universidad de león
Facultad de Ciencias Económicas y Empresariales

Facultad de Ciencias Económicas y Empresariales
Universidad de León

Grado en Economía

Curso 2021/2022

COMPROMISO EN PYMES DE LA PROVINCIA DE LEÓN CON LA PROTECCIÓN DE DATOS DESDE UNA PERSPECTIVA ÉTICA

COMMITMENT OF SMEs IN THE PROVINCE OF LEÓN TO DATA PROTECTION FROM AN ETHICAL APPROACH

Realizado por la Alumna Dª. Patricia Ámez Rodríguez

Tutelado por la Profesora Dª Cristina Flores Acedo Carmona

León, 9 de septiembre de 2022

MODALIDAD DE DEFENSA PÚBLICA: x Tribunal □ Póster

ÍNDICE DE CONTENIDOS

ÍNDICE DE GRÁFICOS

RESUMEN

Cada día cobra más importancia la protección de datos debido a la era de la digitalización en la que nos encontramos. Los cambios en la forma de recopilación masiva de datos (*big data*) han contribuido a la necesidad de realizar cambios en la legislación en materia de protección de datos (RGPD).

Los enfoques de las empresas a la hora de decidir realizar la protección de datos pueden ser variados, y uno de ellos es el enfoque ético. Desde una perspectiva ética, la correcta adecuación de una empresa a la protección de datos podría asimilarse como una estrategia de responsabilidad social corporativa (RSC).

En este trabajo se analiza el nivel de concienciación de las pymes de la provincia de León con la protección de datos y se utiliza esta perspectiva ética para analizar si podría ser eficaz para promover en las pymes la concienciación de la necesidad de garantizar la protección de datos. Se realizaron 130 entrevistas telefónicas a pymes explicando lo que es la RSC y lo que ésta supone para la empresa. Los resultados apoyan la idea del desconocimiento que existe en estas pymes sobre RSC y su posible influencia positiva para aumentar ese compromiso.

Palabras clave: protección de datos, RGPD, big data, responsabilidad social corporativa, ética empresarial, estrategia empresarial

ABSTRACT

Data protection is growing in importance due to the digitalization era the world is living in. The changes in the way data is collected on a massive scale (big data) have contributed to the need for amendments to data protection laws (GDPR).

Companies' approaches when implementing data protection can be manifold, including the ethical approach. From an ethical perspective, a company's proper data protection compliance may be considered as a corporate social responsibility (CSR) strategy.

This paper analyses the level of awareness of SMEs in the province of León regarding data protection. It uses the ethical perspective to assess the effectiveness of this approach when promoting the need for data protection among SMEs. A total of 130 telephonic interviews were conducted explaining SMEs what CSR consists in and what it would imply for the company. The results support the idea of a lack of awareness regarding CSR and its potential positive impact on increasing companies' commitment to it among SMEs.

Keywords: data protection, GDPR, big data, corporate social responsibility, business ethics, business strategy.

1. INTRODUCCIÓN

La protección de datos es una materia todavía desconocida para muchos, a pesar de tratarse de una legislación imprescindible y básica a día de hoy. Esta importancia de la protección de datos puede considerarse consecuencia de que las tecnologías jueguen un papel fundamental en nuestra sociedad, ya que ello conlleva una recogida y traspaso masivo de información personal de todos los usuarios, tanto dentro como fuera de la red.

Este tratamiento masivo de datos, conocido como *Big data*, y al que se hará alusión en numerosas ocasiones de aquí en adelante, sirve como causa explicativa para el avance y actualización del R.G.P.D.[1], así como para el surgimiento de la necesidad de la LOPD.[2]

Por medio de este trabajo, se pondrá *el big data* como contexto de las variaciones de la legislación de protección de datos con el fin de explicar la creciente necesidad, tanto para las empresas como para sus grupos de interés, de llevar a cabo una adecuada política de protección de datos dentro de las organizaciones. También se abordará la forma de realizar la protección de datos correctamente para analizar el nivel de cumplimiento actual de dicha legislación.

En este sentido, resulta interesante señalar que la protección de datos se puede analizar desde diferentes puntos de vista, como puede ser el puramente legislativo, el punto de vista de los derechos fundamentales, o utilizando una perspectiva ética. El enfoque ético será el más utilizado en el presente documento, con la finalidad de proponer la protección de datos como una alternativa de estrategia competitiva de responsabilidad social corporativa (RSC). El hecho de utilizar este enfoque ético explicando lo que supone seguir una estrategia de RSC obedece a la creencia de que este enfoque puede promover un mayor compromiso con el cumplimiento de la legislación en materia de protección de datos por parte de las empresas.

Para ello, la responsabilidad social corporativa será utilizada debido al compromiso que ha de tener la empresa con sus grupos de interés (empleados, trabajadores, clientes…) siendo la protección de datos interpretada como un derecho de estos grupos de interés. De la misma manera, se plantea el cumplimiento de la legislación como el pilar básico de

[1] Reglamento General de Protección de Datos.

[2] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

la responsabilidad social corporativa.

Además, dependiendo del entorno en que se encuentre la empresa (ubicación geográfica, sector, etc…) y del tamaño de la misma, a la hora de llevar a cabo un análisis de su compromiso con la protección de datos, se podría llegar a diferentes resultados, y tratar de dar soluciones a la protección de datos atendiendo a esta diversidad de circunstancias daría como resultado propuestas poco concluyentes y concretas. Por eso, se ha decidido analizar el caso concreto de las pymes[3] de la provincia de León para llegar a conclusiones más específicas adaptadas a este sector.

Más concretamente, el objetivo del estudio se centra en conocer el compromiso ético de las pymes de la provincia de León, analizado desde la perspectiva del cumplimiento y adecuación de estas a la ley de Protección de Datos.

Este análisis y sus conclusiones podrán servir de ayuda a las empresas de la provincia que se dediquen a la guía y adecuación de otras entidades en materia de protección de datos.

De esta manera, explicando la importancia que tiene una correcta adecuación de su empresa al RGPD, y los efectos que tiene sobre la misma desde la perspectiva de la responsabilidad social corporativa, se podría considerar una nueva estrategia de acceso a otras empresas. Es decir, se trataría de exponer los efectos que podría tener la protección de datos tratándola desde una perspectiva ética, concretamente desde la perspectiva de la responsabilidad social corporativa, lo cual podría ser una vía de acceso a nuevos clientes ya que, presentando esta obligación desde esta perspectiva, los clientes considerarán la importancia de la protección de datos más allá de una mera obligación legislativa y valorarán sus consecuencias más allá de una posible sanción.

2. METODOLOGÍA

Con la finalidad de alcanzar los objetivos anteriormente expuestos, se ha procedido, por un lado, a recopilar información bibliográfica, para la elaboración de una parte teórica, y, por otro, se llevó a cabo un proceso de investigación.

El trabajo está estructurado de manera que en primer lugar se realiza una recopilación de información, tanto bibliográfica como legislativa. La literatura académica ha sido

[3] Acrónimo de pequeña y mediana empresa. 1.f. Empresa mercantil, industrial, etc., compuesta por un número reducido de trabajadores, y con un moderado volumen de facturación. (RAE, 2021).

recuperada, de artículos y tesis académicas, y la última se obtuvo del BOE y del Reglamento General de Protección De Datos[4].

Esta información académica y legislativa, servirá para contextualizar y para definir determinados conceptos como son el *big data,* la protección de datos como derecho fundamental, ética empresarial y responsabilidad social corporativa, que más adelante servirán para entender el análisis de los datos obtenidos a través de las entrevistas que se han llevado a cabo.

En segundo lugar, el proceso de investigación se realizó de forma directa, realizando entrevistas telefónicas a 130 pequeñas y medianas empresas de la provincia de León. De estas 130 empresas, 127 eran clientes del contacto[5] que facilitó la conexión con estas empresas, con la previa autorización de las mismas, y con la condición de mantener su anonimato. Otras 3 empresas entrevistadas no figuraban en el listado de clientes facilitado anteriormente, es decir, fueron contactadas directamente. Tras realizar el análisis de esas 130 empresas, se pudo utilizar la información de un total de 114, debido a que el resto de respuestas no aportaba información determinante para el estudio, como se explicará más adelante.

Antes de llegar a ese número de empresas encuestadas, hay que decir que, en un principio, se pusieron dos condiciones para elegir las empresas susceptibles de análisis. La primera condición fue que se tratase de pequeñas y medianas empresas de la provincia de León, y la segunda condición fue que se tratase de empresas con más de un empleado, es decir, que no se tratase de autónomos sin ningún empleado a su cargo, ya que las empresas con empleados han de tener una mayor cantidad de documentos firmados al día, lo que demuestra que esa empresa está correctamente adecuada al Reglamento General de Protección de Datos. Así, considerando solo estas empresas con empleados se conseguirá realizar un estudio más completo de las empresas en lo que se refiere a la protección de datos.

Dadas estas condiciones, se eligieron las empresas clientes del contacto, de las cuales

[4] 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 95/45/CE (Reglamento General de protección de datos).

[5] Empresa de León especializada en la guía y adecuación de otras empresas al Reglamento General de Protección de Datos.

podrían ser parte de la muestra 212, pero solamente se consiguió establecer contacto con 194, y al final accedieron a ser entrevistadas 127 de esas 194.

Estas empresas, antes de ser entrevistadas, fueron evaluadas de forma detallada por medio de un análisis de riesgos periódico realizado por la empresa que les guiaba y adecuaba a la protección de datos para conocer su grado de cumplimiento del RGPD, y los riesgos relacionados con el incumplimiento de la protección de datos a los que se encontraban sometidas.

Por otro lado, se intentó contactar también con otras 43 empresas directamente, se pudo hablar con 21, y solamente 3 de ellas quisieron contestar a las preguntas, así la estrategia de contacto a empresas desconocidas fue descartada debido a la ausencia de éxito en el acceso a las mismas.

Las entrevistas se realizaron sobre una serie de preguntas establecidas a priori, que fueron planteadas y redactadas de forma que se pudiera llegar al objetivo de la forma más breve y precisa. Se buscaba conocer, por un lado, el compromiso que tenían estas empresas con su adecuación al Reglamento General de Protección de Datos, y por otro, el nivel de asociación que mostraban los entrevistados entre la ética empresarial y la protección de datos, haciendo hincapié en el concepto de Responsabilidad Social Corporativa. En algún caso determinado, a pesar de tener las preguntas establecidas, se añadió alguna cuestión extra con el fin de obtener algún dato de interés adicional, o para poder concretar más lo ya aportado. Además, al 100% de las empresas entrevistadas se le explicó la importancia de la Responsabilidad Social Corporativa para el buen funcionamiento de una empresa, en este caso desde la perspectiva de la competitividad y prestigio, y la forma en que ésta se relaciona con la protección de datos, ya que el desconocimiento acerca de estas cuestiones era generalizado.

Se utilizaron dos modelos de entrevista, donde la formulación de las preguntas varió en función de quién era el entrevistado, si era el dueño de la empresa, o un empleado. El empleado no fue elegido de forma aleatoria ni impuesto por el propietario para que accediera a la entrevista, sino que era el responsable del tratamiento[6], en los casos en que este fuera diferente al dueño.

Una vez obtenidas todas las respuestas, se procedió a descartar las realizadas a los

[6] "*La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento"*(RGPD, 2021. p.33)

responsables del tratamiento cuando este era una persona diferente al propietario de la organización, debido a que el número de entrevistas obtenidas fue reducido, y no aportaba una proporción significativa dentro del total, de la misma manera que estas personas carecían de una capacidad suficiente de actuación y modificación de procedimientos en la actividad de la empresa, por lo que no sería útil esa información para los objetivos perseguidos.

Con los resultados obtenidos se trató de exponer unas conclusiones claras, de forma que las empresas dedicadas a la adecuación y guía de protección de datos de otras empresas puedan interpretarlas y utilizarlas para establecer una estrategia empresarial, con el fin de analizar nuevas formas de acceso o concienciación a la hora de adecuarlas y de revisar el cumplimiento del Reglamento General de Protección de Datos que estas empresas están llevando a cabo.

