EL DERECHO DE LA PROTECCIÓN DE DATOS PERSONALES Y LOS MEDIOS DE COMUNICACIÓN CON SEDE SOCIAL EN SEVILLA: DEBERES Y DERECHOS EN PRENSA, RADIO Y TELEVISIÓN

Sevilla, 2 de julio de 2012.

El autor del Trabajo de Investigación,

Lic. Antonio J. Ordóñez Martínez.

Vº. Bº.
Sevilla, ____ de julio de 2012.
Los directores de la Tesis Doctoral.

Prof. Dr. José Manuel Gómez y Méndez.

Profª. Dra. Pastora Moreno Espinosa.

UNIVERSIDAD D SEVILLA

DEPARTAMENTO DE PERIODISMO II

EL DERECHO DE LA PROTECCIÓN DE DATOS PERSONALES Y LOS MEDIOS DE COMUNICACIÓN CON SEDE SOCIAL EN SEVILLA: DEBERES Y DERECHOS EN PRENSA, RADIO Y TELEVISIÓN

Tesis doctoral
realizada por el
Lic. Antonio J. Ordóñez Martínez,
con la dirección del
Prof. Dr. **JOSÉ MANUEL GÓMEZ Y MÉNDEZ**
y la Profª. Dra. **PASTORA MORERO ESPINOSA**

SEVILLA, julio de 2012.

0. ÍNDICE.

1. INTRODUCCIÓN.

1.1. Prenotandos e hipótesis investigadora sobre la Protección de Datos y los Medios.

Una de las grandes cuestiones del Derecho español sigue siendo conciliar derecho a la intimidad con libertad de expresión. Si hasta hace poco el problema ha estribado en delimitar, por la justicia, la frontera que separa la posibilidad de información sobre alguien y la intimidad privada de la persona, el objeto de nuestro estudio lo conforma un derecho que más allá de ceñirse a la esfera íntima, pasa a convertirse en un derecho de nueva generación: la defensa y protección del dato de carácter personal.

El dato de carácter personal es intransferible a todo ciudadano. Es un derecho fundamental reconocido en la Constitución Española que atribuye al titular del derecho la facultad de controlar sus datos y nadie tiene que resignarse a soportar que su información personal pueda circular contra su voluntad y ser tratada o almacenada por los múltiples canales de comunicación e información que proliferan en nuestros días.

Los Medios de Comunicación no pueden quedar exentos ni ajenos a esta realidad, y como agentes que manejan y tratan datos de carácter personal, están obligados a asegurar el derecho fundamental a la protección de los datos personales de que disponen.

Analizar el comportamiento de los periódicos, televisiones y emisoras de radio ante los datos personales de clientes y público en general puede hacerse colocando el punto de mira en su actividad editorial, la propiamente periodística de informar, o apuntando nuestra mirada analítica hacia su actuación como empresas que operan en el mercado del sector de la información, y que deben cumplir la legislación vigente en esta materia. Para lo primero, la ética profesional. Para lo segundo, hay que estar al cumplimiento de la actual legislación europea y española.

La sofisticación de la tecnología permite a la información circular más rápidamente por el mundo y los riesgos son cada vez mayores. Escribo estas líneas pocos meses después de que se haya conocido el mayor robo de

datos conocidos hasta ahora. Una organización se ha hecho con datos personales y de carácter empresarialde decenas de miles de ordenadores de particulares, entidades y organismos de varios grandes países del mundo. Un nuevo tipo de riesgos que no pueden obviar nuestros Medios de Comunicación.

La tecnología, sin embargo y pese a todo, también permite una mayor protección de los datos cuando es preciso, facilitando el control y la búsqueda de la información. Analizaremos la tarea que, en materia de seguridad, han de acometer los Medios de Comunicación a fin de tratar de aislar los datos personales que manejan y protegerlos de manera más rápida y eficaz que antes.

La sensibilidad de los Gobiernos hacia este derecho del ciudadano es tal, que en países como España se ha legislado contemplando las más fuertes sanciones económicas para las situaciones de infracción y violación de los derechos protegidos en este ámbito.

La importancia que tiene el estudio de le Protección de Datos Personales puede verse gráficamente para los menos especializados en Derecho al ver cómo incide en numerosas parcelas del ordenamiento jurídico: Libertad de expresión; derecho a la información; derecho al honor; derecho a la privacidad; derecho a la intimidad personal y familiar; libertad de cátedra; libertad religiosa; propiedad industrial; propiedad intelectual; derecho de petición; resoluciones judiciales o administrativas; leyes y reglamentos, etc.

1.2. Sobre metodología.

No existe ninguna duda sobre el valor del conocimiento científico para el progreso de la sociedad. En nuestros días, es fácil comprobar el importante lugar que ocupa la ciencia dentro del conjunto de todas las actividades sociales. Por ello, la ciencia es considerada como el fundamento más firme y seguro para el conocimiento, utilización y dominio del mundo en el que vivimos. Así para algunos autores[1] "*la característica más destacada de nuestro tiempo es la penetración de la ciencia en todas las actividades sociales*". Ello es debido a que el hombre

[1] SARABIA SÁNCHEZ, F. J. y otros: *Metodología para la investigación en marketing y dirección de empresas*. Pirámide, Madrid, 1999, pág. 22.

es capaz de reconocer mediante la razón la realidad en la que se encuentra o para convivir mejor con ella. Cuando hace uso de esta facultad que le es propia obtiene ideas o representaciones conceptuales del mundo en que vive y que son la base de su actuación y, por tanto, de su presencia social.

Algunos autores, como Sarabia Sánchez[2], afirman que "*el conocimiento científico posee una natural y radical significación humana*" El término "*sociedad científica*" ha surgido como consecuencia del aumento de la importancia que se ha concedido al conocimiento científico y a la interacción ciencia-sociedad. Con él se designa aquella sociedad que dota de un elevado rigor a las actividades sociales, en cuanto éstas parecen impregnarse de un mayor sentido científico y de un mayor uso de términos científicos, tanto en los medios de comunicación social como en el lenguaje de la calle.

El efecto producido por el reconocimiento social de conocimiento científico es la admisión del investigador como el auténtico motor del progreso en todos los sentidos, ya que es la persona que promueve simultáneamente el desarrollo de su propia ciencia y el del ámbito social en el que ésta se aplica. Para ello, la ciencia es conformada por una comunidad de individuos especialmente entrenados para ello que generan las teorías científicas, las decantan por medio de la crítica y asumen el papel de jueces evaluadores respecto a qué construcciones teóricas son aceptables. Por este motivo, es la ciencia todo lo que estos grupos de personas decidan por consenso que es ciencia. En este sentido, el único tribunal de apelación inapelable es el tiempo. Por lo tanto, la comunidad de científicos tiene que desarrollar una doble tarea: por un lado, debe proponer teorías científicas; y por otro, ha de asumir el papel de árbitro para juzgar sobre la aceptabilidad de las construcciones teóricas.

El importante auge que ha experimentado la ciencia en el siglo XX y su influencia en las diferentes áreas del saber humano y de la actividad social han generado una serie de reflexiones críticas realizadas desde distintas perspectivas: citamos, como ejemplos, las críticas de tipo económico[3], de tipo ecológico[4], de orden moral[5] y de tipo político[6].

[2] Ibídem, pág. 22.

[3] Se basa en el elevado coste de algunas investigaciones cuya función social resulta posteriormente muy escasa y, en algunos casos, negativa.

[4] Debido alas graves consecuencias que algunos experimentos científicos producen en el entorno natural.

También se ha mencionado la dependencia económica y tecnológica a la que el progreso, consecuencia de la investigación científica, somete a los países con un menor potencial investigador. Sierra Bravo[7] afirma que, en nuestros días, la ciencia ha concedido un poder inmenso al hombre. Para este autor, este poder es peligroso porque el hombre puede utilizarlo para bien o para mal.

Los tipos de conocimiento por el modo de acceso al objeto son fundamentalmente dos: el conocimiento vulgar o sentido común y el conocimiento científico. Y todo ello con independencia del llamado saber "*mágico*", de capital importancia en las sociedades primitivas y que se basa en las denominadas leyes de la semejanza y del contagio. Los dos -sentido común y conocimiento científico- responden a la misma necesidad humana (búsqueda de la verdad y explicación de los fenómenos) y pueden tener el mismo objeto y la misma naturaleza fundamental; por lo tanto, no son opuestos. Sierra Bravo[8] indica que el conocimiento, que está formando por el conjunto de ideas obtenidas que proporcionan al hombre información para que pueda actuar, no es único, sino que presenta distintas clases. Para Ramón y Cajal[9], las principales fuentes de conocimientos son: la observación, la experimentación y el razonamiento inductivo y deductivo.

López Yepes[10] considera que el conocimiento vulgar está representado por el conjunto de ideas y opiniones de un valor preferentemente individual que el ser humano emite u obtiene en las labores que realiza en su vida cotidiana basadas en el sentido común, en la

---

[5] Han sido suscitadas por los problemas éticos que plantean las nuevas ciencias como la genética o la biotecnología.

[6] Han indicado la función ideológica y de control social que determinadas teorías desempeñan.

[7] SIERRA BRAVO, R.: Tesis doctorales y trabajos de investigación científica. Metodología general de su elaboración y documentación. Paraninfo, Madrid, 1996, pág. 25.

[8] Ibídem, pág. 24.

[9] RAMÓN Y CAJAL, S.: *Reglas y consejos sobre investigación científica. Los tónicos de la voluntad.* Espasa Calpe, Madrid, 1991, pág. 23.

[10] LÓPEZ YEPES, J.*: La aventura de la investigación científica. Guía del investigador y del director de investigación*. Síntesis, Madrid, 1995.

experiencia o en el azar. Esta forma de conocimiento[11] se caracteriza por ser subjetiva, superficial, sensitiva, asistemática, acrítica, cualitativa y no metódica, lo que no quiere decir que sea inútil o prescindible o menos importante. Normalmente este tipo de conocimiento no va seguido de una explicación que indique por qué los hechos son de la manera en que se manifiestan.

Por el contrario, el conocimiento científico tiene su origen en la actitud admirativa del hombre hacia lo que le rodea y se llega a él por la vía de la "*etiología*", es decir por la búsqueda de las causas últimas de las cosas. Sierra Bravo[12] afirma que "*el conocimiento científico es, en su campo, el de la realidad observable, el que tiene la primacía por ser el más preciso, exacto, elaborado y cualificado*" Para este autor, el conocimiento científico es también el que proporciona una información más detallada, completa y eficaz para actuar en el mundo. Por ello, en opinión de Nagel[13], lo que origina la ciencia es el deseo del hombre de encontrar explicaciones sistemáticas y controlables por elementos de juicios prácticos así como el deseo de organizar y clasificar el conocimiento sobre la base de principios explicativos. Debido al carácter sistemático del conocimiento científico, este se utiliza para refinar del conocimiento vulgar al indicar las conexiones existentes entre las proposiciones relativas al sentido común.

El conocimiento científico tiene carácter colectivo puesto que se considera a la ciencia como una traducción acumulativa, en el sentido de que se transmiten los conocimientos de unos científicos a otros. Así, los conocimientos recogidos por sus predecesores los sigue el investigador y le serán de gran utilidad para llegar al objeto de su investigación. A diferencia del conocimiento vulgar, el pensamiento científico posee un mayor rigor lógico y una mayor capacidad para autorregular sus contenidos por medio de la discusión crítica.

El conocimiento científico, como indican algunos autores[14], tiene una clara vocación de permanencia basada en su objetividad, es profundo,

[11] También se le denomina "*conocimiento precientífico*".

[12] SIERRA BRAVO, R.: op. cit., pág. 24.

[13] NAGEL, E: *La estructura de la ciencia*. Paidós, Barcelona, 1989.

[14] SARABIA SÁNCHEZ, F. J. y otros: op. cit., pág. 25.

reflexivo, razonado, sistemático, crítico cualitativo y metódico. Pero los calificativos utilizados para distinguir ambos tipo de conocimientos han de ser interpretados cuidadosamente ya que la frontera entre las características[15] es a veces imprecisa.

Por las dificultades existentes para diferenciar el conocimiento vulgar de las conclusiones conseguidas mediante la actividad científica, se establece el método como el elemento distintivo. El método se sirve para su ejecución de unas reglas que, en todo caso, no son verdaderas invariablemente. De este modo, el método delimita el concepto de conocimiento científico porque es el elemento que más caracteriza la noción de ciencia. Ya apuntaba Descartes[16] que a la capacidad individual hay que añadirle un método adecuado para llegar al descubrimiento de la verdad. Para él lo importante no era tener un buen entendimiento, sino aplicarlo correctamente. Por ello, propone su método, basado en cuatro reglas. La primera establece que la evidencia racial es el único criterio de verdad. Como segunda regla propone el análisis. La tercera regla es la síntesis puesto que agrupar las ideas y ordenarlas es necesario tanto para la inducción como la deducción. Por último, la cuarta regla, que se deduce de la anterior, consiste en la enumeración y en la revisión sin omisiones. De este modo se conseguirá la intuición general de la ciencia y la evidencia intuitiva del conjunto.

Hay que aclarar que el uso del método científico no quiere decir que el investigador tenga que seguir unas reglas prescritas para realizar descubrimientos ni que tenga que utilizar un conjunto especial de técnicas independientemente del tema que se investigue. Ello es debido a que en la ciencia no hay reglas fijas o inamovibles opera el descubrimiento y para la invención.

1.3. Sobre investigación y método científico.

Las teorías científicas están esencialmente relacionadas entre sí. En este sentido, y para expresar esta idea gráficamente, algunos estudiosos[17]

[15] Por ejemplo, la frontera entre lo individual y lo colectivo, entre lo subjetivo y lo objetivo, etc.

[16] DESCARTES, R.: *Discurso del método*. Libsa, Madrid, 2001.

[17] SARABIA SÁNCHEZ, F. J. y otros: op. cit., pág. 37.

estiman que es posible visualizar la totalidad del corpus de la ciencia como una enorme red de teorías, siendo los nudos de esta red las teorías particulares y siendo sus cuerdas las relaciones.

Para Alcina Franch[18], la historia de cada una de las ciencias no es solamente una acumulación de descubrimientos de datos o de hechos, sino que es una cadena de teorías que han servido para explicar estos hechos. Para este autor, las teorías constituyen el contenido sustantivo de la ciencia y estima que lo que llega a ser "*acumulado*" en la situación actual de cada campo científico es una parte del pasado. Consecuencia de estas dos conclusiones, es la que extrae como tercera: que todas las teorías científicas podrían ser reemplazadas por otras que explicasen mejor los hechos; de este modo, aquello que en principio suponíamos que habría que "*transmitir*" es tan deleznable que, aunque no totalmente, en una buena parte podría ser sustituido por otro conjunto de nuevas teoría. Por ello, en opinión de este autor, la ciencia "*no es*", sino que "*está siendo*", es algo absolutamente fluido y casi inasible, de ahí que constantemente sea necesario indicar "*estados de la cuestión*" a todos los niveles.

Sarabia Sánchez[19] y otros autores estiman que el proceso de construcción de teorías facilita la consecución de objetivos importantes en cualquier tipo de ciencia. Estos autores, siguiendo a Bunge[20], afirman que permite:

1. La sistematización del conocimiento mediante el establecimiento de relaciones lógicas entre entidades antes inconexas.

2. La explicación de los hechos a través de relaciones que impliquen las proposiciones que expresan dichos hechos.

3. Aumentar el conocimiento al originar nuevas proposiciones.

4. Reforzar la contrastabilidad de las hipótesis al subordinarlas al control de las leyes del sistema.

---

[18] ALCINA FRANCH, J.: *Aprender a investigar. Métodos de trabajo para la redacción de tesis doctorales. Humanidades y Ciencias Sociales*. Compañía Literaria, Madrid, pág. 22.

[19] SARABIA SÁNCHEZ, F. J y otros: op. cit., pág. 37.

[20] BUNGE, M.: *La investigación*…, op. cit., pág. 37.

5. La orientación de la investigación, bien mediante el planteamiento o reformulación de problemas científicos fecundos, mediante la sugerencia de recopilación de nuevos datos que serían inimaginables sin el apoyo de la teoría o mediante la inspiración de nuevas líneas de investigación.

6. Facilitar un mapa de una parte de la realidad.

Aunque no todas las teorías consiguen alcanzar todos los objetivos expuestos anteriormente, por lo menos deben ser capaces de acercarse a los cuatro primero. Bunge[21] opina que, de este modo, podremos distinguir las teorías de las "*pseudoteorías*". Por lo tanto, un conjunto de conjeturas no puede considerarse una teoría científica a menos que constituye un sistema hipotético-deductivo propiamente dicho, si no suministra explicación y previsión y si no es contrastable; esto es lo menos que ha de exigirse a una teoría científica.

Hemos indicado que la teoría constituye el término de la labor científica. Pero las teorías son algo más. Se puede decir que son su origen, su marco y su fin. Son su origen porque son fuente de nuevos problemas y conducen a la formulación de nuevas hipótesis. Son su marco porque proporcionan el sistema conceptual que se aplica a la observación, clasificación de los datos de la realidad y su fin, porque la investigación debe desembocar en teorías cada vez más perfectas. Por todo ello, algunos autores[22] afirman que en la ciencia contemporánea, la actividad científica más importante, más profunda y más fecunda son las teorías. Así pues, existe una interacción continua entre la realidad y las teorías; con base en los hechos, ayudándose de todo un instrumental de conceptos, modelos e hipótesis, se establecen, complementan y reforman las leyes y teorías; con base en las teorías se formulas nuevos problemas o hipótesis.

Etimológicamente, un método es un camino hacia u objetivo. Con anterioridad hemos señalado que el método delimita la noción del conocimiento científico puesto que es elemento que más caracteriza a la ciencia. Pues bien, Sarabia Sánchez[23] afirma que la unidad de la ciencia

[21] Ibídem, pág. 37.

[22] SARABIA SÁNCHEZ, F. J. y otros: op. cit., pág. 38.

[23] Ibídem, pág. 38.

estriba en la unidad de su planteamiento y no en una teoría única ni en un lenguaje unificado. Por lo tanto, la universalidad del método científico es admitida en un sentido amplio ya que la ciencia se enfrenta en todos sus ámbitos con un solo método y un solo objetivo. Todas las ciencias comparten el método científico. Aunque exista una variedad de modalidades metodológicas específicas que viene exigida por la diversidad de problemas concretos de investigación. Pero la ejecución concreta y, en particular, las operaciones estratégicas, dependen del tema de estudio y del estado del conocimiento respecto a dicho tema. Así, cada rama de la ciencia se caracteriza por un conjunto abierto de problemas que se intentan resolver mediante una serie de tácticas y técnicas específicas.

El profesor Sierra Bravo[24] estima que el método utilizado en las ciencias es, en primer lugar, un método y como tal una forma de realizar una actividad; el camino o proceso que la actividad en cuestión ha de seguir para alcanzar su objetivo. En segundo lugar se trata de un método específico y determinado, que recibe el nombre de "*científico*", ya que su origen, aplicación y desarrollo, ante todo, en las ciencias consideradas típicas (las físicas y naturales). Dentro de los distintos tipos de métodos es un método de investigación en cuanto supone una forma de actuación que se orienta a ampliar el conocimiento de la realidad que nos rodea. Y debido a la perfección y eficacia que ha logrado, constituye sin duda el método de investigación por excelencia. Por eso, cree este autor que debe ser llamado "*método de investigación científico*" y no "*método científico*" sin más. Así, estima que se puede hablar del método peculiar de cada una de las ciencias) de la Química, de la Economía, etc.), formado por las distintas formas de combinación y aplicación en ellas de los sustantivos de pensamiento y de investigación, pero no existe un método científico peculiar de aplicación general en todas las ciencias, sino es el método de investigación científico.

Considera Sierra Bravo[25] que en el método de investigación científico, al igual que en todo método, se puede distinguir su "*contenido*" o método propiamente dicho y su "*base racional*". El primero está formado fundamentalmente por una serie de etapas sucesivas a seguir para alcanzar el resultado pretendido. Su "*base racional*" está constituida por el conjunto de idas que sirve de fundamento y de orientación al método propiamente dicho.

[24] SIERRA BRAVO, R.: op. cit., págs. 29-30.

[25] Ibídem, págs. 29 y 30.

Método, como procedimiento, está constituido para el mencionado autor por las etapas generales de actuación que forman su contenido y por las técnicas o procedimientos concretos, operativos, para realizar en un caso determinado las fases generales de actuación en cuestión.

Sierra Bravo estima que estas "*técnicas*" específicas de cada ciencia, pueden ser muy diversas puesto que cada objeto de investigación reclama sus técnicas propias. Este autor[26] afirma que entre método científico y técnicas científicas existe una relación clara. Ambos tienen la misma naturaleza y son procedimientos, es decir, formas de actuación científica. Pero se diferencian en la amplitud. Así, el método es un procedimiento general del conocimiento científico y es común en lo fundamental a todas las ciencias. Por el contrario, las técnicas son procedimientos de actuación concretos y particulares relacionados con las distintas fases del método científico.

Así, en general cada ciencia o grupo de ciencias tiene sus técnicas específicas, aunque puede haber técnicas comunes a todas o a varias ciencias. También existen técnicas de empleo general en todas las investigaciones científicas (técnicas generales de documentación, de lectura, de diseño de la investigación, etc.).

Como procedimiento general de actuación seguido en el conocimiento científico, el método de investigación científico se concreta en un conjunto de trámites, fases o etapas. Para este autor, la mejor manera de expresar en qué consiste, es describir las actuaciones que comprende. Consiste en formularse interrogantes sobre la realidad del mundo y de los hombres, basándose en la observación y en las teorías ya existentes; en anticipar soluciones a estas cuestiones y en contrastar, con la misma realidad, dichas soluciones previas o hipótesis mediante la observación de los hechos, su clasificación y su análisis.

Para Sierra Bravo[27], el método científico presenta los siguientes rasgos:

* **Teórico.** El método de investigación científico es un método de investigación teórico en su origen y en su fin. Su punto de partida es, en general, una teoría previa o un conjunto racional y sistemático de

[26] Ib., pág. 47.

[27] Ib., págs. 31-34.

ideas sobre la realidad que se estudia. Es su fin, porque los resultados de la puesta en práctica del método científico se deben concretar en los nuevos principios que reformen, complementen o confirmen las teorías iniciales. Además la teoría también es necesaria para poder observar la realidad. Los hechos, por sí mismos, no dicen nada; por ello, es necesario interpretarlos y hay que ir a ellos con ideas y enfoques previos.

*** Basado en la duda científica.** No existe en la ciencia ningún conocimiento, ley, etc., del que no se pueda dudar o que no pueda ser sometido a nuevas revisiones o no puedan ser sustituidos por otros más exactos y verdaderos.

*** Problemático-hipotético.** Puesto que se basa en la formulación de problemas sobre la realidad y en adelantar conjeturas o soluciones probables a dichas cuestiones.

*** Empírico.** Su fuente de información y de respuesta a los problemas que se plantean es la experiencia, es decir que la ciencia toma sus datos y funda sus conclusiones en la observación ordenada y sistemática de la realidad.

*** Inductivo y deductivo, a la vez.** Es inductivo porque procede mediante la clasificación sistemática de los datos obtenidos durante la observación, con el fin de determinar las regularidades que presentan. Aunque la ciencia se base en la inducción sistemática en mayor medida que otros tipos de conocimientos, utiliza la deducción. Esta consiste en la derivación de conceptos y enunciados, no de la observación de la realidad como la inducción, sino de otros conceptos o enunciados establecidos anteriormente. Por ello, en la ciencia, la inducción y la deducción no se oponen entre sí; por el contrario, la deducción está íntimamente unida en ella a la inducción. La inducción sólo da lugar inmediatamente a datos sobre la realidad; pero la deducción relaciona estos datos, establece conceptos y enunciados con base en ellos y saca conclusiones de todo género.

