LLC. April 2018

Gráfico 5.B

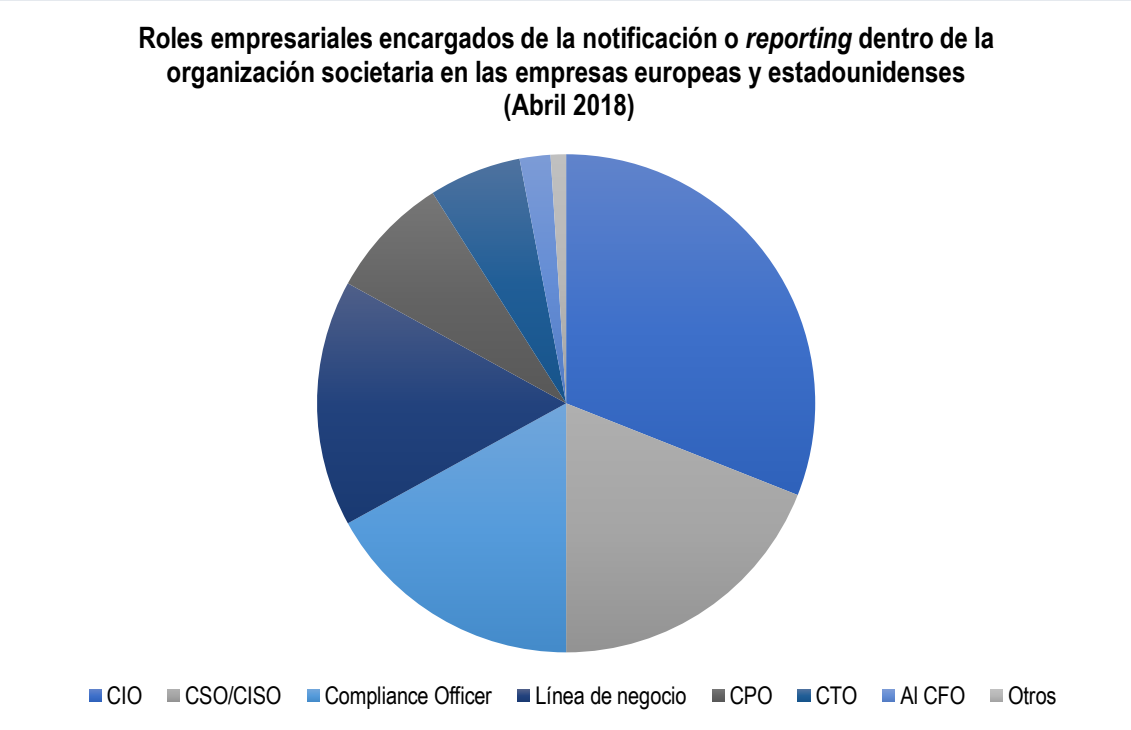
Fuente: *The Race to GDPR: A Study of Companies in the United States & Europe*. McDermott Will & Emery LLP and Ponemon Institute LLC. April 2018

Gráfico 6



Fuente: *The Race to GDPR: A Study of Companies in the United States & Europe*. McDermott Will & Emery LLP and Ponemon Institute LLC. April 2018

Gráfico 7



Fuente: *The Race to GDPR: A Study of Companies in the United States & Europe*. McDermott Will & Emery LLP and Ponemon Institute LLC. April 2018