3. BIG DATA COMO CONTEXTO

3.1.CONTEXTUALIZACIÓN Y DEFINICIÓN DE BIG DATA

El punto de partida para poder hablar de *big data*, es mencionar el proceso de digitalización y evolución de la tecnología, enmarcado por la globalización[7], al que se encuentra sometida la sociedad actual, y no tan actual.

Tal y como recuerda Jorge Aragón (2016), ya en la década de los 80, Marcelino Camacho, en uno de los debates de la Comisión Confederal de Ciencia y Tecnología de CCOO, hizo la siguiente aportación: "La evolución tecnológica se ha presentado en las últimas décadas como una protagonista central de la evolución económica y social. De forma directa, casi en cualquier acto cotidiano, es posible encontrar referencias diversas a la llamada "revolución tecnológica": oferta de hogares computarizados con tele-compra, video-prensa, correo electrónico, robots domésticos…; informaciones instantáneas de lo que acontece en los más alejados países, nuevos alimentos genéticamente controlados, o academias para jóvenes y adultos dispuestas a adentrar a la persona que pague en los aspectos más complejos del conocimiento informático."

Hoy en día, en pleno siglo XXI, la sociedad se encuentra sometida a una observación

[7] "Proceso por el que las economías y mercados, con el desarrollo de las tecnologías de la comunicación, adquieren una dimensión mundial, de modo que dependen cada vez más de los mercados externos y menos de la acción reguladora de los Gobiernos" (RAE, 2021)

continuada casi de cada movimiento, debido a que, dado el contexto mencionado anteriormente, las nuevas tecnologías juegan un papel fundamental en la vida de la mayor parte de la población. Esto se puede explicar por medio del *big data* que, a pesar de carecer de una definición oficial específica, podría describirse como una recopilación y tratamiento de datos masiva.

Específicamente, algunos autores, como Martin et al.(2018), definen el *big data* de diferentes maneras, afirmando que la manera de definir el concepto dependerá del enfoque que se le dé, ya que se trata de un anglicismo[8]. Dos de las definiciones pueden ser las siguientes: [1] "aquel conjunto de datos que, por su tamaño ingente, sobrepasa la capacidad de ser gestionado por bases de datos de integración tradicionales"; [2]" *Big data"* es un activo de información de gran volumen, alta velocidad y gran variedad que exige formas rentables e innovadoras de procesamiento de información para mejorar el conocimiento y la toma de decisiones" (Martin et al., 2018, p.10).

Ahora bien, esta recolección de información se lleva a cabo sin que la población, en la mayoría de las ocasiones, sea consciente de ello. En este sentido, hay una popularización de la idea de que, por medio de los dispositivos móviles, la sociedad es vigilada en todo momento. Este fenómeno, es mucho más complejo de lo que parece, ya que, cuando no se analiza correctamente, puede ser interpretado como una conspiración de que "quién sabe qué se nos espía" a través de los dispositivos móviles y ordenadores.

Lo que realmente sucede, es que, una vez más, la tecnología puede ser un arma de doble filo, aunque es cierto que esta puede facilitar enormemente la vida de muchas personas, tanto a nivel personal como a nivel empresarial.

Lo que muchas personas no saben es que, desde el momento en el que se utiliza una aplicación en cualquier tipo de dispositivo, independientemente del que sea (GPS, pagar con tarjeta de crédito, etc. para lo cual es utilizado un datáfono o el propio teléfono móvil o reloj digital conectado, etc.) se están generando datos de manera automática, y, mucho más lejos de ser un método de espionaje, estos datos son recogidos y analizados, tal y como afirma Antonio Monleón-Getino (2015), por grandes compañías de la información, con la finalidad de mejorar los servicios online en función de las demandas electrónicas de los usuarios.

[8] Según la RAE se podría traducir al castellano como Macro datos. (Martin H., Calderón J., & Vargas J. 2018).

De la misma forma que se comentaba anteriormente sobre que las tecnologías son un arma de doble filo, ocurre lo mismo con el *big data*. No solo se considera una ventaja que mejora o facilita la experiencia de los usuarios a la hora de navegar, sino que también genera una serie de inconvenientes. Así, tal y como afirma la graduada en derecho Mar Guevara Sanmateo (2018), toda esta generación de datos, y su utilización e intercambio por parte de las compañías que recopilan la información, supone un problema más grande que los beneficios que aporta, y es la infracción uno de nuestros derechos fundamentales, el derecho a la protección de datos, ya que, en territorio europeo, este es considerado un derecho fundamental. Esto se recoge en el Tratado de Funcionamiento de la Unión Europea, artículo 16, así como en el artículo número 8 de la Carta de los Derechos Fundamentales de la Unión Europea[9].

3.2.BIG DATA Y TRATAMIENTO DE DATOS PERSONALES

Dada esa generación constante de datos por parte de la población, y su posterior análisis por parte de las compañías mencionadas, se cuestiona la privacidad que tiene la población y el acceso que hay a su información privada o datos personales, en gran parte, sin su consentimiento. El Reglamento General de Protección de Datos define como "datos personales" lo siguiente: "toda información sobre una persona física identificada o identificable (<<el interesado>>); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;" (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, p.33).

De la misma manera, a continuación, se define "tratamiento" como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;"

[9] En el apartado 4.1 se hablará más a fondo de la protección de datos como derecho.

(Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, p.33).

Lo que todo esto quiere decir, es que no solamente datos como nombre, apellidos y DNI son considerados datos personales identificativos de los usuarios, sino que, este concepto va mucho más allá.

Así, datos de carácter personal pueden ser desde datos económicos (como los pagos con tarjeta que se comentaban anteriormente), ideológicos, o políticos, hasta cualquier tipo de rastro que se pueda dejar en redes sociales (una foto, una frase, o un "me gusta" en, por ejemplo, Instagram).

De esta forma, las personas pueden ser identificadas por medio de muchas acciones de su vida diaria, y, entonces, cualquier tipo de acto que pueda llevar a esa identificación se puede considerar tratamiento de sus datos.

Considerando las definiciones aportadas por medio del Reglamento General de Protección de Datos, y su posterior interpretación en el contexto pertinente, la descripción de la situación actual en relación al *big data*, genera la necesidad de asociar el mismo, con la protección de datos personales.

4. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y LOPD

La importancia del big data en la actualidad, se debe a que la posesión de datos de tipo personal puede considerarse un medio de cambio más, incluso puede ser un factor de medida de "riqueza" en el entorno empresarial, ya que estos datos tienen un valor económico, y no económico, muy elevado. El valor de estos datos y el volumen que se maneja de los mismos en la era del *big data*, ha provocado que varíen las necesidades, especialmente legislativas respecto a la legislación relativa a la protección de datos, por lo que esta ley ha tenido que ser sometida a diferentes modificaciones.

4.1. EVOLUCIÓN DE LA LEGISLACIÓN EN MATERIA DE PROTECCIÓN DE DATOS

Una vez definidos el concepto *big data* y la situación actual, se puede partir de la base de

que, como afirma Jorge Seco (2019), la creciente importancia y valor social, económico y político de la información personal o datos personales tiene como consecuencia directa un aumento de la cantidad y gravedad de los riesgos que se derivan del tratamiento de estos datos.

Esto genera la necesidad de una modificación legislativa en materia de protección de datos, incrementando las medidas a adoptar a la hora de proteger dicha información, así como las correspondientes sanciones en función de los riesgos que se generen.

La normativa actual en materia de protección de datos, a nivel europeo, se recoge en el Reglamento General de Protección de Datos, que fue aprobado, después de haberse trabajado y realizado los pertinentes ajustes, durante cuatro años, por el Parlamento Europeo y el Consejo de la Unión Europea. Se trata del "Reglamento (UE) 2016/679 del parlamento 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 datos" (RGPD, 2016).

Hasta ese momento, la normativa que estaba vigente era 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 respecta al tratamiento de datos personales y a la libre circulación de estos datos*"* (Agencia Estatal Boletín Oficial del Estado, 1995).

Dadas las circunstancias, fue necesaria esa modificación, ya que, aunque mantenga principios comunes con la anterior vigente, se persigue la finalidad de que los Estados miembros de la Unión Europea se encuentren ante un reglamento uniforme y homogéneo, para evitar diferencias entre las normativas específicas de cada Estado.

La entrada en vigor de este reglamento se produjo en el año 2018, ante el cual, en España, se generó la necesidad de promover una normativa específica para el territorio nacional, con el fin de adaptarse a este nuevo reglamento.

Y es que, desde el año 1999 hasta ese momento, estaba en vigor la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, la cual se había quedado anticuada y no se correspondía con lo impuesto en el nuevo Reglamento General de Protección de Datos debido a que dicha ley iba en consonancia con la Directiva 95/45/CE. Así pues, esta ley fue derogada, salvo ciertas excepciones[10] (Seco, 2019) con la entrada

[10] "La disposición derogatoria única de la LOPDGDD nos dice que deroga la anterior normativa en materia

en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Con el paso de los años, concretamente tres años, se produjeron ciertas modificaciones y mejoras, que permitieron llegar a una ley actualizada y completa, la cual está vigente hoy en día. Se trata de la "Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales" (Agencia Estatal Boletín Oficial del Estado, 2021) que será conocida como LOPD 7/2021.

Esta última modificación ha producido cambios en torno a los poderes de las fuerzas y cuerpos de seguridad del Estado, así como al poder judicial, respecto a la recopilación y tratamiento de datos de carácter personal. Así, con esta modificación, estos organismos tendrán una capacidad especial en las etapas de toma y tratamiento de datos, eximiéndoles de la necesidad de realizar los procesos adicionales que cualquier empresa está obligada a llevar a cabo para esta recogida y tratamiento de datos, como puede ser, por ejemplo, la obligación de firmar consentimientos para el tratamiento y cesión de datos personales por parte de la persona de la que se recogen los datos.

De cualquier manera, esta reducción de limitaciones en la captación y tratamiento de datos no supondrá un problema para la información que estas figuras jurídicas (fuerzas y cuerpos de seguridad del Estado, así como el poder judicial) puedan recopilar y tratar, sino que, con esta reforma, se estaría determinando concretamente que estas personas tienen un poder especial para la toma de datos, pero no por ello esos datos serán más vulnerables ni se verán sometidos a ningún riesgo.

Por todo ello, con la última modificación, la Ley Orgánica de Protección de Datos, dentro del territorio español, estará cumpliendo la normativa de la UE, de una forma más actualizada y amplia que la LOPD 3/2018, pero sin derogarla.

4.2.APLICACIÓN DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS EN PYMES

de protección de datos sin perjuicio de lo dispuesto en la disposición adicional decimocuarta y transitoria cuarta, relativas al artículo 13 de la Directiva 95/45/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" Jorge Seco (2019).

Desde un lenguaje profesional, se hace referencia a la aplicación del Reglamento General de Protección de Datos en una empresa como "*Adecuación de una empresa al Reglamento General de Protección de Datos".*

El primer aspecto a tener en cuenta es que, en España, cualquier empresa que lleve a cabo procedimientos en los cuales se utilicen datos personales, ha de adecuarse al Reglamento. De no ser así se estaría incumpliendo el mismo, y así, la Ley Orgánica de Protección de Datos. El hecho de incumplir una normativa o ley en España, siempre y cuando el organismo correspondiente[11] tenga constancia de ello, tendrá como consecuencia hacer frente a la correspondiente sanción.

Desde la perspectiva de las empresas, llevar una adecuada política de protección de datos es, realmente, hoy en día, una obligación en el más sentido estricto de la palabra. Aunque más adelante, mediante el estudio de la muestra correspondiente, se analizará si estas empresas se lo toman como una obligación, o existe un compromiso ético de las mismas más allá de la ley.