*** Autocrítico.** El método se autocorrige a sí mismo. Así, por un lado, debe someterse constantemente a contraste y verificación. Y por otro, hay que tener presente que, en ningún caso, los logros científicos son definitivos, ya que siempre están sujetos a la revisión que se puede derivar de nuevos descubrimientos y otros puntos de vistas científicos.

*** Circular.** Puesto que existe una interacción continua en el método científico entre la experiencia y la teoría. Así con base en la experiencia se establece, completa y reforma la teoría, y con base en la teoría se capta y explica la realidad.

*** Analítico-sintético.** Puesto que estudia la realidad distinguiendo y separando unos de otros sus elementos más simples y procura unir y recomponer los elementos separados obteniendo una visión global del conjunto y de las relaciones estructurales entre sus elementos.

*** Selectivo.** El método científico posee esta característica en un triple sentido. En primer lugar, entre la multiplicidad de aspectos de los fenómenos, debe concentrar su observación en lo más importante. En segundo lugar, debe detectar en el análisis los datos más significativos por tener un flujo predominante entre la masa de datos recogidos. Por último, procura trascender las meras apariencias y explicar la realidad lo más profundamente posible.

*** Debe fomentar la intuición y la imaginación.** Además de atenerse alas reglas metodológicas normales.

*** Preciso.** Ya que pretende obtener conocimientos y medidas de la realidad lo más exacto que sea posible. La ciencia tiene vocación de exactitud, por lo que cuanto más exacta es una ciencia, más ciencia es.

1.4. Premisas y objeto de estudio.

El objeto central de nuestro estudio conlleva implícito el examen de una colisión de derechos, el de la intimidad, con los de libertad de expresión y de comunicación. Conflicto que, cuando se concreta, según L. Parejo Alfonso[28], supone una colisión entre los requerimientos del ámbito de lo privado, es decir, lo personalísimo, lo que sólo incumbe a la persona, de un lado, y de lo público, del espacio de lo social o colectivo, de otro; reductibles ambos en la persona en sus diferentes dimensiones.

[28] PAREJO ALFONSO, L.: *Perfiles del derecho constitucional a la vida privada y familiar*. Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 1996, pág. 23.

El desarrollo de las democracias tiene un buen medidor en la soltura de sus libertades, entre ellas, sobre todo, la de expresión. Pero la prevalencia de las libertades de expresión e información frente al derecho fundamental a la protección de datos ha de verse limitada cuando la información personal no goza de interés general ni afecta a personaje público. Ningún ciudadano que no goce de la condición de personaje público, ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen ilimitadamente sin poder reaccionar ni corregir la inclusión de los mismos, como ocurre en nuestros días, en un sistema de comunicación universal como Internet.

La nueva tecnología acelera los movimientos de la información y abre ventanas a más peligros, pero también permite una mayor protección de los datos cuando es preciso. Los mecanismos de defensa ante tan engrandecido escenario de riesgo permanente para nuestros derechos, han de ir haciéndose con los espacios preliminares de todo proceder de empresa de comunicación. Pero eso no resulta una tarea del todo pacífica.

Lograr el importante equilibrio entre las medidas de seguridad y las medidas de protección de los derechos fundamentales innegociables, es también asegurar el respeto de la protección de los datos personales tal como se garantiza en el artículo 8 de la Carta de los Derechos Fundamentales[29].

La regulación de los datos personales es hoy uno de los grandes asuntos que tienen sobre la mesa los responsables comunitarios, aunque hace ya varias décadas que constituye objeto de preocupación. Todo comenzó cuando la Europa de los años ochenta decide levantar aduanas y permitir la libre circulación de personas. Es a partir de ese día, en que todos acogimos con especial y sentida alegría la posibilidad de traspasar fronteras sin pasaporte y tan sólo llevando nuestro DNI en el bolsillo, cuando cuestiones de otra índole empezaron a surgir. La aprobación del Acuerdo Schengen, uno de los hitos más importantes y decisivos en la historia de la Unión Europea, ofrece una nueva dimensión de libertades, pero también suscita la preocupación por la otra cara de lo amable. Las policías alertaron a los Estados sobre nuevos peligros y se pusieron manos a la obra para

[29] Diario Oficial de las Comunidades Europeas C 364, 18/12/2000. Véase web europea: <http://www.europarl.europa.eu/charter/pdf/text_es.pdf>.

abarcar un mayor control de las personas siguiendo la pista de sus datos. De ahí a la necesidad de regular derechos y obligaciones se tardó poco[30].

Nos fijaremos en este estudio en lo que es la actividad no editorial de los Medios de Comunicación Social, además de la actividad empresarial propia inherente a la existencia de la empresa periodística, y requerirá el seguimiento puntual de cómo tratan los periódicos, las emisoras de radio y las televisiones de nuestro país el manejo datos que siempre, en todos los casos, tienen dueño.

1.5. Resultados a obtener.

Nos proponemos conocer los ficheros de datos personales que han registrado oficialmente los Medios de Comunicación con sede social en Sevilla, y la adaptación de los mismos a la hora de afrontar esta legislación, su cumplimiento y la nueva dinámica que supedita.

Clarificar los derechos y obligaciones que adquieren los Medios de Comunicación al dar cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal.

Establecer las nuevas necesidades generadas al gestionar y administrar los datos de carácter personal en su funcionamiento como empresa.

Conocer la repercusión de las infracciones, a tenor de las altas cantidades económicas que contempla la normativa española, y que pueden suponer hasta 600.000 euros por una falta muy grave, y cuyo desconocimiento no exime, obviamente, de su cumplimiento. Infracciones y sanciones que pueden dar lugar a fuertes distorsiones económicos a empresas periodísticas, por ejemplo, de ámbito local y de menores dimensiones.

Comprobar si los riesgos de infracción de una normativa que contempla sanciones económicas tan contundentes, como la relativa a la Protección de Datos Personales en España, son atajados convenientemente por los Medios de Comunicación con la adopción de las debidas cautelas.

---

[30] Sobre Espacio Schengen, véase la página web sobre normativa general comunitaria: <http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_es.htm>

1.6. Agradecimientos.

Agradecimiento especial al profesor doctor José Manuel Gómez Méndez y, de igual modo, a la profesora doctora Pastora Moreno Espinosa, por sus siempre expertas orientaciones a la hora de guiarme en la plasmación de conceptos y por sus apuestas desinteresadas en hacerme creer la posibilidad de concretar este estudio y análisis en una Tesis Doctoral. Mi agradecimiento también para el esfuerzo incomprendido aún de esos jóvenes profesionales que, desde el mundo de la computación y de las nuevas tecnologías, trabajan por adelantarnos y llevarnos al futuro en las mejores condiciones.

2. ALCANCE E IMPORTANCIA DEL DERECHO DE LA PROTECCIÓN DE DATOS PERSONALES EN LOS MEDIOS DE COMUNICACIÓN.

2.1. Una nueva dinámica a afrontar.

El examen de la protección de datos personales en los Medios de Comunicación lo hacemos desde la amplitud de este nuevo ámbito del Derecho, en el intento de orientar a aquellos que diariamente tratan o se encuentran con datos de carácter personal, en qué les afecta y, por tanto, cuáles son sus obligaciones pero, también, qué derechos tienen los interesados que, a la postre, somos todos los ciudadanos. Estar al tanto de las obligaciones propias de las organizaciones públicas o privadas en éste área y estar en condiciones de reconocer las infracciones cuando se producen. Ello nos conducirá al detalle de su interacción con los Medios de Comunicación social.

Un informe del Foro Económico Mundial reunido en enero de 2012 en la ciudad suiza de Davos[31] afirma que la información es una nueva clase de activo económico, como las divisas o el oro. Es, sin duda, una nueva realidad a afrontar pues no es sólo que haya más corrientes de datos personales, sino que son nuevas las dinámicas que se surgen. La abundancia de datos en Internet acelera los avances de la tecnología y la informática. Los negocios, la economía, otros muchos ámbitos, las decisiones se basarán cada vez más en los datos y en el análisis de los mismos, que va convirtiéndose en la nueva gran ambición de algunas compañías en busca del nuevo tesoro.

Este nuevo activo económico, según el Foro de Davos, lo es porque proporciona materia prima para estadística muy valiosa para ventas, precios, economía, demografía, etc. En campos como la ciencia, los deportes, la publicidad y la sanidad hay un cambio de rumbo hacia los descubrimientos y la toma de decisiones basadas en datos que supone '*una revolución*', afirma Gary King, del Instituto de Ciencias Cuantitativas de la Universidad de Harvard[32]. El número de datos personales en internet va

[31] El Foro Económico Mundial trató en 2012 las futuras tendencias tecnológicas, véase: < http://forumblog.org/2012/02/the-2012-top-10-emerging-technologies/>.

[32] Revista de cultura de la edición digital del diario "*Clarín*":
< http://www.revistaenie.clarin.com/ideas/tecnologia-comunicacion/Big-data_0_649735203.html >.

creciendo a un ritmo del 50 por ciento anual. Una explosión de información (tráfico en internet, comentarios en redes sociales, software, sensores controladores de envíos en forma de cookies, proveedores…) que deriva en un cambio de la cultura empresarial, tal y como asegura desde la Universidad de Columbia, en Nueva York, el estadístico Andrew Gelman[33].

Sostiene Tim O'Reilly, gurú de Internet y creador del web 2.0, que el concepto está obsoleto y que "*la privacidad ha muerto*" ante la "*ciencia de los datos, lo más en Silicon Valley*".

Proliferan empresas que se dedican a construir bases de datos sobre ciudadanos valiéndose de toda aquella información de los usuarios que existe en Internet, como pueden ser redes sociales, historiales de compra o interacciones y tráfico entre las diferentes webs.

Como desvela el periodista norteamericano Stephen Baker en su obra 'Numerati'[34], empresas como Tacoda, Umbria, Inform Technologies, entre otras, se afanan en busca de este nuevo activo económico que son los datos personales de ciudadanos del mundo han contratado a especialistas de la estadística para elaborar grandes bases de datos para clasificarlos. La elaboración de esas grandes bases de datos obtenidos a través de cookies o rastreadores corre a cargo de una élite de matemáticos que manejan nuestros datos, y que Baker denomina "*los numerati*". La ambición y el valor de estas compañías que se hacen con millones de datos "*parece no tener límites*", señala.

Ante esta nueva dinámica de comportamientos y devenir que se nos presentan acompañados de obligaciones se encuentran los Medios de Comunicación Social, inmersos en su instintiva dinámica de publicación de informaciones e identidades.

Mucho trabajo queda a los defensores de la privacidad, a tenor de semejante abundancia de datos personales en Internet, al alcance de cualquiera en cualquier punto y los consiguientes peligros que todo ello conlleva. Los grandes dominadores y manejadores de datos personales de Internet, Google y Facebook, sobre todo, se colocan en el punto de mira de defensores de lo privado y autoridades públicas. Se dan situaciones como la protagonizada por la red social Facebook, que se enfrenta en Europa a

---

33 *The New York Times* en "*El País*". Madrid, 23 febrero de 2012.

34 BAKER, Stephen: '*Numerati. Lo saben todo de ti*'. Seix Barral, Barcelona, 2009, págs. 208 y 209.

una multa de 100.000 euros por guardar datos de usuarios que habían decidido eliminarlos.

Esta red social se someterá a una auditoria por la Comisión de Protección de Datos de Irlanda tras registrar 22 quejas por parte de un estudiante austriaco. Denuncia que no es la primera que Facebook afronta porque, a finales de 2009, su creador Mark Zuckerberg ya fue denunciado por su nueva política de privacidad ya que, a juicio de varias asociaciones norteamericanas, atentaba contra los derechos de sus usuarios. En Alemania, por otro lado, el centro de protección de datos del estado de Schleswig-Holstein declaró en agosto de 2011 ilegales los 'plug-ins' sociales como el botón '*Me gusta*', de Facebook, debido a que expone el perfil del usuario[35].

A Google se le ha acusado a inicios de 2012 de utilizar técnicas irregulares que le permitían eludir controles de privacidad para tracear el comportamiento de usuarios de otros buscadores como Safari e Internet Explorer. La controversia surge a partir de un post en el The Wall Street Journal, donde se afirmaba que Google Inc. junto a otras empresas de publicidad habían eludido las restricciones de privacidad de millones de personas que utilizaban el navegador de Apple, Safari, tanto en sus equipos PC como en dispositivos iPhone, para hacer un seguimiento de sus hábitos de navegación.

Las implicaciones que conlleva este tipo de acciones sobre la privacidad de los usuarios han impulsado la creación de una Consumer Privacy bill of Right o Ley de los Derechos de Privacidad de los Usuarios por parte del Gobierno de EEUU, que puede consultarse en la web de la Casa Blanca[36].

La idea de esta ley es establecer un marco estandarizado de buenas intenciones que garantice el control, la seguridad y la transparencia sobre la privacidad y los datos personales de los usuarios. Para ello, ya han mostrado su compromiso empresas como Google, Yahoo o Microsoft.

[35] Disponible en: <http://www.abc.es/20111024/medios-redes/abci-facebook-multa-201110241252.html>.

[36] Véase: <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

EEUU, no obstante, prepara para 2012 una normativa que otorgue el derecho a los internautas de controlar los datos personales que las empresas recogen y la manera en que los utilizan[37].

Se trata, también, según persigue la Administración estadounidense, de asegurar una información comprensible y accesible sobre las prácticas de privacidad de las compañías y que los datos suministrados se utilicen para los fines para los que se recogen y se manejen con seguridad. El bloqueo de datos, pese a todo, no será total. Las empresas aceptan no usarlos para fines de empleo, créditos, seguros o salud así como para personalizar la publicidad, pero podrán emplearse para la investigación de mercado o el desarrollo de productos. Esta medida no bloquearía botones como el empleado por Facebook con el controvertido '*Me gusta*'. La preocupación por el rastreo de la navegación es creciente.

En el marco de una mayor presión a los grandes de Internet para que mejoren sus políticas de privacidad, una treintena de fiscales generales de EE UU han remitido una carta a Google expresando su inquietud por los cambios anunciados por la compañía, que quiere unificar las condiciones de uso de la mayoría de sus servicios que hará compartir los datos del internauta. Google ha vuelto a defender que su plan únicamente pretende una exposición más fácil y comprensible de la política de privacidad.

Europa también ve cómo la actividad de los grandes de Internet (Apple, Google, Facebook, Microsoft, HP, RIM o Amazon), a pesar de tener sede oficial en EE.UU, trasciende fronteras y se ha puesto manos a la obra para establecer una política de privacidad mucho más rigurosa, con multas a las compañías privadas que violen la normativa de recolección de datos privados.

Viviane Reding, Comisaria de Justicia y Derechos Fundamentales de la CE, ha anunciado en enero de 2012 la propuesta, basada en que la protección de datos de los internautas es un "*derecho fundamental pero a veces los ciudadanos ven como se les escapa de las manos*"[38].

---

[37] Disponible en la sección sobre tecnología de la edición digital del "*El País*": <http://tecnologia.elpais.com/tecnologia/2012/02/23/actualidad/1329984921_916013.html>.

[38] Véase la página web sobre información, documentación y legislación europea: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=1&language=ES&guiLanguage=en>.

El objetivo que se traza la UE con la propuesta es que todos los europeos puedan borrar cualquier atisbo de información personal en la red si algún día así lo deciden, incluso si han formado parte de servicios que registran datos personales como Facebook, Twitter, LinkedIn o Foursquare, entre otros muchos. En ello va implícito el denominado 'derecho al olivo digital', el derecho de los ciudadanos a hacer desaparecer de la Red sus datos personales, y del que nos ocupamos en el Capítulo 10 de este estudio.

La Unión Europea quiere dotar de mayor poder a la autoridad pública para alcanzar una mayor protección para los ciudadanos y sus datos personales. El proyecto normativo [39] busca unificar las distintas normas de protección de datos de los Estados miembros y crear un marco común europeo en el que se salvaguarde más la privacidad del ciudadano, pues no todos los Estados adaptaron por igual 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[40].

En virtud de la nueva normativa, en lo sucesivo, cualquier caso de pérdida, robo o piratería de datos debe ser notificado a las autoridades y a los usuarios en un plazo de 24 horas, según establece la propuesta de la Comisión, que incluye también penas para aquellos que no cumplan. Así, los Estados estarán facultados para sancionar las violaciones graves de la privacidad y las negligencias en la custodia de información con multas de hasta el 1% de los ingresos mundiales de la firma. Es decir, que si Google se viera implicado en un caso como éste sería sancionado con una multa que podría rondar los 292 millones de euros. Algo que puede obligar a que las grandes empresas de Internet revisen sus sistemas de salvaguarda de datos[41].

La normativa, que debe pasar por el Consejo Europeo y por el Parlamento[42], es de aplicación en los 27 países de la UE pero también a todas las empresas que ofrezcan bienes y servicios a los consumidores

[39] Véase: <http://www.lexdiario.es/noticias/112677/la-comision-europea-propone-una-reforma-general-de-las-normas-de-proteccion-de-datos>.

[40] Diario Oficial de la Unión Europea n° L 281, de 23/11/1995, págs. 31-50.

[41]<http://www.lopdgest.com/desktopdefault.aspx?tabid=11079&rowid=483038,26512>

[42] Las competencias principales del Parlamento y del Consejo son debatir y aprobar la legislación de la Unión Europea, de aplicación en todos los Estados que la conforman: < http://europa.eu/about-eu/institutions-bodies/european-parliament/index_es.htm>.

europeos, lo que puede suponer que las grandes empresas internacionales que recogen datos en Europa deban responder ante el Derecho comunitario y las autoridades competentes europeas si vulneran las normas de protección de datos, aunque tengan su sede matriz en California.

Desde la Comisión Europea, la responsable de Justicia, Viviane Reding, defiende que "*las compañías que dirigen sus servicios a los consumidores europeos deben estar sujetas a la legislación de protección de datos de la UE. Las compañías que dirigen sus servicios a los consumidores europeos deben estar sujetas a la legislación de protección de datos de la UE. De lo contrario, no debería poder hacer negocios en nuestro mercado interno*", según ha lanzado en una alocución pública[43].

Para la Comisión Europea, lo esencial es que los usuarios puedan controlar sus datos, de ahí que la futura normativa europea exija requerir que los consumidores puedan dar su consentimiento explícito antes de que se utilicen sus datos y, en general, se tenga el derecho de eliminar sus datos en cualquier momento, especialmente los datos que sobre uno mismo pueda estar indexado en Internet. La Comisaria Viviane Reding ha insistido en ese mensaje difundido a finales de 2011 en que la protección de datos es una cuestión de "*gran relevancia para consumidores y empresas*" y, por tanto, "*necesita abordarse a nivel europeo, a través de estándares elevados y comunes europeos de alcance global*"[44].

Entre las argumentaciones de la Vicepresidenta de la Comisión Europea, está el Tratado de Lisboa, que "*ofrece a Europa la oportunidad única para modernizar y reforzar las normas de protección de datos ahora. Creemos que como resultado del proceso de reforma, los consumidores en Europa deben ver fuertemente protegidos sus datos, con independencia del país de la UE en el que residan y con independencia del país en el que las compañías, que procesan sus datos personales, están asentadas*", según las argumentaciones de Reding[45].

---

[43] 'La UE defiende que todas las empresas se sometan a las leyes europeas de protección de datos'. "*El País*", de 8 de noviembre de 2011. Disponible en: <http://tecnologia.elpais.com/tecnologia/2011/11/08/actualidad/1320746463_850215.html>.

[44] Ibídem.

[45] Ibídem.

La estadística indica que el 90% de los europeos se muestra a favor de garantizar los mismos derechos de protección de datos en la UE, según una encuesta del Eurobarómetro realizada a finales de 2011. El 70% de los europeos está preocupado por la utilización de sus datos personales por compañías y considera que solo tiene control parcial sobre los mismos, mientras que el 74% defiende que tengan que dar su consentimiento para recoger y procesar sus datos en la Red, a tenor del Eurobarómetro[46].

Es en lo que se trabaja ante la aparición de nuevos riesgos, pero desde la Unión Europea han sido notables los esfuerzos dirigidos a este fin. Hemos de situarnos en mayo de 1994 cuando un grupo de trabajo, encabezado por el Ministro de Industria del Gobierno de Alemania, Martin Bangemann, sentó los primeros cimientos en la definición y diseño de las medidas a adoptar para la consecución de la Sociedad de la Información. El llamado 'Grupo Bangemann', que fue quién utilizó por primera vez el término 'Sociedad de la Información', elaboró un informe, el denominado 'Informe Bangemann'[47], a partir del cual las iniciativas y documentos comunitarios fueron sucediéndole constantemente.

El Tribunal Superior de Justicia de la UE, con sede en Luxemburgo[48], ha dado un respaldo a estas posiciones sobre protección de datos prohibiendo a los proveedores de Internet espiar a sus usuarios en un pronunciamiento sobre derechos de autor, programas "peer-to-peer", proveedores de acceso a Internet, y establecimiento de un sistema de filtrado de las comunicaciones electrónicas para evitar los intercambios de archivos que vulneren los derechos de autor, al declarar la inexistencia de obligación general de supervisar los datos transmitidos.

Ha sido en la sentencia del TSJE de 24 de noviembre de 2011, a raíz de un caso originado en Bélgica[49], en la que remarca que las reglas

[46] Disponible en: < http://ec.europa.eu/spain/eurobarometro/index_es.htm>.

[47] 'Europa y la Sociedad global de la Información'. Recomendación del Grupo Bangemann al Consejo Europeo, 26 de mayo de 1994.

[48] El Tribunal de Justicia interpreta el Derecho de la UE para garantizar que se aplique de la misma forma en todos los países miembros. También resuelve conflictos legales entre los gobiernos y las instituciones de la UE. Los particulares, las empresas y las organizaciones pueden acudir también al Tribunal si consideran que una institución de la UE ha vulnerado sus derechos:
<http://europa.eu/about-eu/institutions-bodies/court-justice/index_es.htm>.

[49] Diario Oficial de la Unión Europea, n° C 25, de 28/01/2012, pág. 6.

comunitarias establecen "*la prohibición*" de luchar contra las violaciones de derechos de autor a través de "*medidas que obliguen a un proveedor de acceso a Internet a proceder a una supervisión general de los datos que transmita en su red*". El tribunal reconoce que el derecho a la propiedad intelectual está "*consagrado en la Carta de los Derechos Fundamentales de la UE*", pero que su protección no puede "*garantizarse en términos absolutos*". Filtrar la red para vigilar al usuario supondría una "*vulneración sustancial de la libertad de empresa*", pero sobre todo la violación de "*los derechos fundamentales de sus clientes, a saber, su derecho a la protección de datos de carácter personal y su libertad de recibir o comunicar informaciones*"[50].

El derecho fundamental a la protección de datos extiende su cobertura no a los datos íntimos de la persona -que se protegen en el derecho a la intimidad-, sino a los datos de carácter personal. Por tanto, "*la garantía de la vida privada de la persona y su reputación poseen una dimensión positiva que excede del ámbito del artículo 18.1 de la Constitución y que se traduce en un derecho al control sobre los datos por el titular de los mismos*".