Para poder conocer cómo se debe adecuar correctamente una empresa al Reglamento General de Protección de Datos, es interesante diferenciar quienes son los que tienen responsabilidad en estas cuestiones ante dicha legislación.

La Agencia Española de Protección de Datos es el organismo ante el cual hay que responder en caso de incumplimiento, y ante el que se puede presentar una denuncia cuando se conoce que alguien está utilizando información personal sin una adecuada protección, o de una forma poco segura. Por ello, es interesante conocer cómo se define a los responsables de la protección de datos, ya que lo hace de una forma clara y sencilla, tal y como se describe a continuación "Si tratas datos o información sobre personas físicas que permitan su identificación, utilizas estos datos con fines determinados y tomas decisiones relacionadas con los fines para los que utilizas estos datos personales o los medios en los que llevas a cabo el almacenamiento y la forma de procesar los datos, eres "el responsable" de la actividad de tratamiento de estos datos". (Agencia Española de Protección de Datos, derechos y deberes – cumple tus deberes. 2022),

De esta forma, define de forma concisa quiénes son los responsables a los que exigir el cumplimiento de las leyes de protección de datos, ya que, en caso de alguna irregularidad,

[11] En este caso, la Agencia Española de Protección de Datos.

tal y como especifica el Reglamento (UE) 2016/679 en el artículo 82, serán el responsable del tratamiento (la empresa) y el encargado del tratamiento quienes han de responder ante la Agencia Española de Protección de Datos y ante la persona afectada.

En el caso de las pymes, cuando hay más de un trabajador, puede haber una diferenciación de responsabilidades, y la persona que utiliza o trata datos, puede no ser el responsable del tratamiento. En pocas palabras, la Agencia Española de Protección de Datos, derechos y deberes – cumple tus deberes (2022) lo define así: "Si almacenas o procesas datos o información sobre personas físicas siguiendo las instrucciones de quien toma decisiones sobre los fines y los medios en los que los datos son procesados ("el responsable") eres "el encargado" de la actividad de tratamiento de estos datos".

Por último, es importante también mencionar la especificación, respecto al ámbito de aplicación de las normas de protección de datos, a la que hace referencia la Agencia Española de Protección de Datos: "Por el contrario, si almacenas o procesas datos personales únicamente en el ejercicio de tus actividades personales o domésticas, los requisitos de la normativa de protección de datos no son de aplicación en el ámbito de dichas actividades. Para cada actividad de tratamiento de datos personales que llevas a cabo como responsable o en la que participas como encargado, debes tener en cuenta las obligaciones que el RGPD (Reglamento General de Protección de Datos) y la LOPDGDD te exigen para proteger a las personas físicas cuyos datos estás tratando". (Agencia Española de Protección de Datos, derechos y deberes – cumple tus deberes, 2022).

Otra figura a tener en cuenta, y quizá la más importante, sea la del delegado de protección de datos. De hecho, el Reglamento (UE) 2016/679 dedica a este una sección completa[12], especificando que las funciones de este, definidas por el nuevo Reglamento de Protección de Datos (2016), serán como mínimo las siguientes:

- Informar y asesorar al personal competente de la empresa, de las responsabilidades y obligaciones que les correspondieran.
- Realizar los procesos correspondientes con la finalidad de supervisar el adecuado cumplimiento de la política de protección de datos en la empresa.
- Formar y concienciar al personal.

[12] Reglamento UE 2016/679. Sección 4. Delegado de Protección de Datos.

- Asesorar cuanto sea necesario en relación a las evaluaciones de impacto[13] que se ha de llevar a cabo.
- Cooperar con la autoridad de control. En el caso de España, es la Agencia Española de Protección de Datos (AEPD).
- Tener la posición de punto de contacto entre la autoridad correspondiente (AEPD) y las entidades, en materia de dudas y de incidencias.

El Artículo 37 del Reglamento 2016/679 (RGPD) afirma, por medio de diferentes casos y supuestos, que es considerablemente elevada la necesidad de un delegado de protección de datos en el procedimiento de adecuación de una empresa, reduciendo al mínimo las ocasiones en las que se pueda prescindir de uno.

En resumen, el responsable del tratamiento como tal, siempre será la propia empresa, aunque se nombrará una persona física dentro de la misma con el fin de facilitar la identificación del mismo. El encargado o los encargados del tratamiento pueden encontrarse tanto dentro como fuera[14] de la empresa, y el delegado de protección de datos puede ser también interno o externo, pero siempre ha de tener la titulación correspondiente para poder llevar a cabo sus responsabilidades.

Una vez conocidas las principales figuras relacionadas con la protección de datos en una empresa, se puede comenzar a hablar de diferentes pasos dentro del procedimiento de adecuación de una empresa al Reglamento General de Protección de Datos.

En este sentido, hay que distinguir dos tipos de adecuación, por un lado, las que hace la propia empresa, cuando cuenta con un delegado de protección de datos entre el propio personal, y, por otro, las que se realizan contratando el servicio de una empresa ajena especializada en la protección de datos. A pesar de que ambos procedimientos son habituales, en el caso de las pymes, que es el que se analiza en este documento, contratar los servicios de profesionales externos es el procedimiento más habitual y eficiente. Sin embargo, el procedimiento en sí mismo, en su mayoría, indistintamente de la forma en

[13] Evaluación de impacto: procedimiento que se llevará a cabo por parte del personal competente en la protección de datos de la empresa, y que tiene como finalidad analizar los riesgos a los que la empresa está sometida y, como su propio nombre indica, el impacto que tendría, cuando no se está realizando de forma precisa la protección de datos. Se desarrollará de forma más precisa en el apartado 2.3.

[14] Pueden tener la atribución de encargados del tratamiento empresas externas que sean contratadas con la finalidad de realizar determinadas tareas (Por ejemplo: las asesorías para materia fiscal, contable y laboral, o una persona externa que lleve a cabo el mantenimiento del sitio web).

que se haga, (ya sea interna o externa), es prácticamente igual.

Así pues, el primer paso del procedimiento de adecuación de una empresa al Reglamento General de Protección de Datos es la toma de datos por parte del personal de la empresa que se encarga de la adecuación, con el fin de conocer al detalle la forma de trabajo del cliente y analizar la forma de adecuarla correctamente al Reglamento General de Protección de Datos. En esta recogida de datos se obtendrá la información acerca del ciclo de vida de los datos dentro de la entidad (Reglamento General de Protección de Datos, 2016).

El ciclo de vida de los datos se refiere al proceso completo al cual están sometidos los datos personales que se captan por la empresa desde su recogida hasta su eliminación. Dentro de este ciclo de vida, se pueden diferenciar las siguientes 5 etapas: captura de datos, clasificación o almacenamiento, uso o tratamiento, cesión o transferencia, y destrucción o eliminación (Reglamento General de Protección de Datos, 2016).

Todas y cada una de estas etapas son igual de importantes, y en todas y cada una, siempre hay que tener un cuidado especial, por su delicadeza, cuando se trata de datos especialmente protegidos. Este tipo de datos tienen mención especial en el artículo 9 del Reglamento (UE) 2016/679 denominados como "categorías especiales de datos personales" de forma que "Quedan prohibidos los tratamientos de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física" (RGPD, 2016, p.38). Ante los mismos, el Reglamento hace excepciones en determinadas circunstancias, que, en conclusión, se darán cuando las personas o sus representantes legales den un consentimiento expreso al tratamiento de los mismos, para fines siempre especificados de antemano y siempre por parte de un profesional especializado en la materia (RGPD, 2016).

Una vez analizada la información recogida, y teniendo en cuenta las menciones especiales de los datos, el delegado de protección de datos será la figura clave dentro de las empresas especializadas para poder adecuar otras entidades al Reglamento[15]. Este delegado hará un

[15] Fuente: Reglamento General de Protección de Datos. 2016.

meticuloso análisis de la información obtenida, dando lugar al que se podría considerar el segundo paso, que es la elaboración de documentación personalizada para la empresa en cuestión, con el fin de que sea recibida y aplicada por el personal de la empresa (RGPD, 2016).

Entre esta documentación, por ejemplo, se encontrarían los archivos correspondientes a ficheros del consentimiento de uso de datos personales que han de firmar tanto empleados, como clientes, o cualquier persona que facilite información personal a la empresa. Los encargados y responsables del tratamiento, de los que se habló con anterioridad, han de firmar el correspondiente documento, asumiendo la responsabilidad que asumen en sus labores (RGPD, 2016).

El tercer y último paso se puede resumir en que todo lo que la empresa ha de conocer y aplicar se ha de facilitar por su asesor o guía de protección de datos, como resultado del análisis llevado a cabo por el delegado de protección de datos. Es habitual que se entregue en formato papel y en formato digital la documentación correspondiente, por seguridad, pero también se puede dar el caso de que solo se facilite un tipo de fichero (RGPD, 2016)

Desde el momento que la empresa especializada recibe la documentación correspondiente, el personal tendría que recibir la formación necesaria para desempeñar sus labores, así como conocer la identidad de las figuras principales asignadas en la empresa para realizar las tareas de protección de datos.

4.3.RIESGOS DE NO CUMPLIR ADECUADAMENTE EL RGPD Y FORMAS DE DETECCIÓN

Una mala o insuficiente adecuación al reglamento puede ocasionar brechas de datos personales[16], siendo las consecuencias de estas de diferentes niveles de gravedad, así como de diferentes tipos (Agencia Española de Protección de Datos, 2021).

Para evitar incurrir en los problemas ocasionados por el incumplimiento del Reglamento y de la LOPD, o, detectarlos a tiempo, sería de gran interés que los profesionales especializados llevasen a cabo un análisis regular de la actividad empresarial en materia

[16]Definición de brecha de datos personales: "Una brecha de datos personales es un incidente de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizado a los mismos" (Agencia Española de Protección de Datos. 2022)

de protección de datos.

Este análisis, denominado auditoría o estudio de verificación del cumplimiento de la protección de datos, sirve para prevenir los riesgos que se puedan ocasionar, y normalmente se realiza por medio del estudio de los datos necesarios recogidos previamente por la empresa especializada en la protección de datos, mediante un proceso similar a la primera toma de contacto con su cliente, con el fin de obtener la información necesaria para conocer la forma en la que se está aplicando lo dispuesto por el delegado.

Un correcto análisis realizado a tiempo puede evitar que casi cualquier problema detectado por el delegado derive en consecuencias graves para la empresa, ya sean daños económicos directos (pérdidas económicas, sanciones…), o reputacionales. Esto se debe a que si el delegado detecta alguna brecha puede analizar su gravedad, y así determinar el periodo de tiempo en el que se ha de solventar para que no se produzcan daños de gravedad en la empresa. (AEPD, 2021)

El estudio que los delegados llevan a cabo se conoce como evaluación de impacto, el cual incluye un análisis de riesgos mediante el cual se evalúan los riesgos a los que está sometida la empresa cuando se detecta en la misma la mala o insuficiente implementación de alguna de las medidas dispuestas. Posteriormente será entregado al cliente un informe de verificación de cumplimiento de protección de datos, con el fin de que se pueda demostrar por parte del profesional, que está realizando las cosas bien, o, por el contrario, las cosas que debería mejorar (AEPD, 2021).

La Agencia Española de Protección de Datos, en su sitio web, pone a disposición de cualquier ciudadano una guía mediante la cual se pueden identificar los riesgos de los tratamientos, con el fin de realizar de forma correcta la evaluación de impacto (AEPD, 2021).

De la interpretación de los riesgos de la "Guía de gestión del riesgo y evaluación de impacto en tratamientos de datos personales" (2021) de la Agencia Española de Protección de Datos (2021), pueden concluirse las siguientes amenazas generales:

- Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales.
- Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a

las que pueda estar sujeto el responsable del tratamiento.

- Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas, en particular, cuando se producen pérdidas de datos personales.
- Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad.
- Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.
- Incorporación tardía de los expertos en protección de datos (en particular, del delegado de protección de datos o DPO) al proyecto o definición deficiente de sus funciones y competencias.

La utilización de esta guía puede ser llevada a cabo por cualquier persona, pero en ese caso probablemente la interpretación no será óptima, por ello siempre es recomendable dejarlo en manos de los profesionales. Además, el análisis de riesgos posteriormente será necesario para llevar a cabo la evaluación de impacto, por lo que es extremadamente importante que se realice meticulosamente.

Así pues, las consecuencias que podría conllevar un incumplimiento del RGPD, establecidas en la Ley Orgánica de Protección de Datos 3/2018 serían tanto económicas, como reputacionales, sabiendo que estas últimas, indirectamente derivan también en las primeras. Incumplir el Reglamento significaría estar incumpliendo también la Ley Orgánica de Protección de Datos, lo que, estaría penado con importantes sanciones económicas (LOPD 3/2018, 2018).

Estas sanciones se impondrán en función de la gravedad que se les considere. La gravedad de las infracciones es establecida en el título IX "Régimen sancionador" de la LOPD 3/2018, y esta consideración de gravedad se categoriza en "infracciones consideradas muy graves", "infracciones consideradas graves" e "infracciones consideradas leves". Las cantidades de las sanciones, por tanto, variarán en función de estas categorías y de las circunstancias de cada caso individual, y son determinadas por el artículo 83 del Reglamento UE 2016/679, el cual establece que este importe podría ascender hasta 20.000.000 de euros.

Las cifras de las multas podrían ascender a estas cantidades tan elevadas debido a que,

cuando se produce una infracción en relación a los datos personales identificativos de cualquier persona, independientemente de tratarse de datos especialmente protegidos o no, se estaría violando algo considerado como derecho dentro del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (2000).

5. PROTECCIÓN DE DATOS Y ÉTICA EMPRESARIAL

5.1.LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL

El preámbulo de la Carta de los derechos fundamentales de la Unión Europea, con su última modificación en el año 2000, dice lo siguiente, indicando para qué fines se llevó a cabo:

Los miembros de la Unión Europea "han decidido compartir un porvenir pacífico, basado en valores comunes. […] Para ello es necesario, dándoles mayor protección mediante una Carta, reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos. […] El disfrute de tales derechos conlleva responsabilidades y deberes tanto respecto de los demás como de la comunidad humana y de las generaciones futuras" (Carta de los derechos fundamentales de la Unión Europea, 2000, p.8).

Bajo este preámbulo, conociendo la finalidad de la Carta de los derechos fundamentales de la Unión Europea, hay que ubicar la protección de datos personales dentro de esta. El derecho a la protección de datos personales se recoge dentro del Título II sobre Libertades, artículo 8, y dice así:

" 1. Toda persona tiene derecho a la protección de datos de carácter personal que le conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente." (Carta de los derechos fundamentales de la UE, 2000, p.10)

Una vez dicho esto, se puede comenzar a analizar la protección de datos desde otra perspectiva porque desde este momento, se considera el marco legislativo que regula la

protección de datos personales, así como el contexto de la situación a nivel global actual que dan una idea de la importancia que tiene la protección de datos. La razón es que, si hasta ahora se ha mostrado con lo aportado anteriormente lo importante que es llevar una adecuada política de protección de datos, de ahora en adelante, lo será aún más, y en más sentidos, dado que ahora ya se ha expresado que la protección de datos es considerada un derecho fundamental en la Unión Europea.

El derecho a la protección de datos personales tiene tal importancia que se establece en la Carta de los derechos fundamentales de la Unión Europea junto con el derecho a la libertad y la seguridad, así como el derecho a la libertad de pensamiento, conciencia y religión o incluso el derecho a la educación (Carta de los derechos fundamentales de la Unión Europea, 2000).

La diferencia es que, si se analiza el grado de conocimiento de estos derechos entre la población, estos últimos derechos y libertades mencionados serían conocidos prácticamente por todos, y el derecho a la protección de datos personales se podría considerar como desconocido. Por tanto, a partir de aquí, se pasará a analizar este derecho desde otras perspectivas.

Hasta ahora, la legislación era lo que marcaba el cumplimiento del Reglamento General de Protección de Datos, pero, una vez reconocido que es un derecho fundamental, hacerlo cumplir diligentemente, se podría considerar no solo como un acto legítimo, sino también como un acto éticamente correcto.

Y es que la buena conducta de cumplir el Reglamento General de Protección de Datos, en función de su condición como derecho por la información que recoge, tiene un gran valor en cualquier ámbito, pero tiene una especial relevancia dentro del mundo empresarial, debido a que hoy en día, un comportamiento éticamente correcto, puede llegar a tener una repercusión positiva a nivel competitivo debido a que "Nada es más hábil que una conducta irreprochable" (Artiaga, 2009).

5.2. ÉTICA EMPRESARIAL: RESPONSABILIDAD SOCIAL CORPORATIVA

La conducta ética en una empresa no está definida en ningún marco legislativo, sino que, depende la propia empresa hacerlo o no, es decir, la entidad adoptará el comportamiento ético de forma voluntaria. Este tipo de comportamiento se conoce bajo diferentes

denominaciones, como pueden ser: código ético, código de conducta, códigos de buenas prácticas, códigos de buen gobierno… Los códigos de los que hablamos son documentos elaborados por las empresas, en los cuales se desarrollarán las reglas y principios que definen pautas o normas para el buen funcionamiento de una empresa. Los tipos de códigos éticos, tal y como relata Fernando Navarro en su libro "Responsabilidad Social Corporativa: teoría y práctica" (2012) se pueden resumir en 3 categorías:

- "Profesionales o deontológicos", que se determinarán en función del gremio de la empresa.
- "Sectoriales", caracterizados por el tipo de actividad empresarial.
- "Empresariales u organizacionales": serán los que se determinen en el funcionamiento interno de una empresa.

Es habitual que los tres tipos de códigos se lleven a cabo a la vez en las empresas de forma complementaria, y no necesariamente el cumplimiento de uno excluye el cumplimiento de los demás (Navarro, 2012).

En el presente trabajo será de mayor importancia para el estudio que se realizará el código ético empresarial u organizacional, debido a que el siguiente apartado se centrará en la Responsabilidad Social Corporativa, la cual se podría considerar que está estrechamente relacionada a este código ético.

Ahora bien, el código ético empresarial, tiene como principales objetivos, siguiendo las pautas de Navarro (2012):

- "Dar a conocer la personalidad de la empresa, su carácter, su proyecto común, sus compromisos con los grupos de interés"
- "Diferenciarse de otras empresas".

"Un código ético es una carta de presentación que sirve para reforzar aquellos aspectos por los que apuesta la empresa y la distingue del resto." (Navarro, 2012, p. 112).

Resulta interesante hacer un paréntesis en este punto para mencionar la afirmación de Acosta (2013, p. 4): "Todas las empresas tienen una obligación ética, con cada uno de los cinco grupos que las constituyen: propietarios, accionistas, empleados, clientes, proveedores y la comunidad en general. Pero no solo en términos de normas y deberes como reglas, sino en términos de valores: la libertad, la igualdad, la solidaridad, el respeto

activo y el diálogo".

Y es que, como se ha comentado, el código ético empresarial u organizacional determinará los códigos de conducta de una entidad, que deberán ir en función de los intereses propios y de los grupos de interés o *stakeholders.*

El concepto de grupos de interés o *stakeholders,* a lo largo de los años se ha ido definiendo de diferentes formas, sin mostrar notables variaciones, por lo que se van a mencionar tres definiciones:

- "Son llamados colectivamente *stakeholders* de la corporación aquellos hacia los que la empresa tiene cualquier obligación moral" (de George, 1989, p.133)
- "Son *stakeholders* todos los grupos sin cuyo apoyo la organización podría dejar de existir" (*Institute Research Stanford*, 1963; Freeman, 1984, p.31).
- "Cualquier grupo o individuo que puede afectar o ser afectado por el logro de los objetivos de la empresa" (Freeman, 1984, p.24).

En función de estas definiciones, se podría asentar la idea de Acosta (2013) anteriormente mencionada acerca de la obligación ética de las empresas frente a estos grupos. De esta forma, se puede definir el concepto que se utilizará para el posterior análisis empresarial: el concepto de Responsabilidad Social Corporativa[17].

Sería de gran relevancia tener en cuenta tres conceptos que podrían considerarse que están interrelacionados, y que podrían dar lugar a confusión si no se tuvieran claros, que son responsabilidad social, responsabilidad social de la empresa, y responsabilidad social corporativa, por lo que serán definidos antes de avanzar en la materia para establecer sus diferencias. Aunque no sería extraño encontrar estos dos últimos conceptos como sinónimos, no está de más dar a conocer el pequeño matiz que podría permitir diferenciarlos.

La "responsabilidad social" trata del compromiso y el comportamiento de la población en general, así como diferentes instituciones y organizaciones, tanto públicas como privadas, con la finalidad de conseguir el bienestar social. (Fernández, 2009).

[17] Definición de Responsabilidad Social Corporativa o RSC: "Se entiende, según una definición de la Unión Europea de 2001, como "la integración voluntaria por parte de las empresas de las preocupaciones sociales y medioambientales en sus operaciones comerciales y sus relaciones con sus interlocutores" (Miotto, 2010. p. 42.)

En la "responsabilidad social de la empresa (responsabilidad social empresarial)" se podría aplicar la anterior definición, pero en este caso, se trataría del compromiso por parte de las organizaciones en lugar del compromiso de la población. En este caso podría definirse como la filosofía con la que actúa la empresa en el largo plazo frente a sus grupos de interés.

La diferencia entre la responsabilidad social empresarial y la responsabilidad social corporativa radica en que la responsabilidad social corporativa también incluye otras organizaciones, y la responsabilidad social empresarial solamente tiene en cuenta a empresas (Fernández, 2009).

Para hablar de la importancia del concepto de responsabilidad social corporativa, es interesante situarlo brevemente en un contexto socioeconómico reciente, basado en hechos que determinarán su importancia a día de hoy.

Los escándalos que se produjeron ya casi finalizado el siglo XX, acerca de grandes compañías, provocó que la opinión pública influyera de tal forma, que estas compañías tuvieran que dar explicaciones y respuesta a sus comportamientos. Hoy en día, lo que nació como una necesidad de salvación, frente a las exigencias de la ciudadanía, se ha convertido en una estrategia empresarial (Fernández, 2009).

Según Rivero (2006), la influencia de la responsabilidad social corporativa va en aumento en función del tamaño de la empresa, es decir, cuanto más grande es la empresa, mayor es la necesidad de aplicar este concepto, debido a la presión social derivada de los escándalos mencionados en el párrafo anterior. Aun así, en cualquier tipo de organización, una correcta aplicación de la responsabilidad social corporativa puede ser muy beneficiosa para la misma (Rivero, 2006).

Los principios en los que se asienta la responsabilidad social corporativa son los mismos para las pequeñas y medianas empresas como para las grandes compañías. Estos se pueden resumir en los siguientes (Fernández, 2009):

- "Cumplimiento de la legislación", en este caso, será la que esté vigente en cada país, o, cuando corresponda, las que se rijan internacionalmente.[18]

[18] Será de gran interés para, más adelante, poder interrelacionar la protección de datos, por medio del Reglamento General de Protección de Datos y la Ley Orgánica 7/2021, con la Responsabilidad Social Corporativa.

- "Tiene carácter global": afecta a todo el conjunto de la empresa, sin diferenciar departamentos o áreas de trabajo, independientemente de la actividad que se lleve a cabo en cada uno.
- "Comporta compromisos éticos objetivos", por lo que los mismos serán una obligación a partir del momento que se contraigan.
- "Se manifiesta en los impactos que genera la actividad empresarial", tanto a nivel económico, social, como medioambiental.
- "Se orienta a la satisfacción e información de las expectativas y necesidades de los grupos de interés".

Una vez expuestos los principios de la responsabilidad social corporativa, y especificados cuáles son los grupos de interés ante los que la empresa ha de rendir cuentas, sería interesante mencionar dos conceptos, relacionados con la responsabilidad social corporativa e interrelacionados entre sí: reputación y confianza.