Mediante este derecho fundamental se pretende garantizar a la persona un poder de disposición sobre los datos personales, sobre su uso y destino, para salvaguardar la dignidad del afectado. Así lo reconoce una sentencia de la Audiencia Nacional, de 30 de enero de 2008[51], que apoya una Resolución de la Agencia Española de Protección de Datos en la que se condenaba a una compañía eléctrica por utilizar los datos personales de los denunciantes sin su consentimiento. Según establece en sus primeros artículos la Ley Orgánica de Protección de Datos.

En este sentido, la ponente, la magistrada Teso Gamella, alude a la doctrina reconocida por el Tribunal Constitucional por la que "*el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, o cuáles puede este tercero recabar*"[52].

---

[50] Ibídem.

[51] Véase en: < http://audiencia-nacional.vlex.es/vid/-37388626>.

[52] 'El titular de un dato tiene derecho a controlar su uso', en "*El Economista*", Madrid, 26 de septiembre de 2008.

Respecto al conflicto jurídico que pueda plantearse en la actividad periodística entre el derecho a la protección de datos y la libertad de expresión, remarcar de antemano que el legislador español no ha establecido una previsión similar a la establecida por el artículo 9 de la Directiva 95/46/CE, según la cual "*en lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión*"[53].

No obstante, la resolución del conflicto entre los derechos reconocidos en los artículos 18 y 20 de la Constitución ha sido objeto de reiterado análisis por la jurisprudencia del Tribunal Constitucional, sentando como regla general la doctrina emanada del citado tribunal que el segundo de los derechos citados prevalecerá en aquéllos supuestos en los que la información objeto de publicación sea, por una parte, veraz, y por otra resulte de relevancia pública, siendo de interés general las materias a las que la misma se refiere y la relevancia de las personas a las que la misma se refiere. La prevalencia de la libertad de expresión sobre el derecho a la protección de datos[54] ha sido reseñada por la Agencia Española de Protección de Datos en varios de sus Informes jurídicos y muchas de sus Resoluciones, basándose en lo que el Tribunal Constitucional ha asentado en su jurisprudencia[55].

La extensión del uso de la red Internet a todas las actividades de la vida ha proporcionado una nueva y mayor dimensión de lo privado. En términos de Derecho, la esfera íntima de las personas se ha visto en mayor zona de riesgo y, a su vez, más necesitada de cobertura y atención.

---

[53] Diario Oficial de la Unión Europea, nº L 281, pág. 41. Disponible en : <http://www.boe.es/doue/1995/281/L00031-00050.pdf>.

[54] El subrayado es nuestro.

[55] Han sido varios los pronunciamientos del Tribunal Constitucional estableciendo la prevalencia de la libertad de expresión sobre el derecho a la protección de datos, citados por la Agencia Española de Protección de Datos, como la Sentencia 171/1990, la 204/1997, o la 107/1998.

Con la red Internet, el mundo de los buscadores, convertidos alguno de ellos en auténtico 'alter ego' de los Medios de Comunicación en la actualidad, ofrecen su potencial como fuente de información accesible y permanente. El buscador más aplicado por la mayoría de usuarios, Google, no cesa de plantear problemas inquietantes tanto en Estados Unidos como en Europa, por no referirnos ya al resto de áreas del mundo.

Imágenes y detalles de nuestras casas están al alcance de todos en Google Earth Google Street View. Nuestros smartphones permiten localizarnos. Nuestra búsqueda en el buscador es la historia íntima de nuestra vida. Bancos y otras entidades tienen acceso a nuestro historial de crédito. No contento con eso, Google se agiganta y adquiere nuevos instrumentos, como su compra de *DoubleClick*, la gran compañía de publicidad en línea, ganando no sólo en poderío mercantil sino en acceso a información sobre los consumidores[56].

El derecho a la intimidad ya quedó recogido hace décadas en el texto de la Declaración Universal de los Derechos Humanos, en su art.19[57]. La realidad ha sido otra cuestión, porque la Declaración sigue siendo otro gran caballo de batalla de la comunidad internacional por el incumplimiento que hacen de ella numerosos países, y sus redactores, aquellos Gobiernos que tuvieron la ocasión en 1948, no pudieron contemplar los nuevos escenarios de la era digital. La propia ONU promovió una Cumbre mundial celebrada en 2005 en Túnez sobre la Sociedad de la Información, cuyo texto final[58] sólo alcanza a "*exhortar*" a Gobiernos, empresas y ciudadanos a proteger los datos personales mediante leyes o "*el intercambio entre las empresas y los usuarios de mejores prácticas*", según recoge.

Hasta que no llegue este deseado aunque muy complicado Reglamento universal, lo principal es que las empresas hagan públicos sus protocolos de privacidad y los cumplan. La recolección de datos y el empleo que se haga de los mismos ha de ser conocido por su titular, y el

[56] 'Lo privado en Internet', en el editorial de "*El País*", Madrid, 16 de septiembre de 2007, en: < http://elpais.com/diario/2007/09/16/opinion/1189893602_850215.html>.

[57] "*Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión*". Véase en: <http://www.un.org/es/documents/udhr/>.

[58] Declaración de Principios acordados en 2005 en la Cumbre de Túnez: <http://www.itu.int/wsis/docs2/tunis/off/7-es.html>.

internauta tiene el derecho de poderlos gestionar a voluntad. En ese camino se ven inmersos los Medios de Comunicación Social.

Un simple ejercicio de marcar la casilla que nos indica una página web de las que nos ofrece cualquier medio en sus ediciones digital puede costarnos caro. Son cada vez más utilizados y extendidos los programas de intercambio de archivos P2P, llamados así porque van de par a par **(***peer to peer*), o entre iguales[59]. Eso quiere decir que cuando uno se conecta a una de estas redes se convierte en cliente y servidor, recibiendo y enviando archivos al mismo tiempo.

La práctica está en cualquiera de nosotros. Mientras está conectado el ordenador, los archivos que recibe van a una carpeta de entrada creada por el propio sistema, generalmente llamada *incoming*, y automáticamente son compartidos con el resto de la red. El internauta tiene también la opción de compartir otras carpetas de su ordenador, activando la casilla que viene en el menú de archivos compartidos. Y aquí es cuando surge el problema. Si por descuido se marca la casilla equivocada se puede llegar a compartir todo el disco duro. En el eMule, uno de estos programas (junto con BitTorrent, Pando, Ares o Nosolodescargas, entre otros), esa casilla se activa en el menú de preferencias. También se puede cambiar el archivo de destino.

Descuidos así suceden muy a menudo, y los internautas comparten fotos y archivos personales sin tener consciencia de ello. Para buscarlos habría que conocer su nombre o buscarlo *ex profeso* dados los millones de archivos que hay en la Red. Estaríamos incurriendo en una infracción a la protección de datos como veremos en este estudio.

A nivel comunitario, el Consejo, la Comisión Europa y todas las autoridades de Protección de Datos de los países miembros de la UE, en un encuentro celebrado con motivo del Día Europeo de la Protección de Datos[60] se ha propuesto el fin de impulsar el conocimiento entre los ciudadanos europeos de cules son sus derechos y responsabilidades en esta

[59] 'Atención al marcar la casilla', "*El País"*, Madrid, 25 de abril de 2008, en: <http://elpais.com/diario/2008/04/25/sociedad/1209074402_850215.html>.

[60] El Día Europeo de la Protección de Datos es el 28 de enero de cada año. Véase en: <http://www.elpais.com/articulo/internet/denuncias/incumplimiento/proteccion/datos/duplican/elpeputec/20080128elpepunet_1/Tes>.

materia, y familiarizarse con un aspecto normativo que, a pesar de ser menos conocido, está presente en muchas facetas de su vida diaria.

Según el Eurobarómetro, más del 60% de los ciudadanos europeos tienen un conocimiento escaso acerca de sus derechos en materia de protección de los datos y sobre la existencia de autoridades independientes con competencias para su protección. No obstante, la Agencia Española de Protección de Datos está multiplicando el número de demandas de tutela, circunstancia que evidencia una concienciación, cada vez mayor, de los ciudadanos sobre este aspecto legal.

Las tutelas corresponden al derecho de los ciudadanos a conocer la información personal que obra en poder de entidades públicas y eliminar, corregir los datos inexactos o irreales. Los sectores tradicionalmente afectados por las tutela de los datos y que protagonizan el 90% de este tipo de las tutelas son la banca y las telecomunicaciones, básicamente por la inclusión indebida en ficheros de morosos y la obtención fraudulenta de información personal para contrataciones, servicios de agua, gas o telefonía.

Sin embargo, el uso de las nuevas tecnologías e Internet ha abierto un nuevo ámbito de quejas y denuncias en la Agencia Española de Protección de Datos. Desde hace pocos años, este órgano recibe reclamaciones por parte de españoles que sienten vulnerados sus derechos por la inserción de imágenes en el popular portal YouTube[61], o el intercambio de archivos P2P.

Tan es así que se emitió una importante sanción impuesta por la Agencia Española de Protección de Datos, castigando, por primera vez, la grabación y posterior difusión de imágenes a través del Youtube. Algo tan simple en lo que puede incurrir cotidianamente cualquier medio de comunicación televisivo.

---

[61] Sitio web, plurilingüe, que permite a los usuarios compartir vídeos digitales a través de Internet. Fue fundado en febrero de 2005 por antiguos empleados de empresas tecnológicas. YouTube es propiedad de Google, desde su compra, en octubre de 2006 por 1.650 millones de dólares. Utiliza un reproductor en línea basado en Adobe Flash para ofrecer su contenido. Su popularidad, lograda gracias a la posibilidad de alojar vídeos personales de manera sencilla, hace que supere en seguimiento a la inmensa mayoría de Medios de Comunicación Sociales convencionales. Sus enlaces a vídeos pueden ser también puestos en blogs y sitios web personales usando añadiendo códigos html. YouTube ha tenido tal impacto en la cultura popular que en 2006 obtuvo el premio al "invento del año" otorgado por la revista Time.

El caso es que resuelve un procedimiento[62] iniciado de oficio en octubre de 2007, a raíz de las informaciones publicadas en distintos medios de comunicación, en relación con la captación y posterior difusión, a través de YouTube, de imágenes en las que aparecían personas en una calle de Madrid. Las investigaciones realizadas por la Agencia de Protección de Datos concluyen con la declaración de una infracción grave de la Ley Orgánica de Protección de Datos y la imposición de una considerable multa económica a los responsables de la grabación y posterior publicación en Youtube de imágenes en las que se podía identificar a transeúntes, al incumplir el principio de consentimiento de la Ley española, establecido en el artículo 6 de la misma.

En su Resolución, la Agencia Española de Protección de Datos afirma que la medida de distorsión de imágenes personales adoptada en veinte de los veintidós de los vídeos publicados, así como la voluntad de no dañar la intimidad de los viandantes y el deseo de mejorar la seguridad pública de la zona, permite entender que hay una disminución de la culpabilidad del sancionado, reduciendo la gravosidad de las multas económicas previstas en Ley de Protección de Datos para este tipo de infracciones.

Se trata, por tanto, de la primera sanción que impone la Agencia Española de Protección de Datos por la captación y difusión de imágenes a través de sistemas como Youtube, pero posteriormente han sido abiertos otros procedimientos relacionados con este tipo de sistemas[63].

Es importante dejar claro lo que sienta en su Resolución la Agencia encargada de la tutela de los datos personales en España, al establecer que la captación y reproducción de imágenes de personas, siempre que permitan la identificación de las mismas, y su publicación en un sitio web como es Youtube, accesible para cualquier usuario de Internet, se encuentra sometida al consentimiento de sus titulares.

---

[62] Véase procedimientos en la web de la Agencia Española de Protección de Datos: <https://www.agpd.es/portalweb/resoluciones/procedimientos_sancionadores/ps_2008/common/pdfs/PS-00617-2008_Resolucion-de-fecha-26-06-2008.pdf.

[63] Disponible en el apartado dedicado a Notas de Prensa de la web de la Agencia Española de Protección de Datos: <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2008/notas_prensa/common/julio/NP_220708_Youtube.pdf>.

A los Medios de Comunicación Social, la regulación de este segmento del derecho les ha ido aproximando y colocándose en posición a considerar silenciosa pero inevitablemente. La colisión entre lo que publica cotidianamente un periódico, emite una radio o difunde una televisión y los derechos de la intimidad de la persona eran, hasta ahora, cuestión directamente relacionada con la imagen y la esfera de privacidad del ciudadano. A ello se ha sumado la protección de datos de carácter personal, con todas sus obligaciones y procedimientos, lo que lleva a tomar nuevas cautelas y a empezar a mirar le necesidad de forjar alianzas estratégicas a nivel de empresas mediáticas para asegurar una correcta dinámica en el futuro.

De hecho, el director de la Agencia Española de Protección de Datos hasta 2011, Artemi Rallo, ha estado insistiendo durante varios años en la voluntad del organismo estatal de encontrar un equilibrio ante el conflicto existente entre el derecho a la tutela judicial efectiva, en relación a la identificación de la dirección IP de usuarios de Internet, con el derecho a la protección de datos personales[64]. En este sentido, incide en la necesidad de que el ordenamiento proporcione a los usuarios de Internet garantías de sus derechos en materia de protección de datos, buscando una ponderación que no impida o dificulte el ejercicio de otros, como el derecho a la tutela judicial efectiva para la protección de los derechos de autor en las redes P2P[65].

La normativa existente y los tribunales han ido aportando criterio sobre el equilibrio entre ambos derechos, aunque sigue habiendo lagunas que requieren reajustar el actual marco jurídico.

[64] Véase: <http://www.faq-mac.com/noticias/agencia-espanola-proteccion-datos-quiere-terminar-p2p-anonimo/31615>.

[65] Una red informática entre iguales (en inglés, *peer-to-peer* -que se traduciría de par a par- o de punto a punto, y más conocida como P2P) es aquella que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores respecto de los demás nodos de la red. Se trata de una forma admitida de compartir archivos de forma similar a como se hace en el email o mensajeros instantáneos, sólo que de una forma más eficiente. Lo habitual es que en estas redes quede anónimo el autor de un contenido, el editor, el lector, el servidor que lo alberga y la petición para encontrarlo siempre que así lo necesiten los usuarios. En la mayoría de los casos, el derecho al anonimato y los derechos de autor son incompatibles entre sí. El modelo P2P de red contrasta con el de cliente-servidor.

La publicidad es otro ámbito importante, en lo que se refiere a la protección de datos. En los años 2009, 2010 y 2011, las principales quejas ciudadanas fueron las relacionadas con las llamadas telefónicas a móviles sin el conocimiento del usuario, o los *spam*, a través del correo electrónico[66].

Otro de los sectores más polémicos es el de la vigilancia por medio de cámaras de video o circuitos de televisión. Las denuncias por el uso de manera indebida de estos sistemas se han incrementado, ya que se ha dado una implantación progresiva en el ámbito laboral, el comercio y los medios de comunicación. La vigilancia por medio de cámaras videos[67] debe regirse por varios criterios: los dispositivos deben ser suficientemente visibles, aunque de la forma menos agresiva, mientras que la toma de imágenes ha de ser, según la Agencia, "*adecuada*, *pertinente y no excesiva*", garantizando en todo caso el acceso y la cancelación por parte de las personas cuya imagen sea captada.

El Observatorio de la Seguridad de la Información de Inteco[68] ha realizado un diagnóstico del panorama con el '*Estudio sobre el grado de*

[66] Memorias de 2009, 2010 y 2011 de la Agencia Española de Protección de Datos.

[67] Regulada en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Publicada en el B.O.E., núm. 296, de 12 de diciembre de 2006, págs. 43458-43460.

[68] El Instituto Nacional de Tecnologías de la Comunicación, promovido por Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología. Tiene un doble objetivo: contribuir a la convergencia de España con Europa en la Sociedad de la Información y promover el desarrollo regional, enraizando en León un proyecto con vocación global. El Instituto alberga el Centro de Respuesta a Incidentes en TI para pymes y ciudadanos, el Observatorio de la Seguridad de la Información, el Centro Demostrador de Seguridad para la PYME, el Centro de Referencia en Accesibilidad y Estándares Web y el Laboratorio Nacional para la Calidad del Software, entre otros: <http://www.inteco.es>.
El Observatorio de la Seguridad de la Información se inserta dentro de la línea estratégica de actuación de Inteco en materia de seguridad y e-confianza. En cumplimiento de uno de los objetivos encomendados a Inteco en el marco del Plan Avanza, su misión es describir de manera detallada y sistemática el nivel de seguridad y confianza en la Sociedad de la Información en los hogares, empresas y Administración, así como generar conocimiento divulgativo y especializado en la materia, así como la elaboración de recomendaciones y propuestas que definan tendencias válidas para la

adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos (LOPD) y el nuevo Reglamento de desarrollo'.

El 96% de las pymes españolas, entre ellas muchas son empresas de Medios de Comunicación (especialmente numerosos periódicos provinciales y locales) que han de darse por aludidos, disponen de ficheros con datos personales, y el 78% en soporte automatizado. Todas ellas están por tanto sujetas a la normativa sobre protección de datos.

El estudio muestra que el nivel de declaración de ficheros por las pymes ante el Registro General de Protección de Datos es del 16%. Esta cifra es coherente con la manejada por la propia Agencia estatal de Protección de Datos, que estima que entre un 10% y un 15% de las pymes españolas han notificado sus ficheros. Es particularmente relevante señalar que en el último año las inscripciones de ficheros han aumentado un 20%.

La postura de la pyme sobre la protección de datos es receptiva y favorable: el 82% de los encuestados dice estar concienciado con la necesidad de cumplir con la Ley Orgánica de Protección de Datos y el Reglamento que la desarrolla, mientras que el 79% confirman su intención de destinar medios (económicos y/o humanos) para adaptarse a la normativa sobre protección de datos.

El 96% de las empresas españolas de menos de 50 empleados disponen de datos de carácter personal y están, por tanto, sujetas a la normativa sobre protección de datos, según se desprende del estudio de Inteco[69].

La presencia de datos personales entre las pymes españolas es prácticamente universal. Los datos de clientes (72%), proveedores (51%) y nóminas de empleados (30%) son, en este orden, los más habituales en el negocio de las pequeñas y medianas empresas. En estos ficheros se recogen

toma de decisiones de futuro por parte de la industria y los poderes públicos: <http://observatorio.inteco.es>.

[69] El estudio ha sido realizado a partir de encuestas realizadas a 250 responsables de seguridad informática de empresas españolas de hasta cincuenta empleados, así como quince entrevistas en profundidad a juristas, auditores y consultores especializados en la adaptación de las pymes a la normativa de protección de datos, destacando la aportación de la Agencia Española de Protección de Datos. Disponible en: <http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informe>.

principalmente los datos personales referidos al nombre (76%), la dirección (71%), el teléfono (70%) y el correo electrónico (41%) del titular. Son muchas las empresas periodísticas que son pymes.

Otro gran cambio (revolución para muchos) en los Medios de Comunicación ha venido con las redes sociales, que irrumpen como una de las mayores expresiones de participación de los receptores, ya que no podrían existir sin la participación de la audiencia. La finalidad de potenciar el uso de las redes desde los Medios de Comunicación es multiplicar su presencia en estos otros espacios de distribución y aumentar su tráfico de visitas. El uso más común para los Medios es usar Redes marcadores donde se publican noticias, y después redes sociales más privadas. Se percibe, por parte de los Medios españoles más visitados, un interés por la introducción de este nuevo cauce de interactividad, que además les beneficia como plataforma de distribución de sus contenidos entre las diversas redes, produciendo un efecto cadena entre los miembros de la red social y mejorando su repercusión[70].

La formación en la materia va a seguir siendo clave. Con el contexto descrito, todo indica que sigue siendo necesaria una tarea formadora e informadora. El esfuerzo sensibilizador ha de estar orientado específicamente a las necesidades del entorno pyme, que, hablando en términos generales, presentan unas circunstancias comunes que las caracterizan y diferencian de las empresas de mayor tamaño, y ha de proceder de todos los actores implicados: las administraciones públicas y el propio mundo empresarial (cámaras de comercio, patronales, asociaciones, etc. y donde deben estar los Medios de Comunicación de una manera lo más uniforme posible).

Es muy importante a tener en cuenta el hecho de que las sanciones en materia de Protección de Datos a empresas y particulares, pueden llegar a alcanzar los 600.000 euros en los casos más graves.

2.2. Repercusión de las infracciones.

Los Medios de Comunicación se encuentran ante un Derecho y una dinámica que deriva en sanciones por infracciones de la normativa que van

[70] GARCÍA ESTÉVEZ, Noelia. '*Redes sociales en Internet'*. Editorial Universitas, Madrid, 2012, pág. 223.

desde los 600 hasta los 600.000 euros, es decir, cantidades cuya envergadura llega a superar las que reservan normas como la relativa a la Prevención de Riesgos Laborales, que, como puede suponerse, pueden estar afrontando casos con daños en las personas. Sirva contrastar gráficamente normas y sanciones[71].

Contamos en España con la ley más dura de Europa en materia de sanciones por infringir la normativa que regula la protección de datos personales.

Un estudio realizado por las Cámaras de Comercio[72] comparando la legislación española en materia de protección de datos personales con el resto de regulaciones europeas, pone de manifiesto las notables diferencias en lo relativo a la contundencia y gravedad de las sanciones que imponen unas y otras.

Curiosamente, la Ley de Protección de Datos española[73] aparece como el régimen sancionador más severo lo que, de acuerdo con las Cámaras de Comercio, podría perjudicar a las empresas españolas y hacer que los empresarios decidiesen trasladar su centro de negocios a otros países europeos para así gozar de menores sanciones y legislaciones menos estrictas.

Sirve como ejemplo el hecho de que frente a los 1.300 euros que prevé la sanción más elevada que contempla la legislación irlandesa, la Ley española contempla, como hemos indicado, multas de hasta 600.000 euros.

Existen algunas normas que no recogen ni tan siquiera sanciones pecuniarias, como son las del Reino Unido, Dinamarca o Finlandia, mientras que otros Estados no determinan exactamente las sanciones.

Además de poner de manifiesto estas abismales diferencias, el estudio citado[74] considera "*necesario cambiar el sistema de financiación*

[71] Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales. B.O.E., núm. 269, Madrid, de 10 de noviembre de 1995, págs. 32590-32611.

[72] Publicado en la web del Instituto de Marketing Relacional Directo & Interactivo: <http://comunidad.icemd.com/area-entrada/noticias/imprimir.asp?Id=180>.

[73] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. B.O.E., núm. 298, Madrid, 14 de diciembre de 1999, pág. 43088.

[74] Véase: <http://comunidad.icemd.com/area-entrada/noticias/imprimir.asp?Id=180>.

de la Agencia de Protección de Datos". Según el análisis de las Cámaras, y atendiendo a sus conclusiones, la Agencia española encargada de tutelar los derechos y deberes de los datos personales en nuestro país "*debería financiarse mediante partida presupuestaria, y no a través de las multas y sanciones que impone*"[75].

Esta circunstancia que presenta nuestra normativa ha hecho plantear más de una vez y en muchos ámbitos la verdadera eficacia de esta serie de sanciones tan elevadas y duras en materia de protección de datos, y si realmente hace extender en la práctica de empresas, entidades y Administraciones españolas la conciencia y el cumplimiento de los preceptos que trata de salvaguardar.

De otro lado, las legislaciones nacionales en esta materia son fruto de la transposición de la Directiva europea 95/46/CE[76] en los ordenamientos nacionales y, en consecuencia, todas las normas europeas derivan en sus contenidos y exigencias de este texto legal europeo. No obstante, los Estados miembros se reservan la facultad de establecer el régimen sancionador que consideren más conveniente para preservar la materia que es objeto de protección. Es cierto que las sanciones impuestas por la Ley Orgánica de Protección de Datos española (LOPD)[77] son considerablemente elevadas, sin embargo, en términos de "gravedad", puede mencionarse, por ejemplo, que la Ley italiana 127/2001 establece penas de prisión para los transgresores de las disposiciones en ella recogidas. Analizar pormenorizadamente las sanciones impuestas por los regímenes sancionadores europeos en materia de protección de datos como más o menos 'graves' en función de la sanción 'pecuniaria' que impone puede llevarnos a tener una visión limitada sobre esta normativa[78].

Aunque es evidente que existen hay diferencias sustanciales entre las sanciones impuestas por una u otra legislación europea, el contraste más notable se observa en la manera divergente en que las autoridades nacionales interpretan determinados conceptos jurídicos. Otro aspecto en el

---

[75] Ibídem.

[76] Diario Oficial de la UE n° L 281 de 23/11/1995, op. cit., pág. 30.

[77] B.O.E., núm. 298, de 14/12/1999, págs. 43088-43099.

[78] Estudio comentado por Rafael García del Poyo, abogado del despacho jurídico Garrigues de Madrid, en: <http://www.icemd.com/area-entrada/noticias/>.

que verdaderamente se hacen evidentes las diferencias es la forma en la que las autoridades nacionales europeas hacen cumplir la ley, así como la intensidad y el talante con el que estas autoridades tutelan y defienden las libertades públicas de los ciudadanos a través de los mecanismos jurídicos que las propias leyes recogen.

En este sentido, han podido observarse actitudes de responsables públicos nacionales muy dispuestos a colaborar y negociar con las empresas para que la norma fuese cumplida, si bien en otros casos la posición ha sido mucho más autoritaria y menos conciliadora.

La legislación en materia de protección de datos existe para ser cumplida por todos y en toda su extensión. Por ello, visto el grado actual de cumplimiento de esta normativa, lo más idóneo es que las empresas deberán llevar a cabo un esfuerzo aún más profundo, al objeto de alinearse con los preceptos recogidos en la Ley española de Protección de Datos y en su Reglamento, que establece la relación de Medidas de Seguridad, como aquí veremos. Una vez establecida esta premisa, puede afirmarse que la contundencia y repercusión de las sanciones no emana tanto del texto jurídico que resulta de aplicación sino de la interpretación más o menos estricta que del mismo hace la autoridad reguladora en el texto de la Ley Orgánica[79].

Lógicamente, en este punto siempre puede llegar a influir el mayor o menor ánimo recaudatorio de la autoridad reguladora, el cual puede verse afectado en función de si su presupuesto anual proviene de una partida estatal o depende directamente de las sanciones recaudadas. Son cada vez más los autores que apuntan que, con el objetivo de apoyar esa plena independencia funcional que parece rezumar de la Ley española de Protección de Datos en favor de la Agencia de Protección de Datos, su financiación debería estar plenamente garantizada por la correspondiente partida presupuestaria.

En todo caso, la vía de los tribunales de justicia ordinarios siempre queda expedita y abierta para aquellos ciudadanos que piensen que la sanción impuesta por la autoridad administrativa competente no resulta ajustada a derecho, o que, simplemente, la observen desproporcionada.

Se suelen dar situaciones en la vida cotidiana de cualquier ciudadano en las que puede estar rozándose una posible infracción de la Ley de

[79] Ibídem, pág. 43.

Protección de Datos. Riesgo que aumenta en el caso de las relaciones comerciales y/o empresariales, como le puede ocurrir a un Medio de Comunicación Social en su voluntario aunque indeterminado contacto con el consumidor de su producto informativo, lector de periódico, oyente de radio o espectador de televisión.

Ateniéndonos a una visión del estado de cosas desde una perspectiva nacional, constatamos que la comunidad andaluza es la tercera por número de inspecciones de la Agencia Española de Protección de Datos y los sectores de banca y seguros y las compañías de telecomunicaciones acumulan el mayor número de quejas y expedientes por reclamaciones relacionadas con infracciones en materia de protección de datos[80].

Durante la celebración en abril de 2008 de unas jornadas sobre *'Protección de Datos. Riesgos y Límites*', organizada por la firma Marsh[81], fueron expuestas cifras que indican que los sectores más sensibles a la salvaguarda y cumplimiento de los preceptos de la normativa de Protección de Datos fueron, en el año 2007, el de Banca-Seguros y el de las Telecomunicaciones, puesto que abarcaron más de la mitad de las sanciones impuestas por la Agencia Española de Protección de Datos (34% y 23%, respectivamente), seguidos después, a bastante distancia, por las empresas de Distribución y Venta (9%), Solvencia Patrimonial y Crédito (5%) y Publicidad (5%)[82].

Los responsables de la consultora Marsh explican que, al igual que sucede en el resto del territorio nacional, las negligencias más comunes en Andalucía suelen estar relacionadas con errores tecnológicos, como fallos de los equipos y en la seguridad de los mismos; errores humanos, ya sea por falta de procedimientos internos o por falta de atención, o con actos

[80] 'Andalucía es la tercera comunidad por número de inspecciones de la Agencia Española de Protección de Datos', en "*Abc*", Sevilla, 3 de abril de 2008.

[81] Marsh es la primera firma mundial en Consultoría de Riesgos y Corretaje de Seguros. Su actividad la centra en crear soluciones a los riesgos y prestar servicios que contribuyan al crecimiento empresarial y éxito de sus clientes. Desde su fundación, en 1871, ha crecido hasta convertirse en una empresa que cuenta con más de 400 oficinas y 30.000 empleados con presencia en más de 100 países. Presta servicios globales de consultoría de riesgos, correduría de seguros, soluciones financieras y gestión de programas de seguros para empresas, organismos públicos, asociaciones, organizaciones de servicios profesionales y clientes particulares. Los ingresos anuales de Marsh superan actualmente los 5.000 millones de dólares.

[82] Véase: <http://www.marsh.es/press/arch/2008/np_020408.php>.

maliciosos de terceros, es decir, negligencias que vulneran varios de los preceptos principales que establece la normativa española reguladora de la Protección de Datos.

En este sentido, la compañía Legitec, otra de las consultoras especializadas que trabajan en este ámbito advierten que, en general, "*un adecuado cumplimiento de los requerimientos de la normativa en esta materia puede suponer una mejor gestión y control de los riesgos que asume la entidad ante la sociedad, el mercado, sus empleados y en sus responsabilidad ante la Agencia estatal*"[83]. Legitec es una de las primeras compañías que vienen trabajando en Sevilla en este ámbito[84].

Ante esta perspectiva, los especialistas insisten en advertir de la importancia y utilidad de contar con un seguro de Protección de Datos, ya que esta herramienta no sólo cubre las multas y sanciones impuestas por la Agencia estatal, sino también los daños a la imagen y las indemnizaciones por Responsabilidad Civil con las que puede ser castigada la empresa infractora, cuya cuantía puede ser muy superior a la sanción máxima fijada por la ley. Deben tenerse presente, además, otros seguros complementarios como el de Consejeros y Directivos, así como el que protege la infidelidad de empleados.

En este sentido, empieza a extenderse la comercialización de seguros para este fin, y ante la repercusión de las sanciones económicas, pero sólo resultan útiles si las empresas han comenzado a tomar medidas ante la normativa, un porcentaje que, aunque con grandes diferencias en función del tamaño y actividad de la empresa, en términos generales, se estima que en Andalucía no supera el 20 por ciento, parecido al que presenta la tendencia nacional.

Caso muy sonado ha sido la fuerte sanción impuesta desde lo más alto de la justicia española al programa de televisión '*Gran Hermano*'[85].

---

[83] Ibídem.

[84] Legitec es una organización de ámbito nacional, fundada e impulsada por varias empresas especializadas en ofrecer Servicios de Consultoría sobre Legislación del sector de las Nuevas Tecnologías. Ubicada en el Parque Científico y Tecnológico Cartuja 93 de Sevilla, ofrece servicios de Consultoría, Auditoría y Outsourcing en el ámbito de la Ley Orgánica de Protección de Datos de Carácter Personal, y de la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).

[85] El Supremo condena a la productora de Gran Hermano por utilizar ilegalmente datos de los participantes'. Teletipo de la "*Agencia Europa Press*", Madrid, 1 de mayo de 2007.

El Tribunal Supremo confirmaba en abril de 2007 la sanción de 1,08 millones de euros a Zeppelin Televisión S.A, la productora del programa *Gran Hermano*, impuesta por la Agencia Española de Protección de Datos por el tratamiento dado a la información de carácter personal de unos siete mil candidatos a participar en el espacio de televisión emitido por la cadena televisiva Telecinco. La sentencia STS 2778/2007[86] afirma que la productora recabó información relativa a gustos, ideología, creencias religiosas, raza, salud o vida sexual sin que existiera consentimiento de los candidatos para que estos datos se trataran en ficheros informáticos, es decir, automatizados[87]. Resulta que, encima, cedió los ficheros sin la debida seguridad a personas con las que no le unía ningún lazo contractual ni comercial.

El tribunal rechazó todas las alegaciones presentadas por Zeppelin Televisión S.A. contra la sanción, entre ellas las manifestaciones públicas realizadas por el director de la Agencia Española de Protección de Datos. Fue ésta última la institución que presentó la demanda contra la productora, sobre el expediente sancionador de forma previa a la sentencia. No obstante, el alto tribunal entiende, según la sentencia, que el Director no valoró, ni calificó, ni enjuició el procedimiento por lo que sus palabras carecieron de efectos respecto a la situación jurídica de la productora.

La productora llegó a alegar que había encargado la recogida de datos a una empresa[88], con la que firmó el correspondiente contrato y que, en su opinión, debería ser la única responsable de la recogida y tratamiento de los datos. Fue un intento de intentar desviar las culpas ante la inevitable fuerte sanción económica que le acechaba. La sentencia dejó claro que era la productora "*la beneficiaria del fichero y quien decidió la finalidad,*

---

[86] Disponible en la web del Poder Judicial español: <http://www.poderjudicial.es/search/documento/TS/503664/proteccion%20de%20datos%20de%20caracter%20personal/20070531>.

[87] El concepto de fichero automatizado, equivalente en la práctica al de fichero o relación de datos en soporte informático, trasciende con eficacia jurídica. La propia Ley de Protección de Datos de carácter personal 15/1999 así lo señala en su articulado. Es, por tanto, un concepto que debe tenerse en cuenta como objeto jurídico a considerar.

[88] Atento Telecomunicaciones España, fue la empresa que esgrimió la productora Zeppelin en sus argumentos defensivos.

contenido y uso del tratamiento de los datos personales de los aspirantes a concursantes, por lo que no ha podido eludir la responsabilidad"[89].

Establece en su sentencia el Tribunal Supremo que *"la participación en un programa, incluso en el de Gran Hermano, donde va a ser observado a través de las cámaras de televisión por millones de espectadores, no puede 'despojar' a un ciudadano de su derecho ala intimidad, porque su libertad sigue intacta y conserva el pleno derecho a que nadie trate, ceda o revele sus datos personales, aunque voluntariamente el mismo los haya facilitado para concursar*"[90].

La productora atribuía el tratamiento a otra empresa con la que firmó contrato, el gabinete de psicólogos García Huete & Cuadrado, y destacaba que los datos sensibles, es decir, los referentes a religión, raza o sexo, se trataron de forma automatizada. El Tribunal Supremo explicó en su fallo que "*también es necesario para el resto de datos el consentimiento de la persona que los proporciona, sin que pueda entenderse que éste se ha dado al ofrecer los titulares la información de forma voluntaria, haciendo evidente la incongruencia de hablar de un consentimiento tácito cuando ni siquiera se había producido la necesaria información a los titulares sobre la existencia del fichero*"[91].

El incumplimiento de la Ley de Protección de Datos trasciende a numerosos ámbitos y hasta los principales partidos políticos de nuestro país un incurrido, en el afán que les mueve en la captura de votantes, en infracciones durante la campaña electoral de las elecciones generales de 2008.

Según S. Parra, la iniciativa del Partido Popular consistente en poner en funcionamiento una página web donde cualquier interesado podía introducir su número de teléfono y su nombre para que recibiera una llamada con locución del candidato de esta formación y que, según lo difundido, desbordó las previsiones iniciales, lo que motivó la sustitución de la llamada telefónica que hacía el líder electoral por un simple e-mail. Al comprobar la observancia que se hizo de la Ley de Protección de Datos, puede extraerse la rápida conclusión de la comisión de cuatro infracciones,

[89] Sentencia referenciada en nota 83.

[90] Ibídem, pág. 4.

[91] Ib., pág. 10.

cuyas sanciones suponía elevar los costes a elevadísimas multas, puesto que podríamos estar hablando de unos 450.000 euros[92].

De una visita a la página web[93], y haciendo una inserción en la misma, Parra nos explica que "*tan sólo pedían dos datos, el nombre y la dirección de correo electrónico (con anterioridad, pedían el número de teléfono en lugar del mail). El nombre por sí sólo no es posible considerarlo un dato personal, ya que Juan o Pedro no identifican a nadie, pero sí la dirección de correo electrónico. Puede afirmarse, por tanto, que es un formulario que está recabando datos personales*"[94].

Lo mismo podría apuntarse de algunas iniciativas del PSOE, que también han incurrido en infracción. El ejemplo bien merece su conocimiento para evidenciar el hecho de que la normativa de protección de datos sigue siendo una auténtica desconocida no ya sólo en el mundo empresarial, sino también en el ámbito político.

Más fácil aún es que se pueda repetir con frecuencia una acción tan común pero que conlleva obligaciones ante la normativa de protección de datos, la de no tener un nombre de usuario y su contraseña como medidas de acceso y seguridad para unos ficheros con datos de carácter personal, que desde 2008 está siendo ya sancionada por la Agencia Española de Protección de Datos.

Ha sido el caso de un despacho de abogados[95], sancionado por incumplimiento de las medidas de seguridad que establece la normativa de nuestro país, tras la denuncia interpuesta por un particular, en la que, entre otras cosas, informaba que un abogado tenía una base de datos con los clientes de su despacho, sin las medidas de seguridad que exige la ley.

Personados los inspectores en este despacho profesional se comprobó que el denunciado disponía para el desempeño de su actividad

---

92 PARRA, Samuel: '*Protección de Datos Personales'*: <http://www.samuelparra.com/protecciondedatos/partidos_pol%C3%ADticos/>.

93 La página que estuvo en funcionamiento durante la campaña electoral por esta formación política fue: <http://www.tupropuestaen30segundos.com/>.

94 PARRA, S.: Op. cit.

95 Resolución R/00209/2008 de la Agencia Española de Protección de Datos, de 28 de febrero de 2008.

de un fichero automatizado que contenía datos relativos a nombre, apellidos y número de teléfono de sus clientes, y en algunos casos, dirección postal y/o electrónica y número de fax. Circunstancia ésta que puede haberle pasado a cualquier periódico de nuestro país por la tenencia de datos pertenecientes a sus suscriptores, por ejemplo.

Según aquella denuncia, el fichero del despacho de abogados no disponía de medidas de seguridad y, según constataron los inspectores actuantes, el acceso a la base de datos (o fichero) no se encontraba protegido mediante la introducción de un código o contraseña. Y es que, en efecto, tanto la regulación actual, esto es, el Real Decreto 1720/2007[96] como el ya derogado Real Decreto 994/1999, aún vigente en el momento de la denuncia, establecen la exigencia de disponer de este tipo de mecanismos informáticos, en concreto, el artículo 93 del RD 1720/2007 así lo indica[97].

Queda constatado, por tanto, que no sólo es obligatorio que exista, por ejemplo, una contraseña de acceso, sino que además, esa contraseña, por ley, debe ser cambiada y renovada cada año como máximo**,** o lo que es lo mismo, debe tener un periodo de caducidad de un año como máximo. Algo que también es desconocido por la mayoría de las empresas.

Siguiendo con el caso del abogado, éste alegó, entre otras cuestiones, que su oficina disponía de sistemas de alarma, puerta blindada, cerradura de seguridad, cerradura en el cuarto de archivo y seguridad en su despacho y que el sistema de información posee un antivirus. Algo que, seguramente, también tendrán la mayoría de los periódicos de nuestro país. Todo ello parece correcto, pero lo cierto es que la ley es muy clara en este

---

[96] B.O.E., núm. 17, de 19/1/2008, págs. 4103-4136.

[97] "*Artículo 93. Identificación y autenticación.*
1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible". (B.O.E., núm. 17, de 19/1/2008, pág. 4128).

sentido, si no hay un mecanismo que permita identificar y autenticar a los usuarios en el acceso a la información, estamos infringiendo el artículo 9 de la Ley Orgánica de Protección de Datos que establece el principio de seguridad.

El abogado denunciado disponía, curiosamente, de un Documento de Seguridad en el que se especificaban precisamente los mecanismos de identificación y autenticación de los usuarios, pero era sólo en teoría, porque en la realidad no era así, y suele ser éste otro de los grandes errores por parte de las empresas, creen incorrectamente que disponer de un Documento de Seguridad ajustado a la ley les hace cumplir con las exigencias de la normativa de la protección de datos.

Se resuelve finalmente determinar que el abogado había infringido el principio de seguridad de datos consagrado en el artículo 9 LOPD[98], pero que en atención de determinadas circunstancias (aplicando el 45.4 LOPD)[99], en vez de una multa de 60.000 euros, que hubiera sido lo normal, se le sanciona sólo con 600 euros. Puedo ser peor, y a muchos Medios de Comunicación les puede ocurrir lo mismo en cualquier momento.

Existe un gran desconocimiento respecto a las medidas de seguridad que un fichero con datos de carácter personal debe disponer, pensando sobre todo en las medidas de seguridad que el ordenamiento jurídico impone, no a las voluntarias o recomendables. Pocas son las empresas que las cumplen, y si hablamos de profesionales individuales, el grado de cumplimiento tiende a ser cero.

Si a este desconocimiento de la legislación le sumamos la poca concienciación que existe en el ámbito empresarial de entender que el activo más valioso para cualquier profesional son los datos de sus clientes, nos encontramos con que la mayoría de los sistemas de información no cumplen unos requisitos mínimos de seguridad, como los casos sobre la existencia de un mecanismo de identificación y autentificación, o lo que es lo mismo, de usuario y contraseña.

Ante una situación marcada por todas estas características, el camino emprendido puede encontrar numerosas dificultades y el cumplimiento de las normas reguladoras de la protección de datos personales se nos muestra disperso y repleto de lagunas. En el ámbito empresarial, en especial en el

98 B.O.E. Número 298, de 14/12/1999, op. cit., pág.43090.

99 Ibídem, pág. 43098.

ámbito de los Medios de Comunicación Social, la solución para afrontar las obligaciones legales en esta materia puede ofrecerla el consenso entorno a unas normas de funcionamiento y comportamientos ante los datos personales, elaborando los denominados Códigos Tipo.

3. NORMATIVA EN EL ÁMBITO DE ESTE DERECHO.

3.1. La Directiva 95/46 de la Unión Europea y el Convenio 108 del Consejo de Europa de 28 de enero de 1981.

La Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre, (LOPD) entró en vigor el 14 de enero de 2000, y vino a adaptar la legislación española a la Directiva 95/46/CE, del Parlamento europeo[100], 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.

Constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos.

La importancia de esta Directiva del Parlamento europeo es vital para entender toda la plasmación de sus preceptos en las legislaciones estatales comunitarias, entre ellas la española. El surgimiento de esta norma europea no fue sencillo.

En el intento de frenar los nuevos riesgos y amenazas que el rápido e imparable desarrollo de las nuevas tecnologías pudiera causar sobre el derecho de las personas, surgen hace ya más de cuarenta años, los primeros pasos legislativos en el ámbito de la Unión Europea[101].

Es en el año 1967 cuando, en el seno del Consejo de Europa, se constituyó una Comisión Consultiva para analizar las tecnologías de la información y su potencial agresividad a los derechos de los ciudadanos.

El Comité de Ministros del Consejo europeo dictaba años más tarde una serie de Resoluciones dirigidas a los Estados miembros de la entonces

[100] Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. Diario Oficial de las Comunidades Europeas, núm. L 281, de 23 de noviembre de 1995.

[101] DAVARA RODRÍGUEZ, M.: '*La Protección de Datos en Europa. Principios, Derecho y Procedimiento'*, Grupo Asnef Equifaz, Universidad Pontificia Comillas, Madrid, 1998, pág. 29 y ss.

Comunidad Económica Europea (CEE) recomendando la adopción de determinadas precauciones contra el abuso o el mal empleo de la informática como consecuencia de la creciente proliferación de bancos de datos tanto en el sector privado como en el sector público[102].

En la década de los años ochenta es cuando se comienza a tomar conciencia de la dimensión real de lo que se había configurado como un nuevo problema. En 1980 publica la OCDE[103] el destacado documento 'Líneas directrices tendentes a regular la protección de la vida privada y los flujos transfronterizos de carácter personal.

Un año más tarde, en 1981, es aprobado uno de los documentos que producen mayor repercusión en esta problemática, el Convenio 108 del Consejo de Europa[104] denominado 'Para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal'. Ratificado en primera instancia por cinco Estados: Alemania, España, Francia, Noruega y Suecia. A éstos se sumaron después Austria, Dinamarca, Irlanda, Luxemburgo, Reino Unido e Islandia.

El texto de este acuerdo de base legal, muy celebrado en su momento por el propio Consejo de Europa tras arduas negociaciones y esfuerzos, se propone soluciones en el intento de garantizar a toda persona física el respeto de sus derechos y libertades fundamentales, especialmente de su derecho a la vida privada respecto al tratamiento automatizado de los datos de carácter personal.

[102] Resoluciones 73(22), de 26 de diciembre de 1973 respecto a la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector privado y 74(29), de 20 de septiembre de 1974, respecto a la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público.

[103] Organización para la Cooperación y el Desarrollo Económico, constituida para la cooperación internacional, compuesta en la actualidad por treinta países, a fin de coordinar sus políticas económicas y sociales. Fue fundada en 1961 y su sede central se encuentra en la ciudad de París. Su antecesor fue la Organización Europea para la Cooperación Económica. La OCDE se ha constituido como uno de los foros mundiales más influyentes, en el que se analizan y se establecen orientaciones sobre temas de relevancia internacional como economía, educación y medioambiente.

[104] Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal. Estrasburgo, 28 de enero de 1981. B.O.E., núm. 274, Madrid, 15 de noviembre de 1981. No entró en vigor hasta el 1 de octubre de 1985.

El documento de la OCDE y el del Consejo de Europa supondrían notable influencia en aquellos años de proceso de formación de legislaciones comunes en el seno de la Europa que trabajaba por unirse en cada vez más cosas. Merced a ambos documentos se introducían conceptos y garantías básicas en materia de protección de las personas frente al uso de las nuevas tecnologías de la información que el mismo Convenio 108 obligaba a incorporar en su Derecho interno a los Estados que lo suscribieron, como puede leerse en el cuarto de sus artículos.

Fue, así las cosas, el primer texto internacional que permitió la armonización de las leyes de los diferentes Estados y, a la postre, el primer paso realmente decisivo en la elaboración de un armazón legislativo común en el ámbito de la protección de datos. El Convenio había sido modificado con fecha de 15 de junio de 1999 para permitir que se incorporaran a sus indicaciones las Comunidades Europeas[105].

El paso de los años no ha impedido que preceptos del Convenio 108 del Consejo de Europa hayan continuado teniendo plena vigencia. De hecho, su carácter flexible y adaptable al desarrollo y extensión de las nuevas tecnologías de la información ha hecho posible que muchos de sus principios sigan ostentando buena parte de su valor para la protección de los datos personales de los ciudadanos europeos. Hay artículos, como el 5 del Convenio, el referido a la calidad de los datos, que han sido trasladados prácticamente con la misma exactitud literal a preceptos de las leyes de los Estados de la Unión Europea, así como a normas de nivel comunitario.