La importancia del concepto de reputación concepto en la responsabilidad social corporativa reside en la generación de relaciones basadas en la confianza que se crea con los *stakeholders* o grupos de interés debido a que estos se consideran como la base del concepto de responsabilidad social corporativa (Navarro, 2012, y ello tendrá una influencia directa sobre todas las relaciones de la empresa. Esta capacidad que surge del compromiso con la responsabilidad social para influir sobre los grupos de interés y las relaciones dentro y fuera de la empresa es tan importante que la responsabilidad social podría considerarse como un activo (intangible) para la empresa, ya que tiene la suficiente capacidad para atraer a clientes, accionistas potenciales, proveedores, trabajadores, etc., así como para mantener a los actuales (Méndez, 2005).

Por otro lado, el concepto de confianza, en un principio, puede parecer que no tiene relación con la responsabilidad social corporativa, pero están muy ligados, y es que, mediante el compromiso con la responsabilidad social corporativa, tal y como se ha mencionado, se trata de satisfacer necesidades de todos los grupos relacionados, tanto internos (empleados), como externos (proveedores, clientes, etc.) (Miotto, 2010).

La pérdida de confianza, o más bien, generación de desconfianza que sufrió la población[19]

[19] "Según el 2009 Edelman Trust Brometer, en EEUU y Europa, la confianza hacia las empresas por parte de la sociedad bajó de un 58 por ciento a un 38 por ciento, cayendo aún más si consideramos el sector

ante las entidades financieras y las grandes empresas durante y después de la crisis del año 2008, así como hacia los medios de comunicación, según algunos autores como Miotto (2010), Fernández (2009) o Rivero (2006), ha tenido una gran influencia, o incluso se puede considerar el detonante del aumento de importancia de este concepto para las empresas, así como para su reputación.

Esta satisfacción de necesidades se podría traducir, en una generación de confianza por parte de los mismos, o, mejor dicho, el mal hábito de diferentes instituciones de perseguir únicamente una finalidad puramente financiera provoca una desconfianza por parte de toda la sociedad, lo cual supone un perjuicio para la compañía, y sería insostenible en el tiempo (Miotto, 2010).

Además, según algunos autores, como afirma Pedro Rivero (2016), la responsabilidad social corporativa se puede desarrollar e implementar con más eficacia en las pymes, debido a que poseen una capacidad de adaptación más rápida que otras organizaciones de mayor tamaño. Para poder adaptarse, las organizaciones han de conocer su entorno con la mayor precisión posible, y las pymes también cuentan con esa ventaja (Rivero, 2006).

5.3.LA PROTECCIÓN DE DATOS COMO ESTRATEGIA EMPRESARIAL DE RESPONSABILIDAD SOCIAL CORPORATIVA

La responsabilidad social corporativa como tal, puede funcionar como una estrategia empresarial, ya que, implementarla en las empresas, puede ayudarlas a acceder a nuevos mercados que cuenten con la exigencia de ser una empresa responsable (socialmente), a nuevas y mejores fuentes de financiación, o, incluso a un incremento de la publicidad de la empresa, de forma que esta se dé a conocer por su reputación e imagen (Rivero, 2006).

Todo esto se puede traducir en nuevas oportunidades de negocio, suponiendo una ventaja competitiva frente a otras empresas que no se vean comprometidas socialmente. Por ello, la Responsabilidad Social Corporativa puede ser tratada como una estrategia empresarial, basada en la diferenciación (Rivero, 2006).

Uno de los puntos a tratar tiene que ver con lo que se mencionó con anterioridad acerca de los pilares sobre los que se asienta la responsabilidad social corporativa que tenía que

bancario-financiero y el de la automoción. Estos valores son los más bajos desde que se elabora este informe" (Miotto, 2010, p. 42)

ver con el cumplimiento de la legislación correspondiente nacional, o internacional.

Pues bien, el cumplimiento de la "Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales" (Boletín Oficial del Estado, 2021) así como el "Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos", o Reglamento General de Protección de Datos (Boletín Oficial del Estado, 2016), siguiendo los principios ante los cuales se asienta la responsabilidad social corporativa, según RicardoFernández (2009), supondría el cumplimiento de los principios, pero merece la pena hacer especial mención al principio de "Cumplimiento de la legislación".

Por medio de la información aportada en los anteriores apartados del trabajo acerca de la protección de datos, así como al principio de este capítulo, donde se define la función de la responsabilidad social corporativa como estrategia empresarial, se procederá a continuación a enlazar ambos. Así, una correcta adecuación de una empresa al Reglamento General de Protección de Datos supondría estar respondiendo a los intereses de los *stakeholders* o grupos de interés de la empresa.

Este hecho se produciría siempre que la adecuación se realizara de forma correcta y completa, por medio de la firma de los documentos pertinentes, como contratos y permisos con clientes, proveedores, encargados del tratamiento, empleados, etc. y con la adopción de medidas recomendadas o impuestas por las personas especializadas en protección de datos[20].

El seguimiento de los protocolos a lo largo de todo el ciclo de vida de los datos dentro de una empresa supondría una óptima protección de estos, desde que son conocidos y recogidos por la empresa, hasta que desaparecen por completo. Los tipos de datos que recoja cada empresa iría en función de su actividad, de la misma manera que los grupos de interés no serían los mismos, por lo que ocurriría lo mismo con los procedimientos.

Pero, en cualquiera de los casos, la relación de la organización con todos y cada uno de sus grupos de interés, siempre y cuando sean personas (físicas o jurídicas), se podría ver

[20] Ya sea la empresa contratada para la gestión de la protección de datos, o en los casos en que se cuenta con un delegado de protección de datos dentro de la propia organización, el propio delegado.

influenciada por la protección de datos, ya que esta confidencialidad podría suponer un incremento de la confianza en la relación entre ambos.

Los conceptos de reputación y confianza, aparte del principio de cumplimiento de la legislación, serían los pilares sobre los que se podría asentar la relación entre la política de protección de datos de una empresa con la responsabilidad social corporativa.

La demostración de confidencialidad de los datos de personas y empresas asociadas a una entidad a través de la protección de clientes, empleados, proveedores, empresas asociadas (encargados del tratamiento), inversores, etc. incrementaría el bienestar de estos con la empresa, ya que sabrían que la empresa va a cumplir de esta forma su derecho fundamental a la protección de datos personales, y, por tanto, estos verán incrementada la confianza en la empresa.

De la misma manera, la protección de datos influenciaría en las relaciones externas de la empresa (con agentes externos, en este caso, por ejemplo, proveedores u otras empresas), además de generar confianza por parte de estos grupos de interés y esto llevaría a un incremento de la reputación por medio de la visualización externa de las políticas de la empresa.

Con todo esto, se llega a que la adecuación al Reglamento General de Protección de Datos podría dar la capacidad a una organización para optimizar las oportunidades en términos de reputación y confianza, así como para cumplir con los principios básicos de la responsabilidad social corporativa. De esta manera, se estaría afrontando el desafío que suponen los compromisos de la RSC, es decir, los que tiene una empresa con sus grupos de interés.

6. CASO PRÁCTICO: ANÁLISIS DEL COMPROMISO ÉTICO DE LAS EMPRESAS DE LA PROVINCIA DE LEÓN DESDE LA PERSPECTIVA DE LA PROTECCIÓN DE DATOS

6.1.INTRODUCCIÓN

Independientemente del país europeo del que se hable, cualquier empresa estará obligada a la correcta adecuación de la protección de datos tal y como dicta el Reglamento UE 2016/679. Además, este irá afín con la legislación correspondiente de cada país, que habrá de redactarse acorde a dicho reglamento, tal y como se ha especificado en apartados

anteriores. En España esta legislación es actualmente la LOPD 7/2021.

La ética empresarial y responsabilidad social corporativa podrían considerarse conceptos conocidos a nivel global. La finalidad del trabajo hasta este momento era asociar ambos conceptos, así como la aplicación de ambos en las empresas, de forma que dicha relación se utilizará en adelante para ser analizada dentro de una muestra de empresas.

Dada la complejidad de un estudio de grandes dimensiones, así como el riesgo de confusión del análisis de los resultados a gran escala, se procederá a analizar empresas pequeñas y medianas de la provincia de León.

6.2.DISEÑO DEL PROCESO DE INVESTIGACIÓN

En un principio, se ha recopilado información teórica acerca de la legislación vigente en materia de la protección de datos para tratar de explicar cómo funciona y cómo se aplica en las empresas.

Posteriormente, se ha relacionado la aplicación de la legislación en pequeñas y medianas empresas con la necesidad de abordarla en el marco de la responsabilidad social, dada la importancia de la ética empresarial en la actualidad, para que las organizaciones puedan adaptarse a las necesidades de los grupos de interés a nivel social, económico y medioambiental. Todo ello para poner en evidencia la importancia de la protección de datos desde una perspectiva más allá de las obligaciones legales de las empresas, llevado a cabo por medio de la parte teórica de los conceptos abordados[21] y sus contextos correspondientes, y habiendo expuesto su interrelación utilizando la literatura y legislación necesaria para poder analizarlos en casos reales posteriormente.

El siguiente paso fue elaborar una entrevista asociada a la información anteriormente recopilada, en función de los objetivos que se querían perseguir, los cuales tenían que ver con el análisis del cumplimiento de la legislación de protección de datos de pymes de la provincia de León desde una perspectiva ética. Antes de proceder a realizar la entrevista a los contactos facilitados por la empresa profesional de protección de datos, se estudió con detalle la última auditoría periódica o verificación del cumplimiento del Reglamento (UE) 2016/679 que esta realizó, mediante la cual se puede observar el grado de

[21] Protección de datos y responsabilidad social corporativa.

cumplimiento de la protección de datos de las empresas analizadas.

Las preguntas de las entrevistas fueron diseñadas en función de la persona a la que se entrevistase, por lo que se utilizaron dos modelos de plantilla para poder dirigirse al entrevistado dependiendo de su cargo y responsabilidad en la empresa: por un lado, un modelo iba dirigido a los propietarios de cada empresa (ver anexo 1), y, por otro lado, el otro modelo se confeccionó para dirigirse al responsable del tratamiento de datos cuando fuera una persona física diferente al propietario de la empresa (ver anexo 2). Estas entrevistas se realizaron vía telefónica, con una modalidad de respuesta abierta.

Así, uno de los objetivos de la entrevista era analizar los datos que fueran de relevancia para conocer la tendencia de los motivos por lo que pequeñas y medianas empresas de la provincia de León accedían a adecuarse al Reglamento General de Protección de Datos, y plantearles la perspectiva ética de esta actuación.

Con la investigación, se pretendía llegar a la finalidad de saber si dando a conocer la relación entre la protección de datos y la ética empresarial a las empresas que no fueran conscientes de ello, se podría incrementar el compromiso ético de las mismas con la protección de datos.

De esta forma, se podría llegar a una conclusión que permitiera saber si resultaría interesante plantear una estrategia de acceso por esta vía a otras empresas. Es decir, una nueva forma de plantear a las empresas la protección de datos con el fin de concienciarlas de la importancia que tiene en la actualidad, exponiéndoles la relación entre la protección de datos y la RSC, intentando mostrar que la protección de datos, aparte de ser una obligación, podría llegar a ser considerada una estrategia empresarial.

Para establecer la muestra, se utilizaron los contactos que facilitó una empresa dedicada a la protección de datos, que ha permitido utilizar la parte de su clientela que cumple las condiciones previstas en el estudio[22], con los permisos correspondientes previamente establecidos, así como con la condición de que se mantuviera el anonimato de las empresas seleccionadas para el estudio.

Del total de clientes de los que dispone la empresa de protección de datos, se determinó que, siguiendo las pautas establecidas, 212 empresas eran susceptibles de ser encuestadas.

[22] Condiciones para el estudio: pymes que desarrollen su actividad o tengan su sede en la provincia de León, evitando autónomos sin trabajadores a su cargo.