El creciente desarrollo de las tecnologías de la información y las comunicaciones y, muy especialmente, la aparición de la telemática, además de todo ese amplio abanico de posibilidades que han obtenido en su actividad cotidiana los Medios de Comunicación Social, ha venido a plantear a los encargados de legislar nuevos retos que, en su momento, allá a inicios de los años ochenta, no habían podido ser previstos. El surgimiento de nuevos problemas en la transmisión y en el tratamiento de los datos personales llega a poner en cuestión la fiabilidad de las garantías aportadas por el Convenio 108 del Consejo de Europa y obliga, en determinados casos, al replanteamiento de algunos de los conceptos en él

[105] Modificación del Convenio para la protección de las personas en relación con el tratamiento automatizado de sus datos personales (ETS nº 108) permitiendo el acceso de las Comunidades Europeas (aprobado por el Comité de Ministros, en Estrasburgo, el 15 de junio de 1999). Disponible en la web de la Agencia de Protección de Datos: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.30-cp--MODIFICACI-OO-N-CONVENIO-N-1o--108.pdf>.

definidos. Nociones como la de 'fichero', 'responsable de fichero', o la propia noción de 'datos de carácter personal', han de ser analizadas con nuevos ojos a la luz de la rápida evolución protagonizada por la telemática.

Algún autor, como H. Campuzano Tomé, destaca, teniendo en cuenta todo ello, el modo en que se han concebido los tres conceptos citados hasta el momento[106]:

- "*La noción de fichero automatizado, que viene a sugerir una entrada y un tratamiento centralizado de los datos sin correspondencia ya con la nueva realidad de las tecnologías de la información y de los datos dispersos, que se pueden relacionar, si se quiere, mediante diálogos entre ordenadores y entre un terminal inteligente y un ordenador. En sentido contrario se plantea el problema de la 'evasión' en soporte papel de los datos más sensibles que, a menudo, se incluyen en expedientes no informatizados. Sería por ello deseable extender el campo de aplicación del Convenio a la recogida y utilización de datos contenidos en soporte papel. Se propone, pues que se amplíe la protección y que se extienda tanto a los datos automatizados como manuales.*

- *La noción de responsable del fichero, que se aplica difícilmente al marco de los servicios de correo electrónico, pues el contenido y el destino de los mensajes pertenecen a las personas que utilizan el servicio.*

- *La noción de datos de carácter personal, en el momento en que es lanzado el Convenio 108 a nivel europeo, y cuyo texto ofrece una definición más o menos flexible, puesto que se refiere a "cualquier información relativa a una persona física identificada o identificable" pero es preciso tener presente mentalmente que este concepto cubre ya nuevas posibilidades técnicas de tratamiento de las imágenes, el sonido y la voz, lo que conduce a una extensión considerable del campo de aplicación del Convenio 108, y en la que sus autores, responsables estatales de la Europa de inicios de los años ochenta, no pudieron pensar*".

En el año 2007 se celebró por primera vez el "Día Europeo de Protección de Datos", después de que en abril de 2006 el Comité de Ministros del Consejo de Europa estableciera esta celebración, con carácter

[106] CAMPUZANO TOMÉ, H. '*Vida privada y datos personales*: *su protección jurídica frente a la sociedad de la información*', Tecnos, Madrid, 2000.

anual en Europa, el día 28 de enero, conmemorando así el aniversario de la firma del Convenio 108 del Consejo de Europa[107].

Una manera de intentar perpetuar el espíritu del Convenio suscrito el 28 de enero de 1981 para garantizar en el territorio de cada Estado parte a cualquier persona física el derecho a la vida privada con respecto al tratamiento automatizado de los datos de carácter personal.

La Directiva 95/46/CE del Parlamento y del Consejo[108] supone, en su nacimiento, la proyección del reconocimiento y respeto de los derechos y libertades fundamentales de las personas físicas seguidos por las instituciones de la Unión Europea. Surge con el fin de garantizar la protección de los derechos y, en particular, la del derecho a la intimidad en lo referido al tratamiento de los datos personales, garantizando el principio comunitario de libre circulación de tales datos entre los Estados miembros de la Unión[109].

Fue en 1990 cuando, en realidad, nos encontramos con la primera propuesta de Directiva por parte de la Comisión Europea al Consejo, para la protección de datos dentro del contexto de las telecomunicaciones ámbito europeo, que sería luego, años más tarde, la Directiva 77/66/CE, del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones que, debido a los avances técnicos que se han ido produciendo, ha sido sustituida por una nueva Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección a la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Con posterioridad, ésta última ha sido modificada en algunos de sus aspectos por la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

---

[107] Más información respecto a lo que fue la celebración del primer Día Europeo en: <https://www.agpd.es/upload/Actividades/DiaEuropeoNotaAEPD.pdf>.

[108] Ibídem, pág. 53.

[109] Artículo 1.2 de la Directiva 95/46/CE: "*Los Estados Miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados Miembros por motivos relacionados con la protección garantizada en virtud del apartado 1*".

En septiembre de 1992, la Comisión elevó una nueva propuesta de Directiva al Consejo, después de un largo proceso en el que las autoridades de protección de datos de los Estados miembros no llegaban a una posición común. En el año 1995 se alcanza el consenso y es aprobado el documento.

La Directiva fija dos plazos de transposición de las medidas establecidas e indicadas al ordenamiento interno de los países miembros. Por un lado, dejaba un plazo de tres años para trasponer las medidas para los ficheros de datos de carácter personal automatizados, mientras que para los ficheros manuales que aún existieran (muchos en esas fechas) se colocaba un plazo de doce años, es decir, hasta 2007[110].

Es significativo lo que indica el Considerando 11 de la Directiva, al señalar que la norma precisa y amplía el principio del respeto a la intimidad que en su día fue incluido en el Convenio 1981 del Consejo de Europa[111].

La Directiva persigue, esencialmente, y de manera muy especial, que los Estados miembros de la Unión Europea apliquen unas medidas equivalentes para tutelar el respeto a la intimidad en el tratamiento automatizado de los datos de carácter personal.

Más que hacer aquí un análisis exhaustivo del articulado y preceptos que contiene esta crucial Directiva para la materia de nuestro estudio, nos basta con resaltar y comentar los aspectos más relevantes, porque es mucha la doctrina especializada y autorizada que ha profundizado sobre la norma desde una óptica precisa y exactamente jurídica[112].

---

[110] Memoria de la Agencia de Protección de Datos de 1995, disponible en: <https://212.170.242.196/portalweb/canaldocumentacion/memorias/memorias_2007/index-ides-idphp.php>.

[111] NAVALPOTRO NAVALPOTRO, Yolanda: '*Estudio Práctico sobre la Protección de Datos de Carácter Personal' .Capítulo I, Antecedentes de la Ley Orgánica 15/1999*. Lex Nova, Valladolid, 2007, pág. 37.

[112] DRESNER. S. H.: '*Panorama de la legislación europea sobre Protección de Datos Personales'. Informática y Derecho'*. Núms. 6 y 7, pág. 385 a 396. HEREDERO HIGUERAS. M.: '*La Directiva Comunitaria de Protección de Datos de Carácter Personal*'. Aranzadi. Pamplona, 1997. MANSILLA ARCOS, P.: '*El Derecho de Información en la Directiva 95/46 sobre Protección de Datos y su aplicación al sector asegurador*'. Actualidad Informática. Aranzadi. Núm. 25, octubre, 1997. MAÑAN PÁEZ. J.: '*Derecho comunitario y nuevas tecnologías: Libro Verde y Directivas de bases de datos. Jornadas sobre el Marco Legal y Deontológico de la Informática*'. Mérida. 16 a 20 de septiembre de 1997. VIGURY PEREA, A.:'I*ntimidad sobre Informática. La protección de datos personales: perspectiva desde el Derecho comparado*', La Ley, Abril de 1999.

La tendencia tradicional en Europa ha venido siendo que las normas de protección de datos se materialicen en la ley, lo que supone ni más ni menos que un soporte legal para poder sancionar sus incumplimientos, así como conceder a los ciudadanos, de otro lado, el derecho a la reparación del daño. Estas leyes incluyen, además, generalmente, mecanismos o procedimientos adicionales, como suelen ser el establecimiento de autoridades de control con funciones de seguimiento e investigación de denuncias. Ver, en este sentido, el Título IV de la propia Directiva 95/46/CE, relativo a la 'Autoridad de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales: artículo 28. Aspectos estos que se reflejan en las Disposiciones sobre responsabilidad, sanciones, recursos, autoridades de control y notificación, para lo que nos remitimos a los artículos 22, 23 y 24 de la norma comunitaria[113].

Si partimos, por tanto, de considerar lo determinante que ha de resultar, a nuestros efectos, contar con mecanismos de vigilancia de la aplicación de los objetos legales que defiende la norma, está claro que cualquier análisis significativo del panorama legislativo en materia de protección de datos debe comprender dos elementos básicos e imprescindibles: el contenido de las normas aplicables y los medios de garantizar su aplicación efectiva[114].

Teniendo en cuenta las disposiciones de otros textos internacionales sobre protección de datos y utilizando como base inicial la Directiva 95/46/CE, debe resultarnos posible alcanzar el núcleo del contenido de los principios de protección de datos y de los requisitos de aplicación y de procedimiento, cuyo cumplimiento debería considerarse como exigencia mínima para que la protección pueda observarse realmente eficaz.

Esa tutela efectiva ofrecida, normalmente, por los principios se lleva a cabo distinguiendo entre dos momentos fundamentales en la trayectoria vital del dato: el referido a la captura o recolección y el momento propiamente en que se lleva a cabo el tratamiento o procesamiento del dato.

Sobre el instante de la colecta o captación, nos situamos en el ámbito de lo que en los textos aparece bajo la denominación de 'calidad del dato'.

---

[113] Diario Oficial de las Comunidades Europeas, núm. 281, de 23 de noviembre de 1995, págs. 31-50. Disponible en la página web española del Boletín Oficial del Estado: <http://www.boe.es/doue/1995/281/L00031-00050.pdf>.

[114] CAMPUZANO TOMÉ, H.: Op. Cit., pág. 82.

Siguiendo a Herminia Campuzano Tomé[115], hay aquí una serie de principios que han de observarse en lo referente a qué tipo de datos puede captarse o tomarse. Cabe enumerar, al respecto, los siguientes principios generales para el momento de la recogida del dato:

- "*Principio de justificación legal y social. Supone la existencia de un propósito socialmente aceptado que legitime la extracción del dato, enmarcado dentro de los usos generalmente aceptados.*

- *Principio de licitud y limitación de la captación. Se trata de que se utilicen medios específicamente acotados y líticos para la captación del dato, lo que viene a suponer conocimiento y consentimiento del titular o bien autorización legal. Los medios empleados en la captación no podrán, por tanto, ser fraudulentos, desleales o ilícitos, debiendo especificarse los mismos con el propósito de evitar generalidades o vaguedades que puedan hacer todo más proclive a la desviación. Existe asimismo otro perfil en la consideración de este principio, como es el procurar la extracción mínima de datos personales. Únicamente los estrictamente necesarios para cumplir la finalidad perseguida. No deben ser, por tanto, excesivos, evitando recoger aquellos datos innecesarios.*

- *Principio de fidelidad de la información. Los datos han de ser completos, exactos y actuales. No desvirtuarlos. Para cumplir con este propósito de la fidelidad del dato a tratar se consagra la figura de la rectificación y actualización, no solamente como derechos de los titulares de los datos, sino, además, como obligación de los responsables de los archivos.*

- *Principio de pertinencia y finalidad. La recogida del dato de carácter personal debe circunscribirse a aquellos datos que sean adecuados al propósito perseguido en su obtención. De ahí que serán guardados en los archivos respectivos con el único objeto de utilizarlos para la finalidad de la misma. Igualmente, su revelación y eventual difusión no deberán ser incompatibles con esta finalidad*"[116].

A estos principios que hemos de considerar generales y que deben observarse en el instante de la recogida, acompañan otros que, tal y como

[115] Ibídem, pág. 83.

[116] Ib., pág. 83.

sostiene Campuzano Tomé[117] y aquí resumimos, protegen al dato personal en el momento del tratamiento o procesamiento. Son los siguientes:

- ✓ "*Principio de confidencialidad de los datos recogidos. Aquí, en general, es admitido que las personas que trabajan con los archivos de este tipo tienen la obligación del secreto profesional.*

- ✓ *Principio de seguridad. Como una obligación a cargo del responsable del fichero, que serán quien deba adoptar las medidas técnicas y organizativas indispensables para garantizar este aspecto, evitando alteraciones, pérdidas, tratamientos, o accesos no autorizados. Hay un amplio aspecto de medidas concretas a considerar en este terreno, que pasan por la protección del acceso a los locales donde están los equipos de tratamiento de los datos, hasta llegar a la protección lógica de los propios programas contra posibles errores de manipulación o accesos no autorizados.*

- ✓ *Principio de caducidad. Los datos personales no deben tratarse ni mantenerse archivados más allá del tiempo necesario para cumplir con su finalidad. En este sentido, la cancelación supone un correlativo 'derecho al olvido' propio del concepto de libertad informática. Para poder garantizarlo es necesario que se borre por completo el dato del soporte que lo contenga, impidiendo su regeneración por cualquier otra vía o medio. Este principio tendrá una repercusión muy importante en la práctica pues se trata de delimitar el tiempo por el que pueden retenerse o conservarse los datos personales que han sido recabados.*

- ✓ *Principio de consentimiento del afectado. Posiblemente, la piedra angular del derecho de la protección de datos desde el punto de vista del titular de los mismos. Uno de los principios básicos sobre los que se articula la mayor parte de los sistemas generales de protección de datos de carácter personal. Supone un derecho de información, que resulta aplicable en todo proceso de recogida o extracción, tratamiento, disposición y archivo del dato personal, y que constituye todo un deber para quien pretenda recabar el dato*".

El juego jurídico práctico de estos principios enumerados, tanto en el momento la recogida del dato como en el momento del tratamiento, viene a conformar un principio de sentido más amplio y que también encuentra reconocimiento legal en los textos normativos, como es el llamado 'principio de autodeterminación informativa', que otorga al titular del dato

[117] Ib., pág. 85.

una serie de derechos como consecuencia de tal condición, a fin de poder permitirle 'autotutelar su propia identidad', puesta en práctica en las numerosas operaciones de registro informático que, para diversos fines, es sometida la persona durante el transcurso de su vida.

Principios y garantías que aparecen consagrados de manera reiterada en los textos normativas reguladores de la protección de datos y que reconoce, desde luego, la Directiva 95/46 y que, en definitiva, son los que servirán de base legal para la conformación de los mecanismos necesarios de protección de tales datos frente a la compleja e inmensa Sociedad de Información[118].

La doctrina es unánime al considerar que esta Directiva comunitaria europea es de vital importancia jurídica, pues que ha venido a introducir, entre otras cosas, como afirma Campuzano[119], una serie de nuevos parámetros:

- ✓ "*Establece medidas aplicables tanto para ficheros automatizados como para ficheros manuales*
- ✓ *Amplía el concepto de dato de carácter personal incluyendo dentro del mismo la imagen y el sonido*
- ✓ *Se contempla la posibilidad de solicitar el ejercicio de un nuevo derecho como es el derecho de oposición*
- ✓ *La posibilidad de que los países establezcan las excepciones necesarias para conciliar el derecho a la intimidad con la libertad de expresión*
- ✓ *Los datos sindicales también serán datos especialmente protegidos*
- ✓ *Creación una nueva figura: el encargado del tratamiento*".

La Directiva establece que los principios incluidos en su contenido serán de aplicación a todos los tratamientos de datos personales cuando el responsable de tratamiento de datos o fichero con la información desarrolle su actividad dentro del ámbito de aplicación del Derecho Comunitario.

---

[118] Tal y como establece el artículo 5 de la Directiva 95/46/CE: "*Los Estados Miembros precisarán, dentro de los límites de las disposiciones del presente Capítulo, las condiciones en que son lícitos los tratamientos de datos personales*". Y tenor literal, igualmente, de los siguientes artículos.

[119] CAMPUZANO TOMÉ, H.: Op. Cit., pág. 87.

Indica, además, que dentro de ese ámbito de aplicación, quedarán excluidos los tratamientos efectuados como resultados de actividades exclusivamente personales o domésticas, tratamiento relativos a seguridad pública, defensa, seguridad del Estado y actividades estatales en el ámbito penal, así como el tratamiento de datos necesario para la salvaguarda del bienestar económico cuando el referido tratamiento esté relacionado con la seguridad del Estado. Esto derivará luego en normativa específica al margen de la Ley española de Protección de Datos de 1999.

El cambio fundamental que introduce la Directiva en la legislación es la protección de la información personal y personalizada a cualquier dato o información concerniente a una persona física identificada o identificable, cualquiera que sea la forma o modalidad de su obtención, conservación o tratamiento. Se amplía de esta manera el ámbito de protección[120].

Junto a esta serie de aspectos, la Directiva consideró otros nuevos que fueron incluidos en cada una de la normativa de los diferentes Estados integrantes de la Unión Europea. En España, la transición de la normativa se hizo fuera de plazo puesto que finalizaba oficialmente el 25 de octubre de 1998. Se tardó algo más de un año, pero llegó.

Si la Directiva no se aplica, pueden entrar en juego las normas nacionales de protección de datos. De conformidad con lo establecido en su artículo 34, los destinatarios de la Directiva son los Estados miembros. Fuera del ámbito de aplicación de la Directiva, los Estados miembros no están sujetos a las obligaciones que ésta impone, básicamente, adoptar las disposiciones legales, reglamentarias y administrativas necesarias para darle cumplimiento. Sin embargo, como el Tribunal de Justicia de las Comunidades Europeas ha dejado claro, nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a la Directiva a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de Derecho comunitario se oponga a ello. Por consiguiente, puede perfectamente suceder que determinadas situaciones en las que no se puede hablar de tratamiento de datos personales en el sentido de la Directiva, estén, sin embargo, sujetas a medidas protectoras con arreglo al Derecho nacional. Éste puede aplicarse, por ejemplo, a un tema como el de los datos cifrados, independientemente de que se trate de datos personales o no.

[120] VELEIRO, Belén: *Protección de Datos de Carácter Personal y Sociedad de la Información*. Estudios Jurídicos, Ministerio de la Presidencia, Madrid, 2008, pág. 37.

En aquellos casos en que las normas de protección de datos no se apliquen, determinadas actividades pueden infringir el artículo 8 del Convenio Europeo de Derechos Humanos y Libertades Fundamentales[121], que protege el derecho a la vida privada y familiar, de acuerdo con la jurisprudencia de mayor alcance del Tribunal Europeo de Derechos Humanos. Otros conjuntos de normas, como el Derecho de daños, el Derecho penal o las leyes contra la discriminación, pueden también ofrecer protección a las personas físicas en los casos en que las normas de protección de datos no sean aplicables y estén en juego intereses legítimos

3.1.2. Grupo de Trabajo del artículo 29 de la Directiva.

El Grupo de Trabajo se creó en virtud del propio artículo 29 de la Directiva 95/46/CE. Se trata del órgano consultivo independiente de la UE sobre protección de los datos personales y la vida privada de los ciudadanos. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE. La secretaría pertenece a la Dirección C (Justicia Civil, Derechos fundamentales y Ciudadanía) de la Comisión Europea, Dirección General de Justicia, Libertad y Seguridad, y tiene su sede en Bruselas[122].

Es en su primer Informe anual, en 1997, cuando lanza un documento[123] en el que recuerda su conformación y lanza sus primeras directrices en la materia a nivel comunitario que, precisamente, inciden y relacionan directamente la protección de datos y los Medios de Comunicación social.

Está compuesto por representantes de las autoridades nacionales independientes responsables de la protección de datos, un representante de la Comisión, e incluirá un representante de las autoridades de las Instituciones Europeas responsables de la protección de datos, a medida y en el momento en que se creen estas autoridades. Al poner en común la capacidad colectiva de las autoridades nacionales, el Grupo fomentará un enfoque coherente en la aplicación de los amplios principios de la Directiva

---

[121] B.O.E., núm. 243, de 10/10/1979, pág. 23564.

[122] Sitio web: <http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm>.

[123] Disponible en:
<https://www.agpd.es/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/1997/common/pdfs/Primer-informe-anual.pdf>.

y asesorará a la Comisión sobre aspectos relativos a la protección de datos. En especial, deberá dar su opinión respecto del nivel de protección en la Unión y en países terceros, y puede hacer recomendaciones sobre todos los aspectos relativos a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

El Grupo de Expertos, como se le conoce, se reunió por primera vez el 17 de enero de 1996, como relató en su segundo informe anual[124]. Los trabajos se iniciaron bien pronto por la petición de las autoridades nacionales responsables de la protección de datos. Peter J. Hustinx, presidente de la autoridad neerlandesa de protección de datos (*Registratiekamer*) fue elegido el primer presidente del Grupo. Louise Cadoux, miembro de la autoridad francesa de protección de datos (*Commission Nationale de l'Informatique et des Libertés*) fue elegida vicepresidenta. El Grupo se reunió en cuatro ocasiones en 1996. Los debates se centraron en las transferencias de datos hacia países terceros y el nivel de protección en dichos países, en los procedimientos de notificación, en las excepciones a las normas sobre protección de datos y en la aplicación de la ley de protección de datos a los medios de comunicación, a la luz del requisito de la directiva de encontrar un equilibrio entre la libertad de expresión y el derecho a la vida privada. Poco después, aprueba una Recomendación sobre este asunto tan controvertido ya en 1997.

3.1.2.1. La Recomendación 1/97 sobre Medios de Comunicación.

Es la Recomendación 1/97[125], de 25 de febrero de 1997, la que el Grupo de Trabajo dedica a la normativa sobre protección de datos y medios de comunicación. En ella aborda la colisión de intereses que se dan entre la libertad de expresión y la protección de la intimidad, dos derechos fundamentales en cuyo cruce da caminos se dan toda una variedad de situaciones que ha de analizarse caso por caso.

---

[124] Disponible en:
<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp14_es.pdf>, pág.4.

[125] Documento WP1 (XV/5012/97), véase en:
<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp1_en.pdf>.

Lo que afirma el Grupo de Expertos es que, tomando como base el artículo 9 de la Directiva 95/46/CE[126], la normativa reguladora de la protección de datos de carácter personal es aplicable a los Medios de Comunicación y su actividad[127].

Para concluir esa afirmación, de gran relevancia jurídica y proyección posterior en toda la normativa que ha ido desencadenando la Directiva comunitaria en las legislaciones estatales, entre ellas la de España y, por consiguiente, la sujeción a todo ese tipo de normas de los Medios de Comunicación Social de nuestro país, el Grupo de Expertos lo que hace es analizar en su Recomendación los aspectos generales que sustancian la base legal de la libertad de expresión y de la protección de la intimidad, dos derechos que entran en colisión permanente.

En este sentido, recuerda en el texto recomendante que el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales (CEDH)[128] establece que "*Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras*". Se trata de uno de los derechos humanos fundamentales, emana de las tradiciones constitucionales que comparten los Estados miembros y es uno de los elementos más característicos del patrimonio jurídico de las sociedades democráticas.

Históricamente, fue uno de los primeros derechos humanos en ser reclamados y, fehacientemente, garantizados en Derecho. Fue precisamente la prensa la que recibió garantías legales y constitucionales específicas, especialmente contra la censura previa.