De todas ellas, se pudo establecer contacto con 194, y accedieron a ser entrevistadas 127, de las que solamente se ha podido utilizar la información recopilada de 111, por la falta de responsabilidad y capacidad de decisión del entrevistado para llegar a las conclusiones necesarias[23] para el estudio, como más adelante se explicará.

Además, se intentó contactar con 43 empresas que no figuraban como clientes de la empresa profesional de protección de datos, careciendo de éxito, ya que solo accedieron a hablar 21 de ellas y solamente 3 quisieron contestar a la entrevista, debido a la desconfianza generada a la hora de dar información acerca del funcionamiento de su empresa a un desconocido.

Por lo tanto, se ha realizado un total de 130 entrevistas a pymes de la provincia de León, de las cuales han aportado datos útiles para el análisis 114, el 100% de ellas tenía empleados a su cargo ya que los autónomos sin empleados a su cargo fueron descartados desde el primer momento.

La entrevista se estructuró en lo que se podría considerar como dos bloques. En un primer bloque, se buscó conocer cuáles son los motivos de adecuación de los entrevistados al Reglamento, así como sus preocupaciones en relación a la implementación de la política de protección de datos dentro de su empresa.

Posteriormente, en un segundo bloque, se les planteó la protección de datos desde la perspectiva ética que supone una correcta adecuación al Reglamento General de Protección de Datos, relacionándola con la responsabilidad social corporativa, con el fin de analizar si se podía observar un cambio de actitud o de consideración respecto de la importancia de cumplir con la protección de datos planteándolo de una forma completamente nueva.

6.3.ESTUDIO DEL GRADO DE CUMPLIMIENTO DE LA POLÍTICA DE PROTECCIÓN DE DATOS DE LAS EMPRESAS ENTREVISTADAS

Antes de proceder a realizar las entrevistas, se llevó a cabo un estudio de las últimas evaluaciones de impacto realizadas a las pymes seleccionadas, llevadas a cabo periódicamente por los delegados de la empresa profesional de protección de datos.

[23] Las entrevistas con el responsable del tratamiento diferente al propietario de la empresa no han dado resultados relevantes para sacar las conclusiones necesarias.

En estas evaluaciones de impacto figuraban las conclusiones alcanzadas por los delegados tras visitar a las empresas, recoger la información necesaria, y hacer un estudio de los riesgos a los que estaban sometiéndose, con el fin de prevenir una brecha de seguridad o brecha de datos personales. Además, tras realizar este análisis de riesgos en la evaluación de impacto, el delegado elabora un informe de verificación de cumplimiento, tal y como se expone en la teoría, para que la empresa disponga del documento pertinente que le permita demostrar lo que está haciendo bien y las medidas que ha de tomar con el fin de evitar problemas derivados de la mala o insuficiente aplicación del Reglamento General de Protección de Datos en la empresa.

Mediante el estudio de los informes llevados a cabo por el delegado, se observó que el 90.35% de las empresas estudiadas compartía el mismo patrón de riesgos o amenazas de seguridad establecidos por la Agencia Española de Protección de Datos, que se podría resumir en dos:

- Pérdidas económicas y reputacionales derivadas por incumplimiento de legislación sectorial de protección de datos. Estas se asocian a las legislaciones o protocolos en función de la actividad o sector al que pertenezca la empresa objeto de estudio. La causa será definida en función del sector empresarial, pero la consecuencia común por el que se da este riesgo es la falta de medidas de seguridad en el ámbito de la protección de datos personales, determinado por las diferentes características de los hábitos diarios del personal de la empresa. (Por ejemplo: cesión de datos entre el personal de la empresa, o falta de protocolos específicos para cada una de las etapas del ciclo de vida de los datos: captación, uso o tratamiento, cesión, eliminación…).

- Accesos no autorizados a datos personales. Es habitual que en las empresas se archiven datos personales, ya sea en formato físico o papel, de forma susceptible de ser accesible a cualquier persona ajena a la entidad o a su tratamiento. El riesgo de esto es que cualquier persona que no debería de tener acceso a esos datos lo tenga, ya sea tanto personal interno de la empresa, como personas ajenas a la entidad. Un ejemplo, son ficheros en formato papel colocados en estanterías sin estar bajo llave, pudiendo ser vistos por cualquier persona, o un aparato electrónico sin medidas de seguridad para su acceso (contraseñas, reconocimientos faciales…).

Las recomendaciones que hace la Agencia Española de Protección de Datos para las soluciones de estos riesgos, especificados en la Guía de gestión del riesgo y evaluación de impacto (2021), son las siguientes:

- ✓ Para evitar las pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales, se debe formar adecuadamente al personal del personal sobre protección de datos dentro del sector específico del que se trate, y favorecer una comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización.
- ✓ Para evitar los accesos no autorizados a datos personales, se han de establecer mecanismos y procedimientos de concienciación sobre la obligación de mantener en secreto los datos personales, así como valorar la posibilidad de imponer sanciones disciplinarias para quienes incumplan estas obligaciones. Además, se han de establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales.

A pesar de ser comunes estas amenazas y soluciones, se ha de establecer que la gravedad de estos problemas es mayor en las empresas que trabajan con datos especialmente protegidos, que, a pesar de actuar con una mayor diligencia, son más susceptibles de presentar una brecha de seguridad o brecha de datos personales.

6.4.ANÁLISIS DE RESPUESTAS

Las respuestas se han categorizado de forma que, aunque la posibilidad de las respuestas era abierta, se ha podido analizar la tendencia de la mayoría de estas de 3 formas: respuestas afirmativas, dudosas (creo que sí, creo que no, no lo sé, no sabría contestar…) y negativas, con el fin de facilitar el análisis de estas estableciendo este patrón. A continuación, se muestra un resumen de la modalidad de las respuestas de las entrevistas realizadas al propietario de la empresa, con el fin de justificar las conclusiones alcanzadas:

Pregunta 1: ¿Cómo se enteró usted de que debía adecuar su empresa al Reglamento General de Protección de Datos?

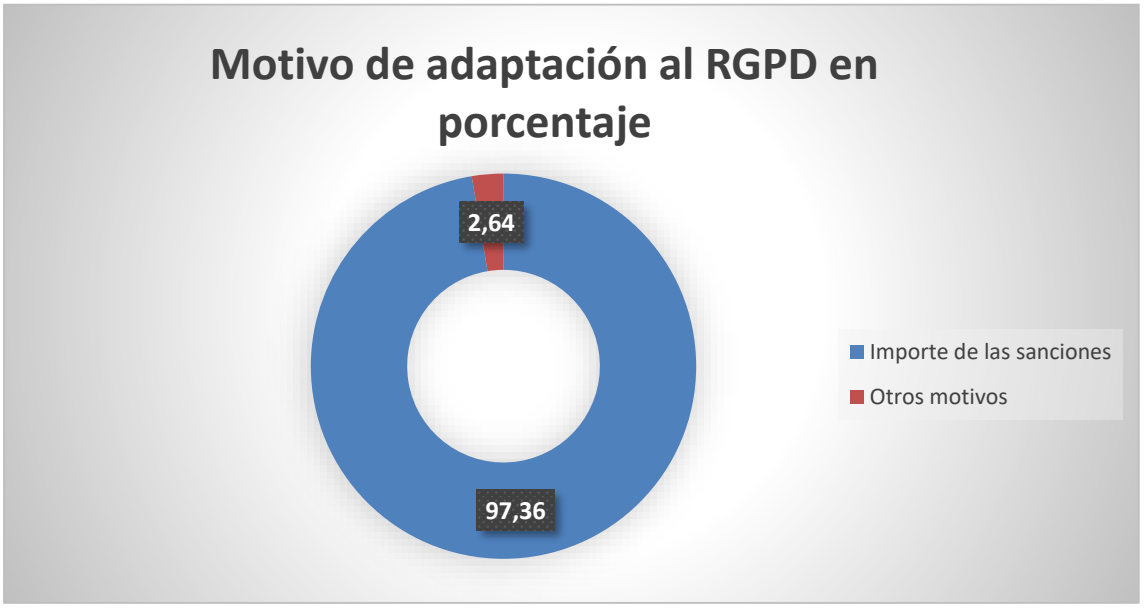
El 88.5% de las personas encuestadas respondían que se tuvo conocimiento de esta

obligación por la gran difusión que tuvo en los medios de comunicación, y el resto comentaron que se enteraron por medio de las asociaciones empresariales, así como por la advertencia de empresas de servicios del tipo gestorías y asesorías.

Pregunta 2: ¿Por qué decidió adecuar su empresa al RGPD?

A esta pregunta 111 de 114 empresas, es decir, el 97.36%, respondieron que el motivo era por miedo al importe tan elevado que se había advertido podrían tener las sanciones. Entre los demás motivos mencionados no se menciona la sanción, pero para indicar el motivo sí usan la palabra "obligación", y solamente en un caso se afirma que se quería actuar de forma responsable (Gráfico 6.1.).

Gráfico 6.1.: Motivo de adaptación al RGPD según los entrevistados



Fuente: Elaboración propia

Pregunta 3: ¿Conoce sus obligaciones como responsable del tratamiento de datos personales de su empresa?

Se observa, por las respuestas, que todos tienen nociones generales de la materia. Y todos afirman que cuando tienen dudas o problemas acuden sin dudarlo a la empresa que se encarga de su adecuación.

Pregunta 4: ¿Conoce los riesgos que conlleva no adecuar su empresa al Reglamento

General de Protección de Datos correctamente?

El 93.85% (107 de 114) de las empresas considera el riesgo como la posibilidad de que la Agencia Española de Protección de Datos les imponga la correspondiente sanción por algún incumplimiento. El otro 6.15% restante da a entender que sabe que hay más riesgos, pero se observa que lo que realmente les preocupa es de la misma forma que los anteriores, el importe de las sanciones.

Además, el 78,07% de las empresas afirman que en un principio realizó el tratamiento de protección de datos como curso de formación o pensando que simplemente se trataba de añadir pies de páginas a facturas y correos electrónicos, y que posteriormente ha tenido que realizar una nueva adecuación completa contratando una empresa especializada en la adecuación de empresas al Reglamento General de Protección de Datos, debido a la creciente preocupación por hacerlo bien a causa del miedo a la elevada cantidad que habría que pagar de sanción.

Pregunta 5: En caso de ser consciente de un incumplimiento de su empresa en materia de protección de datos personales, ¿cuál sería su mayor preocupación?

El importe de la sanción económica ha sido la única respuesta. Llama la atención que el 100% de los encuestados ha respondido de un modo taxativo lo mismo.

Pregunta 6: Si tuviera conocimiento de que se está produciendo un incumplimiento de la legislación en materia de protección de datos en su empresa, y únicamente este se conociera a nivel interno, ¿haría algo al respecto o no le sería de gran preocupación?

A partir de las respuestas obtenidas de esta pregunta se han podido observar 3 patrones de comportamiento ante la legislación. Así se ha dividido a las empresas en 3 grupos en función de lo siguiente:

1. Las empresas que consideraron en su momento (cuando supieron que tendrían que adecuarse al Reglamento) que era suficiente con contratar los servicios, es decir, con pagar a las empresas profesionales en materia de protección de datos, y a partir de ahí no hacer nada más, ni llevar a cabo ninguna actuación de las que se les exigía en su día a día. Se limitaron a poner el pie de página que les facilitaron

donde creyeron conveniente, y nada más.