Indica la Recomendación que hacen los expertos en 1997 que, de modo análogo, el derecho a la intimidad está garantizado por el artículo 8 del CEDH. La protección de datos se encuadra dentro de la protección de

[126] El artículo 9 de la Directiva 95/46/CE dispone lo siguiente: "*En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con lasnormas que rigen la libertad de expresión*".

[127] El subrayado es nuestro.

[128] B.O.E., núm. 243, 10/10/1979, págs. 23564-23570.

la vida privada garantizada en el marco de dicho artículo. Las excepciones a los principios de protección de datos y al artículo 8 del CEDH han de estar en consonancia con la legislación en vigor y respetar el principio de proporcionalidad[129].

Del mismo modo, los límites a la libertad de expresión, tales como los que puedan surgir de la aplicación de los principios de protección de datos, también han de ser conformes a derecho y respetar el principio de proporcionalidad[130]. No obstante, no se ha de considerar que los dos derechos fundamentales entran en conflicto de forma inherente. Si no se garantiza adecuadamente su intimidad, cabe la posibilidad de que las personas físicas se muestren reacias a expresar sus ideas. De modo análogo, resalta a nuestros efectos la afirmación que hace el Grupo de Expertos al señalar que resultará probable que la identificación y la descripción del perfil de los lectores y usuarios de los servicios de información reduzca el deseo de las personas físicas de recibir o difundir información.

La importancia que tiene el artículo 9 de la Directiva 95/46/CE hace que el Grupo de Expertos recuerde, en sus argumentaciones de la Recomendación, cuáles son los antecedentes legales de este precepto tan determinante, y reseña que, de conformidad con lo dispuesto en el Tratado de la Unión Europea, que ha dejado redactado de la siguiente manera el nuevo artículo 6, tras la aprobación del Tratado de Lisboa[131]: "*los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales*". El legislador comunitario ha reconocido el caso específico que constituyen los Medios de Comunicación y la necesidad de lograr un equilibrio entre la protección de la intimidad y la libertad de expresión[132].

---

[129] Por ejemplo, Tribunal Europeo de Derechos Humanos (TEDH), *Sunday Times*, Serie A, nº 30.

[130] Véase, T.E.D.H., *Goodwin/Reino Unido*, 27/03/1996.

[131] Ley Orgánica 1/2008, de 30 de julio, por la que se autoriza la ratificación por España del Tratado de Lisboa, por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, firmado en la capital portuguesa el 13 de diciembre de 2007. B.O.E., núm. 184, de 31/07/2008, pág. 32919.

[132] La necesidad de lograr un equilibrio entre los intereses protegidos por estos dos conjuntos de normas también se había reconocido en el Convenio 108/81 ("el Convenio"). Su informe explicativo (*Informe explicativo sobre el Convenio para la*

El artículo 19 de la propuesta[133] inicial de la Comisión establecía que los Estados miembros podían conceder excepciones a lo dispuesto en la Directiva para la prensa y los medios audiovisuales de comunicación. El informe explicativo aclaraba que la característica básica de este artículo es la obligación de lograr un equilibrio entre los intereses en juego y que dicho equilibrio puede tener en cuenta la disponibilidad de otras medidas de reparación o de un derecho de réplica, la existencia de un código de ética profesional, los límites establecidos por el TEDH y los principios generales del derecho. El artículo 9 de la propuesta modificada de la Comisión[134] estableció la obligatoriedad de la concesión de excepciones para los medios de comunicación. El texto se modificó también con objeto de incluir a los periodistas y de limitar las excepciones a las actividades periodísticas. Fue modificado posteriormente hasta quedar establecido en su redacción actual de forma que las excepciones no puedan aplicarse indiscriminadamente a todas las disposiciones de protección de datos.

En el texto actual, es evidente que las excepciones son de obligado cumplimiento, aunque "*sólo si son necesarias*", es decir, que sólo se han de conceder las excepciones a cada principio específico de la Directiva en la medida en que sean necesarias (en la versión francesa "*dans la seule mesure où*", o en la alemana "*nur insofern vor, als sich dies als notwendig erweist*") para lograr un equilibrio entre la defensa de la intimidad y la libertad de expresión. Por otra parte, estas excepciones sólo podrán referirse a las normas generales sobre la licitud del tratamiento de datos, las normas sobre la transferencia de datos a terceros países y las relativas a la autoridad de control. Con arreglo al '*considerando 37*' de la Directiva 95/46[135], no se podrán aplicar excepciones a las normas de seguridad y se

protección de las personas físicas con relación al tratamiento automático de datos personales, Consejo de Europa, Estrasburgo, 1991) incluye a la libertad de expresión como uno de *"los derechos y libertades de los demás*" para cuya protección los legisladores nacionales, de conformidad con lo dispuesto en la letra b) del apartado 2 del artículo 9 del Convenio, pueden apartarse de los principios básicos de la protección de datos.

[133] COM (90) 314 final - SYN 287.

[134] COM (92) 422 final - SYN 287.

[135] "*Considerando que para el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la*

deberá dotar a las autoridades de control responsables de este sector de, al menos, determinados poderes *a posteriori*, tales como la facultad de publicar informes periódicos o de remitir determinadas cuestiones a las autoridades judiciales.

Con independencia de la normativa de cada Estado, y de si aplica cada uno más o menos excepciones a los medios en el ámbito de la protección de datos personales, el Grupo de Expertos estima que, al margen de las diferencias, en la mayoría de los casos, el régimen de excepción expresa que pueda haber, la normativa de protección de datos no se aplica plenamente a los medios de comunicación como consecuencia de la situación constitucional especial de las normas relativas a la libertad de expresión y de prensa. Estas normas limitan *de facto* la aplicación de las disposiciones sustantivas de protección de datos o, al menos, su cumplimiento efectivo.

La importancia de estas consideraciones lleva a establecer al Grupo de Expertos comunitarios en su Recomendación 1/97[136], que "*el régimen normal de protección de datos se aplica, por regla general, a las actividades no editoriales llevadas a cabo por los Medios de Comunicación. A la hora de aplicar la normativa relativa a la protección de datos, las autoridades de control reconocen las particularidades de los Medios de Comunicación, tanto si existe un régimen normativo especial como si no. Por otra parte, el alcance efectivo de las excepciones no puede analizarse en términos abstractos, sino que depende de la estructura global de la normativa de protección de datos de cada país específico. Es evidente que la magnitud de las excepciones requeridas depende de la*

persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; que por lo tanto, para ponderar estos derechos fundamentales, corresponde a los Estados miembros prever las excepciones y las restricciones necesarias en lo relativo a las medidas generales sobre la legalidad del tratamiento de datos, las medidas sobre la transferencia de datos a terceros países y las competencias de las autoridades de control sin que esto deba inducir, sin embargo, a los Estados miembros a prever excepciones a las medidas que garanticen la seguridad del tratamiento; que, igualmente, debería concederse a la autoridad de control responsable en la materia al menos una serie de competencias a posteriori como por ejemplo publicar periódicamente un informe al respecto o bien iniciar procedimientos legales ante las autoridades judiciales". Véase en la página web de normativa comunitaria: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML>.

[136] Documento WP1 (XV/5012/97), op. cit.

medida en que las normas sustantivas tengan realmente relación con las actividades de los medios"[137].

Sobre la aplicación de la normativa de protección de datos a los Medios de Comunicación, la Recomendación 1/97 hace alusión al empleo de la tecnología, cada vez más, por parte de los Medios de Comunicación y al hecho de que se haya desplazado la actividad y el interés hacia el concepto de tratamiento, lo que lleva a un contexto en que "*los Medios de Comunicación, o al menos la prensa, están obligados a respetar determinadas normas que, aunque no forman parte de la normativa relativa a la protección de datos en sentido estricto, contribuyen a la protección de la intimidad de los individuos. Esta normativa y la a menudo más que abundante jurisprudencia existente en la materia han generado formas específicas de resarcimiento que a menudo se considera que suplen la ausencia de medidas cautelares de resarcimiento en el marco de la normativa de protección de datos*"[138].

Agrega que, a la hora de evaluar cómo se protege la intimidad del ataque de los Medios de Comunicación, se ha de tener en cuenta el derecho de réplica y la posibilidad de rectificar informaciones incorrectas, las obligaciones profesionales de los periodistas y los procedimientos autorregulatorios especiales (como estudiaremos en nuestro estudio en el Capítulo 12, sobre los Códigos Tipo).

La evolución de los Medios tradicionales hacia la publicación electrónica y la prestación de servicios en línea (on line) viene a proponer nuevos elementos para la reflexión, según sugiere en ese momento (año 1997) el Grupo comunitario de Expertos en la materia[139].

La Recomendación deja sentado algo tan relevante como que la distinción entre actividades editoriales y no editoriales aporta nuevas dimensiones en relación con los servicios en línea que, al contrario que todos los medios tradicionales, permite identificar a los beneficiarios de los servicios.

[137] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/1997/common/pdfs/Recomendaci-oo-n-1-97.pdf>, pág. 7.

[138] Ibídem, pág. 7.

[139] Ib., pág. 8.

En sus conclusiones, lo que afirma el Grupo de Expertos, en un momento de cierta incertidumbre en los legisladores de los países integrantes de la Unión Europea poco después de haberse publicado, con todas sus obligaciones, la Directiva 95/46/CE, es que resulta necesario que en cada Estado miembro se lleve a cabo una reevaluación general del marco jurídico para la aplicación a los medios de comunicación de la normativa relativa a la protección de datos. A este respecto, dice el Grupo de Expertos de manera concluyente que se ha de evaluar en qué medida es preciso limitar la aplicación de las disposiciones de los capítulos II, IV y VI de la Directiva, con objeto de proteger la libertad de expresión.

La Recomendación 1/97[140] deja establecido que, para ello, tal y como recoge, han de tenerse en cuenta una serie de elementos. En tal sentido, afirma, en primer lugar, que la normativa relativa a la protección de datos se aplica, en principio, a los Medios de Comunicación. "*Sólo cabe la posibilidad de conceder excepciones y exenciones en relación con el capítulo II, sobre las medidas generales relativas a la licitud del tratamiento de datos, el capítulo IV, sobre las transferencias de datos a terceros países, y el capítulo VI, sobre los poderes de las autoridades de control. No se podrán conceder excepciones o exenciones en relación con las disposiciones sobre seguridad. En cualquier caso, las autoridades de control responsables de este sector habrán de mantener determinadas atribuciones a posteriori*".

A continuación, establece que las excepciones y exenciones contempladas en el artículo 9 de la Directiva comunitaria reguladora de la protección de datos, han de ajustarse al principio de proporcionalidad, y acota que sólo se podría limitar la libertad de expresión en la medida en que sea necesario.

Deja entrever que "*cabe la posibilidad de que no sean necesarias las excepciones y exenciones contempladas en el artículo 9 en el caso de que la flexibilidad de varias disposiciones de la Directiva o las excepciones otorgadas en el marco de otras disposiciones específicas (que, evidentemente, también se han de interpretar de forma estricta) ya haga posible que exista un equilibrio entre la defensa de la intimidad y la libertad de expresión*"[141]. Y remarca, a continuación, con una evidente

[140] Ib., pág. 8.

[141] Por ejemplo, a la hora de analizar si se han de conceder exenciones a la aplicación del artículo 11, es decir, la obligada información que hay que proporcionar cuando los datos no han sido recabados del propio interesado, se ha de considerar que no se está

perspectiva claramente abierta que "*el artículo 9 de la Directiva respeta el derecho de las personas físicas a expresarse libremente. No se pueden conceder excepciones o exenciones con arreglo a lo dispuesto en el artículo 9 a los Medios de Comunicación Social o a los periodistas, como tales, sino a quienes traten datos con fines periodísticos"*.

Las consideraciones establecidas en esta interesante norma comunitaria maneja ya en 1997 la posibilidad, hoy cada vez más imperante, de otras formas de difusión de la información, redactando que "*es posible que las excepciones y exenciones abarquen exclusivamente al tratamiento de datos con fines periodísticos (editoriales), entre los que se incluye la publicación electrónica. Cualquier otra forma de tratamiento de datos por parte de los periodistas o los medios de comunicación está sujeta a las normas ordinarias de la Directiva. Esta distinción es especialmente relevante en relación con la publicación electrónica. El tratamiento de los datos de los suscriptores a efectos de facturación o el tratamiento con fines de marketing directo (incluido el tratamiento de datos de los Medios de Comunicación Social a efectos de establecer perfiles de la clientela) se encuadran en el ámbito de aplicación del régimen normal de protección de datos*"[142].

Recuerda, con vocación de hacer confluir derechos sin desvirtuar uno por otro, que la Directiva exige que se establezca un equilibrio entre dos libertades fundamentales, estableciendo que "*con el fin de determinar si las limitaciones de los derechos y obligaciones emanados de la Directiva guardan proporción con el objetivo de proteger la libertad de expresión, se debería prestar especial atención a las garantías específicas de que gozan las personas físicas en relación con los medios de comunicación. Las limitaciones al derecho de acceso y rectificación con anterioridad a la publicación sólo podrían ser proporcionales en la medida en que las personas físicas gozasen del derecho de réplica o a que se rectifiquen las informaciones falsas que se hayan publicado. Las personas físicas tendrán derecho, en cualquier caso, a formas adecuadas de resarcimiento en caso de que se violen sus derechos*"[143].

---

obligado a informar a los individuos a los que se refieren los datos siempre y cuando ello implique un esfuerzo desproporcionado.

[142] <https://www.agpd.es/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/1997/common/pdfs/Recomendaci-oo-n-1-97.pdf>, pág. 9.

[143] Ibídem, pág. 9.

Pero lo más importante y de mayor calado lo afirma al finalizar su cuarto recomendante, al considerar el Grupo de Expertos comunitarios sobre la protección de datos y la libertad de expresión que "*a la hora de evaluar si las excepciones o exenciones son proporcionales, se ha de prestar atención a la ética y a las obligaciones profesionales de los periodistas, así como a las formas autorregulatorias de control establecidas por la profesión*"[144].

Es aquí donde todavía falta camino por recorrer en todo el campo de actuación de los Medios de Comunicación Social españoles en atención al respeto de las normas esenciales y los derechos fundamentales de las personas.

3.1.2.2. Sobre la definición legal de 'Datos Personales'.

El Grupo de trabajo lanza el Dictamen 4/2007[145] sobre el concepto de datos personales para ofrecer una serie de orientaciones sobre cómo debe entenderse y aplicarse el concepto de datos personales de la Directiva 95/46/CE y de la legislación comunitaria adoptada en aplicación de la misma en diversas situaciones.

En términos generales, señala el Dictamen, se ha estimado que el legislador europeo se propuso adoptar un concepto amplio de datos personales, aunque ese concepto no es ilimitado. Nunca hay que olvidar, indica este documento del Grupo de expertos europeos, que el objetivo de las disposiciones de la Directiva es proteger los derechos y libertades fundamentales individuales, en especial el derecho a la intimidad, en lo que se refiere al tratamiento de datos personales. Por ello, estas normas se concibieron para ser aplicadas en situaciones en las que los derechos individuales pueden correr peligro y, por tanto, necesitar protección.

El ámbito de aplicación de las normas de protección de datos no debe llevarse a su extremo, pero también debe evitarse una limitación indebida del concepto de datos personales. La Directiva ha definido su ámbito de aplicación, excluyendo diversas actividades, y permite cierta flexibilidad al aplicar las normas a las actividades que entran en su ámbito de aplicación. Las autoridades de protección de datos desempeñan una

---

144 Ib., pág. 9.

145 Véase: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf>.

misión fundamental en la búsqueda de una aplicación equilibrada de las mismas.

El análisis del Grupo de trabajo se ilustra con ejemplos extraídos de las prácticas de las autoridades nacionales encargadas de la supervisión de la protección de datos y se basa en los cuatro «*componentes*» principales que pueden distinguirse en la definición de «datos personales», esto es: «*toda información*», «*sobre*», «*identificada o identificable*» y «*persona física*». Estos cuatro componentes están estrechamente ligados y se complementan entre sí, pero juntos determinan si una determinada información debe ser considerada como «*datos personales*»[146].

Para el Grupo europeo de protección de datos, la expresión «toda *información*» utilizada en la Directiva indica claramente la voluntad del legislador de dar un sentido amplio al concepto «*datos personales*». Esta redacción exige una interpretación amplia.

Desde el punto de vista de la naturaleza de la información, el concepto de datos personales incluye todo tipo de afirmaciones sobre una persona. Por consiguiente, abarca información «*objetiva*» como, por ejemplo, la presencia de determinada sustancia en su sangre, pero también informaciones, opiniones o evaluaciones «*subjetivas*». Esta última clase de afirmaciones constituye una parte considerable del caudal de datos personales tratados en sectores como el de la banca, para evaluar la fiabilidad de los prestatarios («*Fulano es un prestatario fiable*»), el asegurador («*no se espera que Fulano muera pronto*») o el laboral («*Fulano es un buen trabajador y merece un ascenso*»).

Para que esas informaciones se consideren «*datos personales*», no es necesario que sean verídicas o estén probadas[147]. De hecho, las normas de protección de datos prevén la posibilidad de que la información sea incorrecta y confieren al interesado el derecho de acceder a esa información y de refutarla a través de los medios que ofrece la legislación.

Desde el punto de vista del contenido de la información, el concepto de datos personales incluye todos aquellos datos que proporcionan información cualquiera que sea la clase de ésta. Por supuesto, esto incluye la información personal considerada «*datos sensibles*» en el artículo 8 de la Directiva a causa de su naturaleza particularmente delicada, pero también otras categorías más generales de información.

---

146 Ibídem, pág. 6.

147 Ib., pág.7.

El término «datos personales» comprende la información relativa a la vida privada y familiar del individuo stricto sensu, pero también la información sobre cualquier tipo de activad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o social. El concepto de «datos personales» abarca, por lo tanto, información sobre las personas, con independencia de su posición o capacidad (como consumidor, paciente, trabajador por cuenta ajena, cliente, etc.). De ahí que los Medios de Comunicación, al estar incidiendo permanentemente en este tipo de información, deban atender con cuidado y minuciosidad lo establecido en la Directiva y en la ley española.

Hay que considerar, por una parte, y esto concierne muy directamente a quienes tratan y gestionan información, que el concepto de vida privada y familiar es sumamente amplio, tal como el Tribunal Europeo de Derechos Humanos dejó claro[148]. De otro lado, las normas sobre protección de datos personales van más allá de la protección del amplio concepto del derecho al respeto de la vida privada y familiar.

Cabe señalar que, en su artículo 8, la Carta de los Derechos Fundamentales de la Unión Europea consagra la protección de los datos de carácter personal como un derecho autónomo, separado y diferente del derecho al respeto de la vida privada, mencionado en su artículo 7, y lo mismo sucede en algunos Estados miembros[149].

---

[148] Sentencia del Tribunal Europeo de Derechos Humanos en el asunto Amann/Suiza de 16.2.2000, apartado 65: «[…] el término" vida privada" no debe interpretarse restrictivamente. En especial, el respeto por la vida privada comprende el derecho a establecer y a desarrollar relaciones con otros seres humanos; además, no hay ninguna razón de principio que justifique la exclusión de actividades de una naturaleza de profesional o empresarial de la noción de la "vida privada" (véase al Niemietz v. Sentencia de Alemania del 16 de diciembre de 1992, serie A no. 251- B, pags. 33-34, § 29, y la sentencia Halford, pags. 1015-16, § 42). Esa interpretación amplia se corresponde con la del convenio del Consejo de Europa de 28 de enero de 1981 […]»

[149] La Carta de los Derechos Fundamentales reconoce una serie de derechos personales, civiles, políticos, económicos y sociales de los ciudadanos y residentes de la UE, consagrándolos en la legislación comunitaria. Elaborada por una convención compuesta por un representante de cada país de la UE y de la Comisión Europea, así como por miembros del Parlamento Europeo y de los Parlamentos nacionales. Fue formalmente proclamada en Niza en diciembre de 2000 por el Parlamento Europeo, el Consejo y la Comisión. En diciembre de 2009, con la entrada en vigor del Tratado de Lisboa, la Carta adquirió el mismo carácter jurídico vinculante que los Tratados. A tal efecto, había sido enmendada y proclamada por segunda vez en diciembre de 2007.
<http://europa.eu/legislation_summaries/justice_freedom_security/combating_discrimination/l33501_es.htm>

Esto se ajusta a los términos del artículo 1, apartado 1, de la Directiva, dirigido a la protección de «las libertades y los derechos fundamentales de las personas físicas y, en particular [pero no exclusivamente] del derecho a la intimidad». Por consiguiente, la Directiva hace una referencia concreta al tratamiento de los datos personales en ámbitos distintos del hogar y de la familia, como el del Derecho laboral [artículo 8, apartado 2, letra b)], las condenas penales, las sanciones administrativas o las sentencias en procesos civiles (artículo 8, apartado 5) o la prospección [artículo 14, letra b)]. El Tribunal de Justicia de las Comunidades Europeas ha refrendado este enfoque amplio.

Desde el punto de vista del formato o el soporte en que la información está contenida, señala el Dictamen 4/2007 que "*el concepto de datos personales incluye la información disponible en cualquier forma, alfabética, numérica, gráfica, fotográfica o sonora, por ejemplo. Desde este punto de vista, el concepto incluye la información conservada en papel, así como la información almacenada en una memoria de ordenador, utilizando un código binario, o en una cinta de video, por ejemplo. Se trata de una consecuencia lógica de la inclusión en su ámbito de aplicación del tratamiento automático de datos personales*"[150].

En particular, los datos que consisten en sonidos e imágenes están calificados como datos personales desde este punto de vista, en la medida en que pueden contener información sobre una persona. A este respecto, la referencia particular a los datos consistentes en sonidos e imágenes del artículo 33 de la Directiva debe ser entendida como la confirmación de que esta clase de datos entra en efecto en su ámbito de aplicación (siempre y cuando se cumplan las restantes condiciones) y de que la Directiva se aplica a ellos. De hecho, esto entra dentro de la lógica de este artículo que intenta evaluar si las normas de la Directiva proporcionan respuestas legales apropiadas en esos ámbitos. Esto queda aún más claro en el considerando 14, en el que se afirma que «*considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos*».

Por otra parte, y según expresa el citado Dictamen comunitario "*para que la información sea considerada como datos personales no es necesario*

---

[150] < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf>, pág. 8.

que esté recogida en una base de datos o en un fichero estructurado. También la información contenida en un texto libre en un documento electrónico puede calificarse como datos personales, siempre que se cumplan los otros criterios de la definición de datos personales. El correo electrónico, por ejemplo, contiene datos personales"[151].

Ilustra todo ello el Grupo europeo de trabajo en su Dictamen 4/2007 con ejemplos gráficos: en videovigilancia, las imágenes de personas obtenidas por medio de un sistema de vigilancia por vídeo pueden considerarse datos personales en la medida en que esas personas sean reconocibles. En banca telefónica, en aquellas operaciones en las que la voz del cliente que da instrucciones al banco se graba con una cinta, esas instrucciones grabadas deben ser consideradas como datos personales.

En este punto, cabe hacer una referencia especial a los datos biométricos. "*Estos datos pueden definirse como propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad. Ejemplos típicos de datos biométricos son los que proporcionan las huellas dactilares, los modelos retinales, la estructura facial, y las voces. Aunque también la geometría de la mano, e incluso determinada habilidad profundamente arraigada u otra característica del comportamiento (como la caligrafía, una manera particular de hablar, etc.)*"[152].

Una particularidad de los datos biométricos es que se les puede considerar tanto como contenido de la información sobre una determinada persona (Fulano tiene estas huellas dactilares) como un elemento para vincular una información a una determinada persona (este objeto lo ha tocado alguien que tiene estas huellas dactilares y estas huellas dactilares corresponden a Fulano; por lo tanto Fulano ha tocado este objeto). Como tales, pueden servir de 'identificadores'.

Respecto a la componente de persona 'identificada o identificable', el Dictamen 4/2007 del Grupo europeo del art. 29 establece que, "*de modo general, se puede considerar «identificada» a una persona física cuando, dentro de un grupo de personas, se la «distingue» de todos los demás miembros del grupo. Por consiguiente, la persona física es «identificable»*

[151] Ibídem, pág. 8.

[152] Ib., pág. 9.

cuando, aunque no se la haya identificado todavía, sea posible hacerlo (que es el significado del sufijo «ble»)"[153].

La identificación se logra normalmente a través de datos concretos que podemos llamar «*identificadores*» y que guardan una relación privilegiada y muy cercana con una determinada persona. Cabe citar como ejemplos su apariencia exterior, es decir su altura, el color del cabello, la ropa, etc. o una cualidad de la persona que no puede percibirse inmediatamente, como su profesión, el cargo que ocupa, su nombre, etc.

La Directiva menciona esos «*identificadores*» en la definición de «datos personales» del artículo 2 cuando establece que «*se declarará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*»[154].

Esta idea se aclara aún más en los comentarios a los artículos de la propuesta modificada de la Comisión, en donde se afirma que «*una persona puede ser identificada directamente por su nombre y apellidos o indirectamente por un número de teléfono, la matrícula de un coche, un número de seguridad social, un número de pasaporte o por una combinación de criterios significativos (edad, empleo, domicilio, etc.), que haga posible su identificación al estrecharse el grupo al que pertenece*.»

Los términos de esta declaración indican claramente que el que determinados identificadores se consideren suficientes para lograr la identificación es algo que depende del contexto de la situación de que se trate. Un apellido muy común no bastará para identificar a una persona, es decir, para aislarla, dentro del conjunto de la población de un país, mientras que es probable que permita la identificación de un alumno dentro de una clase. Incluso una información auxiliar, como, por ejemplo, «el hombre que lleva un traje negro», puede identificar a alguno de los transeúntes que esperan en un semáforo. Así pues, el que se identifique o no a la persona a la que se refiere una información depende de las circunstancias concretas del caso[155].

---

153 Ib., pág.13.

154 Diario Oficial de la Unión Europea, núm. 281, de 23/11/1995, pág. 31.

.

155 El Dictamen 4/2007 comunitario marca de esta manera una clara apreciación acerca del apellido y el nombre de una persona, que pueden no bastar para convertirse en dato de carácter personal, pese a lo que pueda pensarse a priori con cierta generalidad. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf>, pág. 14

Añade, sobre esto, en lo que se refiere a la expresión personas «directamente» identificadas o identificables, que "*el nombre y apellidos de una persona es efectivamente el identificador más común y, en la práctica, el concepto de «persona identificada» implica muy a menudo una referencia a sus apellidos. En algunas ocasiones, para establecer con toda certeza esta identidad, hay que combinar el nombre y apellidos de la persona con otros datos (fecha de nacimiento, nombres de los padres, dirección o una fotografía de su rostro) para evitar toda confusión con otras personas del mismo nombre y apellidos. Por ejemplo, puede considerarse que la información de que Fulano debe una cierta suma de dinero hace referencia a una persona identificada porque está ligada al nombre y apellidos de esa persona*"[156].

Amplía, posteriormente, estas apreciaciones el Dictamen 4/2007 comunitario al describir que "*el nombre y apellidos de una persona es una información que revela que ésta utiliza esa combinación de letras y sonidos para identificarse y para que la identifiquen otras personas con las que establece relaciones. El nombre y apellidos de una persona también pueden ser el punto de partida para obtener información sobre el lugar en el que vive o se la puede encontrar, o sobre sus familiares (a través de sus apellidos) y sobre toda una serie de relaciones jurídicas y sociales vinculadas a ese nombre y apellidos (expediente académico, expediente médico, cuentas bancarias, etc.). Se puede incluso conocer la apariencia física de la persona si su fotografía se asocia con su nombre y apellidos. Todos estos nuevos datos ligados al nombre y apellidos nos permiten centrarnos en un individuo de carne y hueso. Así pues, a través de los identificadores la información original se asocia con una persona física que puede ser distinguida de otros individuos*"[157].

El contexto en el que se incluye a una persona y su caracterización es otro de los elementos que puede definir un dato personal, sin tener que acudir al nombre ni al apellido de esa persona, merced a la posibilidad de combinar circunstancias. Lo explica de la siguiente manera: "*En los casos en que, a primera vista, los identificadores disponibles no permiten singularizar a una persona determinada, ésta aún puede ser «identificable», porque esa información combinada con otros datos (tanto si el responsable de su tratamiento tiene conocimiento de ellos como si no) permitirá distinguir a esa persona de otras. Aquí es donde la Directiva se refiere a «uno o varios elementos específicos, característicos de su*

---

156 Ibídem, pág. 14.

157 Ib, pág. 14.

identidad física, fisiológica, psíquica, económica, cultural o social». Algunas de esas características son tan únicas que permiten identificar a una persona sin esfuerzo (el «actual Presidente del Gobierno de España »), pero una combinación de detalles pertenecientes a distintas categorías (edad, origen regional, etc.) también puede ser lo bastante concluyente en algunas circunstancias, en especial si se tiene acceso a información adicional de determinado tipo. Este fenómeno ha sido estudiado ampliamente por los estadísticos, siempre dispuestos a evitar cualquier quebrantamiento de la confidencialidad"[158].

El Grupo comunitario de Expertos recoge expresamente en el texto del Dictamen 4/2007 'el ejemplo de la información dispersa en la Prensa'. Se trata del caso número 10 del texto literal del Dictamen[159]: "*Se publica un artículo de prensa sobre un antiguo asunto penal que en su día suscitó mucho interés. En este artículo no se da ninguno de los identificadores tradicionales, en especial ni la identidad ni el lugar de nacimiento de ninguna de las personas involucradas. No parece excesivamente difícil obtener información adicional que nos permita descubrir cuáles son las personas más directamente implicadas en el asunto, por ejemplo, echando un vistazo a la prensa de la época en que se desarrollaron los acontecimientos. De hecho, no es inconcebible que alguien consulte los periódicos de la época o dé otros pasos que muy probablemente le proporcionen los nombres u otros identificadores de las personas a las que veladamente se hace referencia en el artículo. Por lo tanto, parece justificado considerar el tipo de información al que se hace referencia en este ejemplo como «información sobre personas identificables» y, por tanto, como «datos personales»*". Lo que convierte esta aseveración en un indudable axioma que despeja cualquier tipo de dudas acerca de las informaciones que se publican sobre personas de las que se vuelcan suficientes detalles que vislumbran su personalidad e identidad sin necesidad de escribir ni decir sus nombres y apellidos. Informaciones dispersas en la prensa y Medios de Comunicación en general que, al fin y al cabo, están difundiendo datos personales. A menudo ocurre que, el paso del tiempo puede variar esas circunstancias que vinculan a una persona, y que pueden quedar indexadas en un sitio web pese a que hayan cambiado y la relación hechos-persona ya no tenga sentido, lo que daría lugar a la

158 Ib., pág. 15.

159 Ib., pág. 15.

posibilidad del ejercicio de derecho cancelación, o 'derecho al olvido', que abordaremos en siguientes Capítulos[160].

Aclara el texto normativo que aborda la definición que, llegado a este punto, "*si bien la identificación a través del nombre y apellidos es en la práctica lo más habitual, esa información puede no ser necesaria en todos los casos para identificar a una persona. Así puede suceder cuando se utilizan otros «identificadores» para singularizar a alguien. Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones. Sin ni siquiera solicitar el nombre y la dirección de la persona es posible incluirla en una categoría, sobre la base de criterios socioeconómicos, psicológicos, filosóficos o de otro tipo, y atribuirle determinadas decisiones puesto que el punto de contacto del individuo (un ordenador) hace innecesario conocer su identidad en sentido estricto. En otras palabras, la posibilidad de identificar a una persona ya no equivale necesariamente a la capacidad de poder llegar a conocer su nombre y apellidos. La definición de datos personales refleja este hecho*"[161].

El Tribunal de Justicia de las Comunidades Europeas se ha pronunciado en ese sentido al considerar que "*la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un tratamiento de datos personales en el sentido del artículo 3, apartado 1, de la Directiva 95/46*"[162].

3.1.3. Directivas 97/66/CE y 2002/58/CE del Parlamento Europeo y del Consejo.

Antes de ir desgranando más Directivas, dejar constancia de que la elevada atención que prestamos a la normativa comunitaria en este ámbito, como pudiera ser si nos refiriésemos a otras parcelas, no obedece a otra cosa que a la primacía del Derecho Comunitario que emana de las instituciones europeas sobre el Derecho interno estatal español. Esta

[160] El derecho de cancelación, uno de los cuatro que reserva Ley española de Protección de Datos al ciudadano titular de los datos, y que recoge en el artículo 16 de la LOPD. B.O.E., núm. 298, de 14 diciembre 1999, pág. 43091.

[161] Dictamen 4/2007: Op. cit., pág. 15.

[162] Ibídem, pág. 16.

primacía se da en nuestro país, como en el resto de Estados que componen la Unión Europea, en esa estructura tan magna y cada vez más compleja pero que, según algún teórico del Derecho Comunitario, como afirma J.P. Jacqué, "*está siguiendo en todo momento un sentido pragmático de organización*"[163].

La necesidad de adecuar la normativa sobre protección de datos a los cambios que se estaban produciendo en el sector de las telecomunicaciones llevó al legislador comunitario a elaborar, pocos años después, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[164] (Directiva sobre la privacidad y las comunicaciones electrónicas). La nueva Directiva sustituye y deroga a la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre, relativa al tratamiento de los datos personales y a la protección de la intimidad en sector de las telecomunicaciones.

La Directiva 2002/58/CE[165] tiene por objeto establecer y garantizar un alto nivel de protección de los datos personales de los abonados y usuarios de los servicios de comunicaciones electrónicas, al tiempo que hace respetar el principio de 'neutralidad tecnológica'.

El ámbito de protección conferido por esta Directiva, al igual que ya ocurría con la Directiva 97/66/CE, es el del tratamiento de los datos personales en redes públicas de comunicaciones electrónicas. Aunque toca tangencialmente a la actividad de los Medios de Comunicación, es conveniente tenerla en consideración como marco sectorial de lo que aquí tratamos, debido además al asentamiento que hace de determinados conceptos importantes para cualquier titular de datos de carácter personal.

Además, la Directiva 2002/58/CE es la norma específica sobre protección de datos en el sector de las comunicaciones electrónicas, que complementa a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en los que respecta al tratamiento de los datos personales y a la libre

[163] JACQUÉ Jean-Paul: *Droit institutionnel de l'Union européenne.* Dalloz, Parution, 2006, pág. 313.

[164] Diario Oficial de las Comunidades Europeas, L 201/37, de 31/07/2002. Véase: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:>.

[165] Ibídem.

circulación de estos datos, que es la norma general aplicable a todas aquellas cuestiones que no queden cubiertas por la Directiva específica. La analizaremos con mucho más detalle en el Capítulo 3.5 de nuestro estudio.

3.2. La Ley Orgánica española de Protección de Datos Personales de 1999.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)[166] es producto de la transposición de la Directiva 95/46/CE a nuestro ordenamiento jurídico y ya desde el comienzo de su aprobación y publicación extendió un gran número de conceptos jurídicos indeterminados, lo que plantea problemas de interpretación[167].

Vino a derogar y sustituir a la Ley 5/1992 Orgánica de Regulación de Tratamiento Automatizado de Datos de Carácter Personal[168], que supuso la primera norma en regular los datos personales en España, y que permaneció vigente durante siete años.

La Ley 15/1999 fue aprobada con la pretensión final de ser el principal instrumento para impedir que, por un mal uso de las nuevas tecnologías de la información y las comunicaciones que, imparables, han ido abriéndose camino en nuestra sociedad, las personas puedan sufrir graves perjuicios en sus derechos.

La LOPD consta de siete títulos, cuarenta y nueve artículos, seis disposiciones adicionales, tres disposiciones transitorias y tres disposiciones finales, sin que cuente con una exposición de motivos.

Con esta nueva LOPD aparecen una serie de nuevos aspectos que no habían sido recogidos en su antecesora, la Ley Orgánica sobre Regulación del Tratamiento Automatizado de Datos de Carácter Personal, 5/1992, de 29 de octubre, que sin embargo fue objeto de numerosas y fuertes críticas porque evidenciaba notable diferencias entre el tratamiento conferido a los

166 B.O.E., núm. 298, de 14/12/1999, pág. 43088.

167 VELEIRO, Belén: '*Protección de Datos de Carácter Personal y Sociedad de la Información'*, op. cit., pág. 38.

168 B.O.E., núm. 262, de 31/10/1992, pág. 37037.

ficheros privados con respecto al que se otorgaba a los ficheros de carácter público, que se vieron mucho más favorecidos.

Los nuevos aspectos que introduce la LOPD vigente pasan por la ampliación del objeto de la Ley, ya que se incluyen los ficheros manuales estructurados, en opinión de Yolanda Navalpotro, quien indica que "*la Directiva comunitaria no sólo persigue la protección de la intimidad y de los derechos y libertades de los titulares de los datos, sino también el respeto a las libertades y derechos fundamentales de las personas físicas y, en especial, de su intimidad. Con todo esto se pretende evitar que, a través del conocimiento de aspectos personales de un individuo, se vulneren sus derechos fundamentales*"[169].

3.2.1. Ámbito de aplicación y definiciones.

La LOPD amplió su campo de acción al reducir el número de ficheros que quedaban fuera del ámbito de aplicación de la normativa relativa a protección de datos personales, ampliando por tanto el área de influencia de sus preceptos.

El ámbito geográfico de aplicación de la norma no sólo afecta a los tratamientos que tengan lugar en territorio español y cuyo responsable éste establecido en algún punto de España, sino que también afecta la Ley a los casos en que el responsable del tratamiento no esté establecido en territorio español pero sí sea objeto de aplicación de la legislación española en virtud de las normas de Derecho Internacional Público.

Es de aplicación esta LOPD también en caso de que el responsable no esté situado en territorio español o de la Unión Europea pero utilice para el tratamiento medios situados en el territorio de nuestro país, a excepción sólo de que sean utilizados con fines de tránsito. Concibe exactamente el artículo 3 de la Ley el dato personal como "*cualquier información concerniente a personas físicas identificadas o identificables*"[170].

Sobre esto, conviene decir antes que nada que al referirse la LOPD a "*personas identificadas e identificables*", está abriendo la posibilidad de aplicación de esta norma a datos que pueden identificar, hoy por hoy, a una persona sin excesivas dificultades técnicas, como son los correos

[169] NAVALPOTRO NAVALPOTRO, Yolanda: '*Estudio Práctico sobre la Protección de Datos de Carácter Personal'*, op. cit., pág. 45.

[170] B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43088.

electrónicos o el número de teléfono. Así como datos como los genéticos o los biométricos, que están siendo utilizados y presentes en esta vida cotidiana sofisticada caca vez más.

3.2.1.1. El e-mail como dato personal.

Las dudas sobre si la dirección de correo electrónico es un dato de carácter personal que requiere toda su cobertura legal han quedado resueltas. A pesar de no pocos debates y pareceres encontrados.

Son lógicamente planteadas las dudas por el hecho de que la dirección electrónica se forma por un conjunto de signos o palabras que la diferencian de las demás, configurándose mediante dos parámetros, el denominado 'login', que se elige y designa por el usuario de la dirección de correo electrónico, y el denominado 'nombre de dominio', designado por la empresa o empresas que prestan el servicio de correo electrónico, y que se precede siempre con el símbolo 'arroba' [@], que coincide con el nombre de dominio de Internet de la página web de la empresa prestadora del servicio de correo[171].

Este último componente, el nombre de dominio, ha sido objeto de regulación mediante la Orden del Ministerio de Fomento del 21 de marzo de 2000 por la que se regula el sistema de asignación de nombres de dominio de Internet bajo el código de país correspondiente a España, en nuestro caso '*.es*'[172].

Se impone como único límite en la determinación de la dirección electrónica para designar el 'login' es que no exista otra dirección idéntica correspondiente a otro titular, prestada en el mismo dominio. En la selección de la dirección electrónica se pueden elegir tanto combinaciones que no contengan significado alguno, como que lo contengan, incluso también el nombre de la persona o algún otro dato identificativo.

En todo caso, el problema de la calificación de la dirección electrónica como dato de carácter personal no se plantea respecto del caso de que esté referida a una persona identificada o identificable, vinculándola a un manejo o tratamiento al titular identificado, según la definición de dato personal del artículo 3 de la LOPD, esto es, cuando se realiza un

---

[171] APARICIO SALOM, J.: *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Editorial Aranzadi, Elcano, Navarra. 2000, pág. 43.

[172] B.O.E., núm. 77, de 30/03/2000, pág. 13342.

listado de direcciones y de las personas a quienes corresponde, sino por la consideración de que, cuando el distintivo personal de la dirección, el 'login', está formado por el nombre del titular, esta circunstancia puede determinar que tenga la naturaleza de dato personal sin necesidad de vinculación, puesto que en este caso la dirección está formada por medio de la identidad.

En el caso de que la dirección electrónica se componga de modo tal que no revele la identidad de aquel a quien corresponde, cuando no tenga significado alguno o el significado no sea identificativo, pueden caber dudas sobre su consideración como dato personal.

En este sentido, la Agencia Española de Protección de Datos ya emitió en 1999 un Informe Jurídico[173], al planteársele si la venta o cesión de un fichero que contenga direcciones de correo electrónico ha de ser considerada como cesión de datos a los efectos de la Ley, lo que exigía analizar el concepto establecido en el artículo 3.a) de la LOPD. Dejó sentado el citado Informe "*que la dirección de correo electrónico se forma por un conjunto de signos o palabras libremente elegidos generalmente por su titular, con la única limitación de que dicha dirección no coincida con la correspondiente a otra persona. Esta combinación podrá tener significado en sí misma o carecer del mismo, pudiendo incluso, en principio, coincidir con el nombre de otra persona distinta de la del titular*", de ahí que tengamos dos supuestos esenciales de dirección de correo electrónico, atendiendo al grado de identificación que la misma realiza con el titular de la cuenta de correo, y que describe el Informe Jurídico de la Agencia Española de Protección de Datos de la siguiente manera:

"*a) El primero de ellos se refiere a aquellos supuestos en que voluntaria o involuntariamente la dirección de correo electrónico contenga información acerca de su titular, pudiendo esta información referirse tanto a su nombre y apellidos como a la empresa en que trabaja o su país de residencia (aparezcan o no estos en la denominación del dominio utilizado). En este supuesto, no existe duda de que la dirección de correo electrónico identifica, incluso de forma directa al titular de la cuenta, por lo que en todo caso ha de ser considerada la dirección electrónica como dato de carácter personal. Ejemplos característicos de*

[173] Informe Jurídico de la Agencia Española de Protección de Datos sobre la dirección de correo electrónico, accesible en su página web: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/1999-0000_Direcci-oo-n-de-correo-electr-oo-nico.pdf>.

este supuesto serían aquellos en los que se hace constar como dirección de correo electrónico el nombre y, en su caso, los apellidos del titular (o sus iniciales), correspondiéndose el dominio de primer nivel con el propio del país en que se lleva a cabo la actividad y el dominio de segundo nivel con la empresa en que se prestan los servicios (pudiendo incluso así delimitarse el centro de trabajo en que se realiza la prestación).

b) Un segundo supuesto sería aquel en que, en principio, la dirección de correo electrónico no parece mostrar datos relacionados con la persona titular de la cuenta (por referirse, por ejemplo, el código de la cuenta de correo a una denominación abstracta o a una simple combinación alfanumérica sin significado alguno)"[174].

Parece evidente, dicho así, que no cabría dudas de que el correo electrónico es un dato de carácter personal, pero se hace obligado vislumbrar más allá. Como explica el citado Informe Jurídico, al añadir que, "*incluso en este supuesto, la dirección de correo electrónico aparecerá necesariamente referenciada a un dominio concreto, de tal forma que podrá procederse a la identificación del titular mediante la consulta del servidor en que se gestione dicho dominio, sin que ello pueda considerarse que lleve aparejado un esfuerzo desproporcionado por parte de quien procede a la identificación. Por todo ello, se considera que también en este caso, y en aras a asegurar, en los términos establecidos por la jurisprudencia de nuestro Tribunal Constitucional, la máxima garantía de los Derechos Fundamentales de las personas, entre los que se encuentra el derecho a la "privacidad", consagrado por el artículo 18.4 de la Constitución, será necesario que la dirección de correo electrónico, en las circunstancias expuestas, se encuentre amparada por el régimen establecido en la LOPD*", concluye el citado Informe de la Agencia[175].

Por tanto, y teniendo en cuenta estas consideraciones, cabe afirmar que la dirección electrónica es un dato personal cuando se personaliza. El código de singularización de la dirección tendrá el carácter de dato personal según la forma que éste adopte por voluntad de su titular, no en atención a su naturaleza propia.

En opinión de J. Aparicio Salom, la naturaleza jurídica del e-mail dependerá no del acto de asociación a la identidad del titular por parte del responsable del tratamiento, sino de la forma en que se haya determinado la

[174] Ibídem, pág. 1.

[175] Ib., pág. 2.

dirección por parte del usuario de la misma. Sin embargo, y como el e-mail puede adoptar cualquier forma, sin contenido o con algún significado, sostiene Aparicio, "*no debe entenderse siempre y de manera automática que la información que pueda desprenderse de la dirección electrónica pueda tener carácter de dato personal. Tengamos en cuenta que la identificación que resulta de ella puede ser la del titular o la de cualquier otra persona distinta, pues no hay norma que prohíba la utilización de nombres ajenos o distintos al del titular*"[176].

La dirección electrónica sólo tendrá el carácter de dato personal cuando se vincule, por medio de un tratamiento o manejo efectuado por el responsable, a la persona titular de la misma, es decir, cuando el tratamiento suponga la vinculación de la identidad del afectado a la dirección electrónica.

Transcurridos numerosos debates doctrinales sobre esta cuestión, podemos concretar que, en la actualidad, está ya claramente asentada la idea de que el e-mail es un dato de carácter personal. Algunos autores, como Castañeda González, coinciden en afirmar que "*la composición de la dirección de correo electrónico está formada por un conjunto de signos o palabras diferenciadores, y puesto que el concepto de dato personal establecido por la LOPD requiere la concurrencia de un doble elemento, por un lado, la existencia de un dato e información, y, por otro, la vinculación del dato o la información a una persona física identificada o identificable, en el caso de las direcciones de correo electrónico, en la medida en que las palabras o signos que la formen permitan su vinculación directa o indirecta con una persona física, la convierte en dato personal*"[177].

Hay pronunciamientos de la justicia española al respecto. La Audiencia Nacional ha establecido en una sentencia de 2006 que la dirección de correo electrónico es un dato de carácter personal aunque en la composición de la leyenda inicial de la dirección no apareciera el nombre y apellidos del titular, "*ya que se trata de una información que concierne a la persona física, que le afecta y que forma parte del ámbito de intimidad protegido por la LOPD*"[178].

---

[176] APARICIO SALOM, J.: Op. cit., pág. 45.

[177] CASTAÑEDA GONZÁLEZ, A. y AA.VV.: *Guía práctica de Protección de Datos de Carácter Personal*, Ediciones Experiencia, Barcelona, 2002, pág. 26.