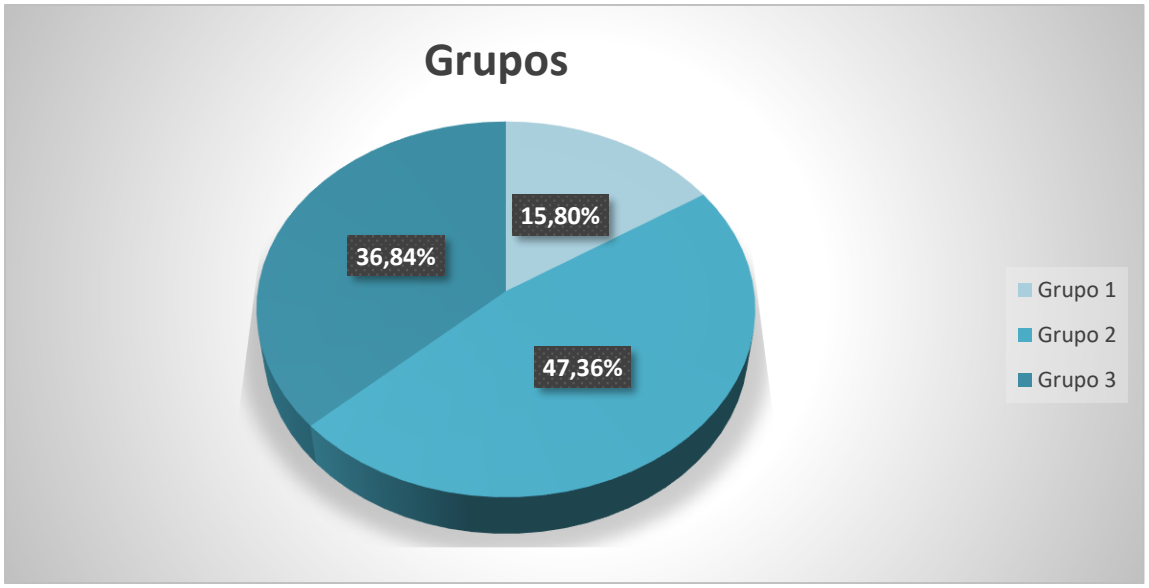
2. Las empresas que intentan adecuar su actividad a la protección de datos de la manera más laxa posible, tomando las medidas básicas (firma de documentos básicos con otras personas), porque consideran que llevar a cabo un tratamiento correcto requiere un esfuerzo desproporcionado en relación con el riesgo que corren. Es decir, ninguna de las medidas, como proteger la documentación bajo llave, determinación de encargados del tratamiento, etc. consideraban que eran de importancia suficiente como para dedicarle mayor preocupación y tiempo.

3. Las empresas que cumplen la legislación y realizan un correcto tratamiento de datos personales, siguen todas las orientaciones y consultan las dudas que les surgen con los profesionales que han contratado, mostrando preocupación por hacer las cosas bien.

En resumen, las respuestas del grupo 1 son claramente negativas, no les preocupa, no consideran importante la adecuación si nadie se entera de los problemas. El grupo 2preguntaría al delegado lo que estos fallos le supondrían, y en función de la respuesta del profesional valoraría si tomar alguna medida dependiendo del nivel de trabajo y/o coste que les pudiera suponer. El grupo 3 afirmaba que con ayuda del delegado intentaría buscar una solución al problema.

La mayor parte de las respuestas se centra entre los grupos 2 y 3 , con un total de 96 empresas de 114, entre las que se han categorizado en ambos grupos. Concretamente, el 84,2% del total pertenece a los grupos 2 y 3, del cual un 47,36% pertenece al 2 y un 36,82% al grupo 3, por lo tanto, el grupo 1 solamente queda con un 15,8% del total. Estas proporciones se podrán observar con mayor claridad en el gráfico 6.2.:

Gráfico 6.2.Categorización por grupos de las respuestas obtenidas.



Fuente: Elaboración propia

Pregunta 7: Respecto a la pregunta anterior, ¿consideraría usted que se está llevando a cabo un comportamiento éticamente responsable en caso de no tomar medidas?

Casi la totalidad de los entrevistados, un 95,6%, afirmó que éticamente su actuación es responsable, independientemente de lo que hagan con la protección de datos, del resto no se puede obtener una respuesta concreta, pero sí se pueden categorizar como dudosas, ya que todas contenían las palabras "no sé".

Pregunta 8: Si no hubiera una legislación que obligara a cumplir la normativa en materia de protección de datos y se tratase únicamente de un protocolo de suscripción voluntaria, ¿lo haría?

La tendencia de respuestas a esta empresa es claramente negativa, solamente una de las personas entrevistadas afirmó que lo haría de todas formas. Esta era una respuesta previsible en todo momento desde que se comenzaron a obtener las respuestas anteriores, especialmente después de las respuestas de la pregunta número 2, ya que la misma persona que afirmó que había adaptado su empresa al RGPD "por tener un comportamiento responsable" fue la misma que contestó a esta pregunta de forma positiva.

Pregunta 9: ¿Se ha planteado usted alguna vez la existencia de una relación entre la protección de datos y ética empresarial, dado el perjuicio que se puede causar a las personas asociadas a la empresa por una mala praxis en el tratamiento de sus datos personales?

La respuesta fue claramente negativa. En el 96,49% de las respuestas de las empresas encuestadas se mencionó que ni siquiera se habían planteado esta cuestión, solamente una de las empresas, que representa el 0,87% del total, respondió de forma positiva, y el resto de respuestas, que supone un 2,63% podrían resumirse en lo siguiente:

- Dos de ellas no ve clara la relación entre ambos conceptos.
- Otra dice que no considera que la gravedad del perjuicio que pueda causar a alguien por medio de una mala adecuación de su empresa a la protección de datos sea de tal importancia como para tachar el comportamiento de una empresa ético o no ético.

Sin embargo, tal y como se expone más adelante, una vez que el entrevistador explica la casuística y las consecuencias de una mala praxis en el tratamiento de los datos, el entrevistado tiende a modificar la visión del comportamiento ético que se encuentra detrás de una adecuada protección de datos en la empresa, aceptando que sí existe una parte ética dentro del comportamiento que se lleve a cabo en relación a la protección de datos.

Pregunta 10: ¿Conoce el término RSC? ¿Y su repercusión en el ámbito de la competitividad empresarial?

Todos afirman conocer el concepto, pero lo consideran como un hecho ajeno a ellos y a su actividad, aplicable en grandes empresas u organizaciones de mayor entidad.

Una vez llegados a este punto, se expone brevemente la importancia de la responsabilidad social corporativa dentro de todo tipo de organización, y los efectos positivos que podrían tener en cualquier tipo de empresa. Para ello, no se utilizó un patrón de exposición específico, sino que, en términos generales, fueron utilizados los conocimientos adquiridos en la elaboración de la teoría del trabajo, transmitiendo con claridad a los entrevistados la importancia de la responsabilidad social corporativa como estrategia dentro de cualquier tipo de empresa, independientemente de su tamaño, así como lo que significa que una empresa lleve a cabo un comportamiento ético para la generación de

confianza de grupos de interés (tras definir quiénes son estos) así como para un incremento de la reputación de la empresa.

Tras esta explicación se pasó a caracterizar la protección de datos, la cual todos conocen, como una estrategia de responsabilidad social corporativa, defendiendo el principio de cumplimiento de la legislación vigente en cada territorio de la RSC, así como la influencia de la protección de datos en la generación confianza e incremento de la reputación de una empresa. Cuando se observaba aceptación y entendimiento de esta explicación, se procedía a continuar con la entrevista.

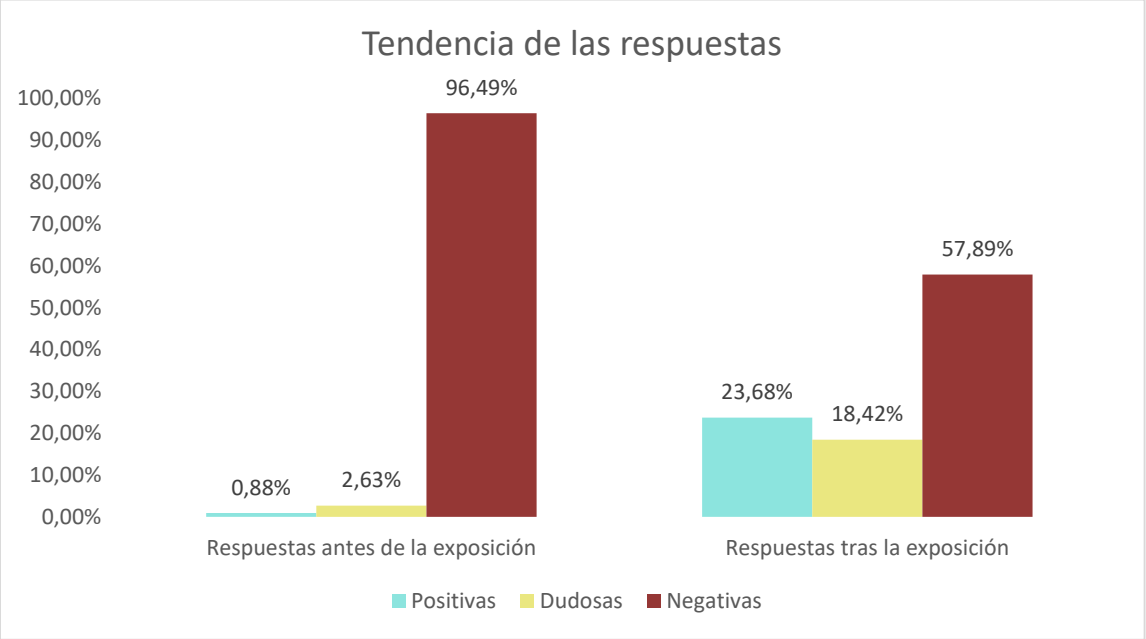
Pregunta 11: ¿Incrementaría su compromiso en el tratamiento de los datos personales si supiera que se podría tratar de una estrategia de RSC que supusiera mejoras en la competitividad de su empresa?

De las respuestas a esta última pregunta, fueron categorizadas como negativas el 57,89/%, como dudosas (del tipo "puede que sí" "a lo mejor sí"," no sabría decirte") el 18,42%, y como positivas el 23,68%.

La tendencia general de opinión en las respuestas a esta pregunta, comparándola con la pregunta número 9 sobre si las empresas encuestadas se han planteado alguna vez la existencia de una relación entre la protección de datos y ética empresarial, dado el perjuicio que se puede causar a las personas asociadas a la empresa por una mala praxis en el tratamiento de sus datos personales, cambia tras haberles planteado otra perspectiva de la protección de datos y su aplicación. Este patrón de opinión pasó de ser totalmente negativo, al no encontrar esta relación entre la protección de datos y el efecto negativo que ello puede causar en las personas, a incrementar hasta casi la mitad los resultados dudosos y positivos respecto a la posibilidad de comprometerse con la protección de datos para mejorar la competitividad de la empresa.

Mediante el gráfico 6.3. se procede a representar la variación de la tendencia de las respuestas antes y después de exponer al entrevistado la importancia de la responsabilidad social corporativa dentro de la empresa y su relación con la protección de datos pero considerando las posibilidades de la RSC para mejorar la competitividad de la empresa, ya que actuar éticamente supone mejorar la confianza con los grupos de interés de la empresa y, con ello, mejorar las ventajas competitivas para la empresa, es decir, la diferencia entre las respuestas a la pregunta 9 y la 11.

Gráfico 6.3: Comparativa de las respuestas en porcentajes a las preguntas 9 (izquierda) y 11 (derecha).



Fuente: Elaboración propia

De las respuestas obtenidas en la segunda modalidad de entrevista a los responsables del tratamiento de datos cuando se trata de personas diferentes al propietario de la empresa (Ver anexo 2), no se ha obtenido el resultado esperado, ya que la mayoría de estas empresas ha respondido de forma que se ha categorizado como dudosa al no aportar respuestas concluyentes. Los entrevistados, en este caso, tal vez no querían verse comprometidos con las respuestas al no ser los propietarios de las empresas.

Como consecuencia de ello, se han desechado las respuestas obtenidas de la segunda modalidad de encuesta por la falta de concreción y el reducido número de respuestas, para que no interfirieran en las conclusiones globales.

7. CONCLUSIONES

El presente trabajo perseguía estudiar la relación existente entre la ética empresarial y la protección de datos por medio de la responsabilidad social corporativa, con la finalidad de estudiar este compromiso en pequeñas y medianas empresas de la provincia de León.

Una vez llevada a cabo la revisión de literatura, se procedió a ajustar las pautas a seguir en las entrevistas, con el fin de analizar lo previamente establecido. Tras poder acceder a 114 empresas que cumplían las condiciones impuestas, se pudo observar que el mayor compromiso que tienen la mayoría de las empresas en la provincia de León es únicamente debido a la obligación legislativa que lo ampara.

Gran parte de las empresas entrevistadas es consciente de que no realizar un correcto adecuamiento al Reglamento General de Protección de Datos puede traer graves consecuencias, tanto para la empresa como para las personas que tienen relación con esta, y, aun así, la mayor preocupación de estas empresas son las elevadas sanciones que puede imponerles la Agencia Española de Protección de Datos.

Una vez llegados a ese punto, se procede a plantearles la protección de datos desde otro punto de vista, desde la perspectiva de la ética empresarial. Desde un primer momento nadie se planteaba esta relación, a pesar de conocer la influencia que tiene la protección de datos en tantos aspectos éticos.

Cuando se hace mención del término de responsabilidad social corporativa todos afirman conocerlo, pero se muestra quizá aquí la raíz del problema en que nadie se haya planteado esa perspectiva de la protección de datos, y es que, está generalizada la visión entre las empresas estudiadas de que la responsabilidad social corporativa es un concepto que no les incumbe, que no les afecta ni tienen la necesidad de adoptarlo. Este problema quizá sea más profundo que el del desconocimiento de la protección de datos como estrategia competitiva, ya que se observa una desinformación acerca de los efectos de la responsabilidad social corporativa como estrategia en las empresas y quiénes se pueden beneficiar de sus efectos. Esta conclusión se alcanza tras observar que, según los resultados de la entrevista, las pequeñas y medianas empresas de la provincia que accedieron a la entrevista, como norma general, parecen desconocer la influencia que la RSC puede tener sobre su actividad empresarial, por lo que podrían estar perdiendo oportunidades de negocio, más allá de considerar la protección de datos desde una perspectiva puramente ética.

A pesar de que las empresas consideran a la responsabilidad social corporativa como algo que no necesitan porque consideran que tendría un elevado coste adoptar medidas para esa finalidad, o porque no son conscientes de los efectos que tendría implementarla en su empresa, pasaron de ser 4 a ser 48 las empresas entrevistadas que cambiaron su forma de percibir la protección de datos en la última pregunta, mostrándose así más accesibles a comprometerse con la protección de datos.

Además, se dio el caso de que de las tres empresas que se entrevistaron, y no eran actuales clientes de la empresa que ayudó en este estudio, se captó uno de ellos una vez terminada la entrevista, mostrándose interesado en la implicación de la protección de datos en la responsabilidad social corporativa.

Dicho esto, merecería la pena reflexionar acerca de la posibilidad de utilizar este método de acceso a los clientes a la hora de mostrarles las influencias de la protección de datos más allá del mero cumplimiento con la ley. Quizá esto podría suponer un incremento de éxito en la concienciación de las empresas con el cumplimiento de la legislación vigente en materia de protección de datos.

De cualquier manera, del estudio llevado a cabo, se ha obtenido el resultado de que el compromiso ético de las empresas de la provincia de León con la protección de datos es, quizá por su desconocimiento, prácticamente inexistente.

REFERENCIAS

Acosta F. (2013). La ética empresarial en el desarrollo profesional. Universidad militar nueva granada. División de posgrados – Facultad de Economía. Páginas 4 – 30. Recuperado de https://repository.unimilitar.edu.co/handle/10654/10681

Agencia Española de Protección de Datos (2021). Gestión del riesgo y evaluación de impacto en tratamiento de datos personales. Páginas 73-158. Recuperado de https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

Agencia Española de Protección de Datos (2022). Derechos y deberes. Cumple tus deberes. Cumplimiento de las obligaciones. Recuperado de https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes

Agencia Española de Protección de Datos (2022). Medidas de cumplimiento. Notificación de brechas de datos personales a la Autoridad de Control. Recuperado de https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-datos-personales-notificacion

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 esos datos. Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678

Aragón, J. (2016). Notas sobre ¿Una nueva Revolución Industrial? Economía digital y trabajo. Gaceta sindical. Vol 27, páginas 13-17. Recuperado de https://www.ccoo.es/152806c7bbdfac28c2bde95f40e00c0d000001.pdf

Martin H., Calderon J. & Vargas J., (2018) *Big data*, el futuro de las predicciones certeras. Avenir 2018, 2, 2. ISSN 2590-8758. Páginas 10 – 14. Recuperado de https://fundacionavenir.net/revista/index.php/avenir/article/view/33

Carta de los derechos fundamentales de la Unión Europea. (2016). Recuperado de https://www.boe.es/doue/2016/202/Z00389-00405.pdf

Embid, J., & Del Val, P. (2016). La responsabilidad social corporativa y el Derecho de sociedades de capital: entre la regulación legislativa y el soft law. Páginas 21-46.

Fernández, R. (2009). Responsabilidad Social Corporativa. Una nueva cultura empresarial. Páginas 9-116.

Gil E., (2015). Big data, privacidad y protección de datos. XIX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos. Páginas 44- 82. Recuperado de https://www.aepd.es/sites/default/files/2019-10/big-data.pdf

Guevara, M. (2018). El impacto del Big data en la protección de datos personales. Análisis de los avances normativos en materia de protección de datos. Trabajo Fin de Grado. Universitat Jaume I. Páginas 8-30. Recuperado de http://repositori.uji.es/xmlui/bitstream/handle/10234/175806/TFG_2018_Guevara_Sanmateo_Mar.pdf?sequence=1&isAllowed=y

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Jefatura del Estado <<BOE>> núm. 294, de 06 de diciembre de 2018. Referencia: BOE –A-2018-16673. Recuperado de https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

Méndez, T. (2005). Ética y Responsabilidad Social Corporativa. Ética y economía. ICE. Nº 823. Páginas 141-149. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=1292668

Miotto, G. (2010). RSC 2.0, el barómetro de la confianza. Responsabilidad Social Corporativa. Capital Humano, nº44. Páginas 42-45. Recuperado de https://factorhuma.org/attachments_secure/article/205/c313_RSC2.0.pdf

Monleón-getino, A.(2015). El impacto del Big-data en la Sociedad de la Información. Significado y utilidad. Historia y Comunicación Social. Vol 20, número 2, páginas 427-445. Recuperado de https://revistas.ucm.es/index.php/HICS/article/view/51392/47672

Navarro F. (2012). Responsabilidad social corporativa: teoría y práctica. ESIC. Bussiness Marketing School. Páginas 10-115. Recuperado de https://books.google.es/books?hl=es&lr=&id=LyqG6yzMNnsC&oi=fnd&pg=PA103&dq=fernando+navarro+garcia+responsabilidad+social+corporativa+teoria+y+practica&ots=kH5W6xeEgm&sig=qyZ5Veze9iIApAfz8KMakeMs36k#v=onepage&q&f=false

Real Academia Española. (2021). Diccionario de la lengua española. Recuperado de https://dle.rae.es/globalizaci%C3%B3n

Real Academia Española (2021). Diccionario de la lengua española. Recuperado de https://dle.rae.es/pyme

R. de George (1982). Business Ethics. New Jersey, Prentice-Hall, Englewood Cliffs. 4ª Ed. Página 33.

R. Freeman (1984). Strategic Management. A Stakeholder Approach. Páginas 24-31.

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). Recuperado de https://www.boe.es/doue/2016/119/L00001-00088.pdf

Rivero, P. (2006). La Responsabilidad Social Corporativa en las pymes. Páginas 77-87. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=2195027

Saco, J., (2019). Buen gobierno corporativo y protección de datos de carácter personal: El principio de accountability en el ámbito de las sociedades mercantiles. Máster en derecho de la ciberseguridad y el entorno digital. Universidad de León. Páginas 10-23. Recuperado de https://buleria.unileon.es/bitstream/handle/10612/12562/Saco%20Vega%2c%20Jorge.pdf?sequence=1&isAllowed=y

ANEXOS

ANEXO 1: ENTREVISTA REALIZADA AL PROPIETARIO DE LA EMPRESA.

Nombre de la empresa:

Nº empleados:

1. ¿Cómo se enteró usted de que debía adecuar su empresa al Reglamento General de Protección de Datos?
2. ¿Por qué decidió adecuar su empresa al Reglamento?
3. ¿Conoce sus obligaciones como responsable del tratamiento de datos personales de su empresa?
4. ¿Conoce los riesgos que conlleva no adecuar su empresa al Reglamento General de Protección de Datos correctamente?
5. En caso de ser consciente de un incumplimiento de su empresa del Reglamento General de Protección de Datos, ¿cuál sería su mayor preocupación?
6. Si tuviera conocimiento de que se está produciendo un incumplimiento de la legislación en materia de protección de datos en su empresa, y este se conociera únicamente a nivel interno de la empresa, ¿haría algo al respecto o no sería de preocupación?
7. Respecto a la pregunta anterior, ¿consideraría usted que se está llevando a cabo un comportamiento éticamente responsable en caso de no tomar medidas?
8. Si no hubiera una legislación que obligara a cumplir la normativa en materia de protección de datos y se tratase únicamente de un protocolo de suscripción voluntaria, ¿lo haría?
9. ¿Se ha planteado usted alguna vez la existencia de una relación entre protección de datos y ética empresarial, por el perjuicio que se puede causar a las personas asociadas a la empresa por una mala praxis en el tratamiento de datos personales?
10. ¿Conoce el término Responsabilidad Social Corporativa? ¿Y su repercusión en el ámbito de la competitividad empresarial?
11. ¿Incrementaría su compromiso en el tratamiento de los datos personales, si supiera que se podría tratar de una estrategia de Responsabilidad Social

Corporativa que supusiera mejoras en la competitividad de su empresa?

ANEXO 2: ENTREVISTA AL RESPONSABLE DEL TRATAMIENTO CUANDO ES UNA PERSONA FÍSICA DIFERENTE AL PROPIETARIO DE LA EMPRESA.

Nombre de la empresa:

Nº empleados:

1. ¿Cómo se enteró usted de que debían adecuar la empresa en la que trabaja al Reglamento General de Protección de Datos?
2. ¿Por qué cree que en su empresa decidieron adecuarse al Reglamento?
3. ¿Conoce sus obligaciones como responsable del tratamiento de datos personales de la empresa?
4. ¿Conoce los riesgos que conlleva no adecuar una empresa al Reglamento General de Protección de Datos correctamente?
5. En caso de ser consciente de un incumplimiento de la empresa en la que trabaja del Reglamento General de Protección de Datos ¿cuál sería su mayor preocupación como responsable del tratamiento?
6. Si tuviera conocimiento de que se está produciendo un incumplimiento de la legislación en materia de protección de datos dentro de la empresa, y únicamente este se conociera a nivel interno, ¿cree usted que se haría algo al respecto o no sería de gran preocupación?
7. Respecto a la pregunta anterior, ¿consideraría usted que se está llevando a cabo un comportamiento éticamente responsable si no se hiciera nada al respecto?
8. Si no hubiera una legislación que obligara a cumplir la normativa en materia de protección de datos y se tratase únicamente de un protocolo de suscripción voluntaria, ¿cree usted que su empresa lo haría?
9. ¿Se ha planteado usted alguna vez la existencia de una relación entre protección de datos y ética empresarial, por el perjuicio que se puede causar a las personas asociadas a la empresa por una mala praxis en el tratamiento de datos personales?
10. ¿Conoce el término Responsabilidad Social Corporativa? ¿Y su repercusión en el

ámbito de la competitividad empresarial?

11. ¿Cree usted que se incrementaría el compromiso en el tratamiento de los datos personales, si se supiera que se podría tratar de una estrategia de Responsabilidad Social Corporativa que supusiera mejoras en la competitividad de su empresa?