[178] Sentencia de la Audiencia Nacional, Sección 1ª, de 22 de febrero de 2006. Recurso 911/03.

3.2.1.2. Los datos biométricos (la huella cibernética).

Los datos biométricos son aquellos que se refieren a determinados aspectos físicos que, mediante un análisis técnico, permite distinguir ciertas singularidades que se dan en los aspectos analizados y que, resultando imposible la coincidencia de dos individuos, permiten servir para identificar a la persona en cuestión. Por ahora, han sido poco o casi nada utilizados por los Medios de Comunicación social, pero conviene tener bien en cuenta su naturaleza jurídica ya de antemano porque van a ser elemento objeto de cuestión en el futuro más próximo.

El uso de los datos biométricos permite garantizar que quien se identifica mediante un medio electrónico de control capaz de emplear tales recursos es, sin lugar a dudas, la persona que dice ser, de modo que se otorga una efectividad absoluta a los sistemas automáticos de control del acceso a dependencias o sistemas informáticos, frente a la inseguridad que existe en el caso de uso de los sistemas tradicionales e identificación, como los números o códigos secretos de carácter personal, las tarjetas con bandas magnéticas únicas, etc., que se presentan más sujetas a esa inseguridad que deriva de su probable robo o falsificación[179].

No obstante la exactitud del sistema y el hecho de que algunos de ellos puedan utilizarse en investigaciones policiales, lo cierto es que el procesado de datos biométricos y su vinculación con la identidad de los ciudadanos no tiene mayor trascendencia respecto de la intimidad que los métodos de personalización más tradicionales y menos exactos que se emplearon con anterioridad, puesto que no revelan nada de la personalidad del individuo, salvo ADN. Por ello, la obtención y el uso de datos biométricos para identificar a las personas no tiene por qué considerarse, en sí, como un sistema que altere los medios tradicionales, con la salvedad ya comentada de las pruebas biológicas.

En consecuencia, al no tener ninguna información adicional, el tratamiento de los datos biométricos no parece que, por sí, el artículo 4.1 de la Ley Orgánica de Protección de Datos, que establece que los datos sometidos al tratamiento automatizado no debe ser excesivos en relación con el ámbito y las finalidades legítimas para las que se han obtenido, sino que la eventual infracción de dicho principio dependerá de la finalidad del tratamiento y la adecuación de esos datos a la obtención de finalidad.

---

[179] APARICIO SALOM, J.: Op., cit., pág. 55.

La huella digital es, en la actualidad, el dato biométrico más utilizado. Se planteó a la Agencia de Protección de Datos por un Ayuntamiento la posibilidad de tratamiento automatizado de la huella digital para la comprobación de la identidad de los funcionarios al servicio de la Corporación y el cumplimiento por los mismos de su jornada de trabajo. La cuestión a resolver era determinar si la huella digital podía considerarse dato personal y, en caso de serlo, si se encuentra sometida a algún tipo de regla especial. Planteándose en el mismo caso si el empleador puede tratar la huella sin consentimiento de los empleados.

Entendió la Agencia que "*los datos biométricos tienen la condición de datos de carácter personal y que, dado que los mismos, no contienen ningún aspecto concreto de la personalidad, limitando su función a identificar a un sujeto cuando la información se vincula con éste, su tratamiento no tendrá mayor trascendencia que el de los datos relativos a un número de identificación personal, a una ficha que tan sólo pueda utilizar una persona o a la combinación de ambos*"[180].

3.2.1.3. El Documento Nacional de Identidad.

Las dudas que había, si es que alguien las sostenía, sobre si el Documento Nacional de Identidad (DNI) es un dato personal las han resuelto los tribunales. Ha sido la Audiencia Nacional la que asienta el concepto al confirmar la sanción impuesta a una empresa de telefonía por infracción del principio de calidad del dato, al haber dado de alta una incidencia en un registro de morosos haciendo constar un DNI que no se correspondía con el del verdadero deudor. La recurrente negaba que el DNI fuera por sí solo un dato personal alegando, en su defensa, que no identificaba a la persona. El tribunal declaró que sí tiene la consideración de datos de carácter personal[181].

En su Informe 0669/2009, la Agencia determina que "*el número de DNI es un dato de carácter personal, al explicar que, según la Ley Orgánica 15/1999, el concepto de dato personal, comprende según el artículo 3 a) "cualquier información concerniente a persona física identificada o identificable", entendiendo que se requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o*

[180] CASTAÑEDA GONZÁLEZ, A.: Op. cit., pág. 26.

[181] Sentencia de la Audiencia Nacional, Sección 1ª, de 27 de octubre de 2004.

dato y, de otra, que dicho dato pueda vincularse a una persona física identificada o identificable"[182].

Este concepto se confirma y se concreta tras la entrada en vigor del Reglamento que desarrolla la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, en el que se define tanto dato de carácter personal como persona identificable en su artículo 5.1 estableciendo que son *"f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. Y, además, persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados*"[183].

Las de la normativa de protección de datos hay que relacionarlas con la finalidad que tiene el DNI, que aparece recogida en el Real Decreto 1553/2005, de 23 diciembre, por el que se regula la expedición del documento nacional de identidad y certificados de firma electrónica del DNI, que regula en su artículo 1 la naturaleza y funciones del DNI señalando que "*1. El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y conservación del mismo. 2. Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo. 3. A cada Documento Nacional de Identidad, se le asignará un número personal que tendrá la consideración de identificador numérico personal de carácter general. 4. Igualmente, el Documento Nacional de Identidad permite a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular, así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica*"[184].

---

[182] Informe Jurídico de l Agencia Española de Protección de Datos sobre creación de ficheros que incluyen, entre otros datos, el DNI de personas. Véase: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdfs/2009-0669_Fichero-con-datos-de-contacto-y-D.N.I.-sujeto-LOPD.pdf>.

[183] B.O.E., núm. 17, de 19/01/2008, pág. 4103.

[184] B.O.E., núm. 307, de 24/12/2005, pág. 42090.

La naturaleza de dato personal del DNI resulta clara atendiendo a lo anteriormente expuesto, concluye la Agencia en el citado Informe de 2009. Ningún autor lo pone ya en duda.

3.2.1.4. El número de teléfono.

Es un dato personal desde el instante en que es asociado a un nombre y apellidos, puesto que nos proporciona información sobre una persona identificada. Pero incluso el propio número de teléfono, (ya sea móvil o fijo) sin aparecer directamente asociado a una persona, puede tener la consideración de dato personal si a través de él puede identificarse a su titular[185].

Otra cuestión es el caso de las conversaciones telefónicas. El problema lo aborda la Agencia en su Informe 0549/2008 y 0078/2009 al analizar las conversaciones telefónicas que se reciben en una Jefatura de Policía Local (situación aplicable a las que pueda recibir una Cadena de Emisoras de Radiodifusión) y el almacenamiento posterior de las mismas, teniendo en cuenta que no queda registrado el número de teléfono desde el que se efectúan dichas llamadas y sin entrar en la finalidad con la que se procede a dichas grabaciones[186].

La primera cuestión que resuelve la Agencia en el citado Informe, consiste en discernir si las conversaciones telefónicas se encontrarán sometidas a lo dispuesto en la Ley Orgánica. A tal efecto y, con carácter general, debe indicarse, señala, "*que los artículos 1 y 2 de la citada Ley, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento automatizado o no de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la Ley Orgánica como "cualquier información concerniente a personas físicas identificadas o identificables". b) En segundo término, y aun cuando nos hallemos ante un supuesto en que existan datos de carácter personal, será necesario que dichos datos se encuentren incorporados a un fichero, definido como "todo*

---

185 Sentencia de la Audiencia Nacional, Sección 1ª, de 26 de enero de 2005. Rec. 1258/2002.

186 Informe Jurídico emitido por la Agencia Española de Protección de Datos: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2008-0549_Grabaci-oo-n-de-conversaciones-telef-oo-nicas-por-la-Policia-Local.pdf>.

conjunto organizado de datos de carácter personal..", por el artículo 3 b) de la Ley".

No obstante, si la grabación estuviera digitalizada, nos encontraríamos ante un tratamiento automatizado necesariamente sometido a los preceptos de la Ley Orgánica 15/1999, aunque no haya fichero. Con todo esto, dice la Agencia que "*las grabaciones de conversaciones telefónicas sólo podrán ser consideradas datos de carácter personal en caso de que las mismas permitan la identificación de las personas que aparecen en dichas grabaciones, no encontrándose amparadas en la Ley Orgánica en caso contrario*"[187].

A juicio de la Agencia Española de Protección de Datos, en el caso del citado Informe Jurídico, aunque no pueda asociarse la grabación a un número de teléfono, las conversaciones telefónicas sí podrían contener muy probablemente datos de carácter personal que pudieran identificar, no ya a los interlocutores de la llamada, sino a cualquier persona a la que pudieran referirse en dichas conversaciones. Si las grabaciones pueden considerarse estructuradas en un fichero el modo al que se ha hecho referencia, el mismo se encontrará sometido a lo dispuesto en la Ley Orgánica 15/1999. Por tanto, será necesario para proceder al tratamiento de los datos el consentimiento de los afectados, tal y como dispone el artículo 6.1 de la Ley, debiendo informarse a los mismos de los extremos contenidos la norma. Es decir, será imprescindible que, al proceder a la grabación de las conversaciones telefónicas en cuestión, se comunique al interesado, de forma que conste claramente su conocimiento, los extremos a los que hace referencia el artículo 5.1 de la Ley Orgánica, según el cual "*los afectados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco….de la existencia de un fichero y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos., de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, así como de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante*"[188].

Con carácter general, indica la Agencia en este importante Informe Jurídico, que "*debe partirse de que si tales grabaciones tienen trascendencia y entran dentro del ámbito de aplicación de la Ley 15/1999*

[187] Ibídem, pág. 2.

[188] B.O.E., núm. 298, de 14/12/1999, pág. 43089.

desde el momento en que en las mismas se recojan datos personales de quienes contactan con dicho servicio de atención telefónica, ello determinará la plena aplicación de los preceptos de la Ley española en relación con el tratamiento de datos de carácter personal que implica tal grabación"[189].

3.2.1.5. Datos relativos al ejercicio de una profesión.

Los datos personales que se refieren al ejercicio de una profesión no impiden la aplicación del régimen jurídico sancionador contemplado en la LOPD, "*pues la protección de datos que se reconoce en el art. 18.4 de la Constitución española (CE) extiende su cobertura no a los datos íntimos de la persona, protegidos en el derecho a la intimidad del artículo 18.1 de la CE, sino a los datos de carácter personal, tal y como ha establecido el Tribunal Constitucional*"[190].

Por tanto, la garantía de la vida de la persona y su reputación poseen una dimensión positiva que excede del ámbito del artículo 18.1 de la CE[191], y que se traduce en un derecho al control sobre los datos. "*Se pretende garantizar ahora a la persona mediante el control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad del afectado, y que los datos sólo podrán ser tratados y cedidos con su consentimiento*", como ha señalado la Audiencia Nacional[192].

No es preciso, por tanto, en modo alguno, que se haya vulnerado el derecho a la intimidad, ni que el dato afecte a esa esfera íntima de la persona, para que pueda ser sancionada una conducta en materia de protección de datos, pues este derecho fundamental tiene un objeto distinto y una dimensión que excede de la del derecho a la intimidad. A tener en cuenta que la sentencia aquí citada del Tribunal Constitucional 292 de 2000 declara que "*el objeto de protección del derecho fundamental a la*

---

[189] Informe Jurídico 0549/2008 de la Agencia Española de Protección de Datos, op. cit.

[190] Sentencia del Tribunal Constitucional 292/2000.

[191] Constitución Española, artículo 18.1: "*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*".

[192] Sentencia de la Audiencia Nacional, Sección 1ª, de 11 de febrero de 2004. Rec. 119/2002.

protección de datos no se reduce solo a los datos íntimos de las personas, sino a cualquier tipo de dato personal, sea o no íntimo"[193].

3.2.1.6. La imagen de la persona.

Aunque ya ha quedado establecido, incluso con mención expresa en la normativa legal, que la imagen de una persona es un dato de carácter personal, la cuestión no ha estado exenta de controversia. Especialmente preocupa cuando la imagen de la persona aparece recogida en fotografías (algo de lo que deberían tomar mucho más en consideración los periódicos, como Medios de Comunicación Social ocupados, por excelencia, en la publicación de fotografías) en películas o en otros medios de reproducción, como, por supuesto, son las televisiones.

Los tribunales han abordado este punto en algunos pronunciamientos importantes. El Tribunal Constitucional, resolviendo un recurso de amparo, entró de lleno en la cuestión en 2003[194]. El amparo fue interpuesto tras la difusión por la policía de la fotografía de un detenido, tomada para su reseña en los archivos policiales. El afectado, que recurrió, había presentado ante la Administración una reclamación por responsabilidad patrimonial por el uso indebido de su imagen, reclamación que no había prosperado. Tampoco tuvo éxito ante la Audiencia Nacional.

El Tribunal Constitucional empezaba recordando, en su dimensión basada en la CE, que el derecho a la propia imagen proclamado en el art. 18.4 se configura como un derecho de la personalidad, derivado de la dignidad humana y dirigido a proteger la dimensión moral de las personas, que atribuye a su titular un derecho a determinar la in formación gráfica generada por sus rasgos físicos personales que puede tener difusión pública. La facultad otorgada por este derecho, en tanto que derecho fundamental, consiste en esencia en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad, que puede ser informativa (en el caso de los

[193] Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de varios preceptos de la Ley Orgánica. B.O.E., núm. 4. Suplemento. 4/01/2001, pág. 104.

[194] Sentencia del Tribunal Constitucional 14/2003, de 30 de enero. Recurso de amparo 4184/2000.

periódicos y las televisiones) comercial, científica, cultural, etc. perseguida por quien la capta o difunde[195].

Ahora bien, como todo derecho fundamental, no es un derecho incondicionado y sin reservas, de suerte que se pueda impedir en todo caso la captación o difusión de la imagen sin autorización, sino que su contenido se encuentra delimitado por el de otros derechos y bienes recogidos en la Constitución española.

Desde la perspectiva concreta de la protección de datos de carácter personal, esta Sentencia del TC considera que la fotografía es un dato personal sujeto al régimen legal de protección, doctrina extensible a los Medios de Comunicación como los periódicos y las televisiones, y, desde luego, a cualquier medio de reproducción de imagen.

Es más, incluso hay casos en que se ha considerado la simple 'silueta' de una persona como hecho identificable de la misma y, por tanto, dato personal. La Sentencia del Tribunal Supremo de 2004[196] estudió una demanda por vulneración de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen[197] que conecta con la protección de datos al tratarse de una demanda planteada por una joven cuya fotografía apareció en la portada del periódico La Voz de Almería. La imagen, de gran tamaño, en la que se apreciaba la imagen de una chica, paseando con su perro, era la de su silueta y había sido captada en una playa nudista de Vera, por lo que la joven iba desnuda. Ni se le informó que estaba siendo fotografiada ni tampoco se le solicitó consentimiento para publicar posteriormente su imagen en la portada de un periódico. La única cortesía que tuvo el fotógrafo fue hacer la foto de forma que no se apreciara el rostro y sólo el contorno o silueta de la chica aparecía nítidamente visible. Ella se reconoció en la portada del periódico e inició una demanda por intromisión ilegítima en su derecho a la propia imagen y acabó ganando y obteniendo una indemnización de 6000 euros[198].

---

[195] Sentencia del Tribunal Constitucional 81/2001, de 26 de marzo de 2001, Fundamento Jurídico 2. STC 139/2001, de 18 de junio de 2001, FJ 4. STC 83/2002, de 22 de abril de 2002, FJ 4.

[196] Sentencia del Tribunal Supremo núm. 784/2004, de 12 julio.

[197] B.O.E., núm. 115, de 14/5/1982, pág. 12546.

[198] <http://www.samuelparra.com/2008/08/27/la-silueta-como-dato-personal/>.

El Tribunal Supremo se basó en que los testigos que declararon en la instancia, todos los cuales conocían la chica desde hacía varios años, identificaron la fotografía como reproducción de la figura de la misma, siendo indiferente que el círculo de conocidos de esa persona fuera mayor o menor, fundamentando la afirmación de que la chica es reconocible porque hay testigos que así lo demuestra.

La imagen, la silueta, se torna dato suficiente para identificar a una persona, en este caso a la fotografiada, por lo que el Tribunal Supremo concluye en la estimación del recurso, con la consecuencia de tener como hecho probado que la fotografía de la mujer que aparece en la fotografía publicada en la portada del periódico reproduce la imagen de la demandante.

Es decir, que si la silueta de una persona (aun sin verse la cara) ha sido suficiente para identificarla, estamos, por tanto, ante un dato de carácter personal. El Reglamento de desarrollo de la Ley española de Protección de Datos Personales, R.D. 1720/2007, contempla expresamente la imagen como dato de carácter personal[199].

3.2.1.7. La voz

Interesa a las emisoras de radio, en especial, la clarificación de esta facultad de las personas en su sentido jurídico. Han sido varios los pronunciamientos de la Agencia sobre la estimación de la voz como un dato de carácter personal objeto de protección. En la Resolución nº R/01127/2009[200], respondiendo a una reclamación efectuada por un particular contra Telefónica España, que no atendió el derecho de acceso a los datos personales del reclamante contenidos en los ficheros de la entidad.

Durante la tramitación del procedimiento, Telefónica atendió el acceso solicitado, facilitando los datos de base, pero sin aportar los de voz por considerar que no son de carácter personal.

---

[199] B. O. E., núm. 17, de 19/01/2008, pág. 4103.

[200] Procedimiento Nº: TD/01640/2008 de la Agencia de Protección de Datos. Véase: <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2009/common/pdfs/TD-01640-2008_Resolucion-de-fecha-27-04-2009_Art-ii-culo-15-LOPD.pdf>.

Explica entonces la Resolución de la Agencia que " *los artículos 1 y 2 de la LOPD, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, siendo definidos estos en el artículo 3.a) de la Ley Orgánica como 'cualquier información concerniente a personas físicas identificadas o identificables'. Por lo tanto, la voz recogida en grabaciones, sólo podrán ser consideradas como datos de carácter personal cuando las mismas permitan la identificación de las personas que aparecen en dichas voces, no encontrándose amparadas en la Ley Orgánica en caso contrario*"[201].

Serán necesarios, asimismo, -señala la Resolución citada- que dichos datos se encuentren incorporados a un fichero, definido como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso", por el artículo 3.b) de la Ley. En consecuencia, señala, "*en caso de haberse hecho efectiva la recogida de las voces en un fichero y haberse procedido a la identificación de las voces por asociación con otros datos personales, dicha circunstancia debería comunicarse a quienes pudieran aparecer en esas voces, debiendo además el fichero resultante ser inscrito en el Registro General de Protección de Datos*"[202].

Respecto al tratamiento de registros de voz, ya en 1999 fueron planteadas a la Agencia Española de Protección de Datos[203] diversas cuestiones relacionadas con la recopilación por parte de una empresa de diferentes registros de voz, con la finalidad de elaborar un programa de "software" de reconocimiento de voz. La recopilación tendría lugar mediante la realización de llamadas telefónicas efectuadas desde un Estado miembro de la Unión Europea. Resolvió esta cuestión, considerando la Agencia que siempre que quien haya de realizar el tratamiento tenga conocimiento directo o indirecto de quién es la persona cuya voz está siendo objeto de grabación, así como de su número de teléfono, la grabación efectuada tendrá la naturaleza de dato de carácter personal y el tratamiento efectuado estará sometido a la normativa de protección de datos, al incorporarse al mismo los datos identificativos del sujeto (nombre y apellidos), su número de teléfono y su voz, conforme a lo dispuesto en el

[201] Ibídem, pág.3.

[202] Ib., pág. 4

[203] Informe Jurídico de la Agencia Española de Protección de Datos sobre recopilación de registros de voz. Véase: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/1999-0000_Tratamiento-de-registros-de-voz.pdf>.

artículo 3.a) de la LOPD y en Real Decreto 1720/2007, que indican que dichos datos podrán proceder de información acústica.

Se suscitaba, de otro lado, la cuestión de que los datos iban a ser recogidos mediante llamadas telefónicas efectuadas desde otro Estado miembro de la Unión Europea, planteándose si en dicho caso existirá una transferencia internacional de datos. A estos efectos, se indicó, en primer término que, como se desprende de lo establecido en el artículo 4 de la Directiva 95/46/CE, será aplicable la Ley española siempre que el tratamiento se efectúe en territorio español, considerándose a estos efectos que habrá de tenerse en consideración el lugar en que radique la persona cuyos datos están siendo objeto de recogida. Por ello, la recogida de estos datos exigirá el cumplimiento de las disposiciones de la LOPD.

3.2.1.8. La Internet Protocol (IP).

El Grupo comunitario de Expertos comunitarios considera en su Dictamen 4/2007[204], al explicar el rasgo de 'directa o indirectamente identificable' del concepto de dato personal, que las direcciones Internet Protocol (IP), la serie de números que identifica a un ordenador en la red, son datos sobre una persona identificable.

Los equipos comunican a través de Internet mediante el protocolo IP (Protocolo de Internet). Este protocolo utiliza direcciones numéricas denominadas direcciones IP compuestas por cuatro números enteros (4 bytes) entre 0 y 255, y escritos en el formato xxx.xxx.xxx.xxx. Por ejemplo, 194.153.205.26 es una dirección IP en formato técnico. Los equipos de una red utilizan estas direcciones para comunicarse, de manera que cada equipo de la red tiene una dirección IP exclusiva[205].

El Dictamen 4/2007 ha declarado que "*los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor HTTP. En estos*

[204] Dictamen 4/2007: op. cit.

[205] Definiciones en: <http://es.kioskea.net/contents/internet/ip.php3>.

casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 2 de la Directiva"[206].

Especialmente en aquellos casos en los que el tratamiento de direcciones IP se lleva a cabo con objeto de identificar a los usuarios de un ordenador (por ejemplo, el realizado por los titulares de los derechos de autor para demandar a los usuarios por violación de los derechos de propiedad intelectual), el responsable del tratamiento prevé que los medios que pueden ser razonablemente utilizados para identificar a las personas pueden obtenerse, por ejemplo, a través de los tribunales competentes (de otro modo la recopilación de información no tiene ningún sentido), y por lo tanto la información debe considerarse como datos personales.

En nuestro país, la Agencia Española de Protección de Datos se ha pronunciado sobre la IP y el concepto de dato personal en su Informe Jurídico 327/2003[207], en el que contesta a una consulta planteando diversas cuestiones referentes a la consideración como dato de carácter personal de una dirección IP de acuerdo a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, y sus implicaciones de cara a la adopción de las medidas de seguridad.

Para resolver la cuestión de si las direcciones IP son consideradas como datos de carácter personal debe partirse, en todo caso, según señala la Agencia española en el citado Informe, de la definición de dato de carácter personal que establece el artículo 3 a) de la Ley Orgánica de Protección de Datos, que lo define como "*cualquier información concerniente a personas físicas identificadas o identificables*".

El Transmision Control Protocol/Internet Protocol (TCP/IP) es un protocolo básico de transmisión de datos en Internet, donde cada ordenador se identifica con una dirección IP numérica única. Las redes TCP/IP se basan en la transmisión de paquetes pequeños de información, cada una de los cuales contiene una dirección IP del emisor y del destinatario.

Por otro lado, el DNS (sistema de nombre de dominio) es un mecanismo de asignación de nombres a ordenadores identificados con una

[206] Documento de trabajo WP 37: Privacidad en Internet: - Enfoque comunitario integrado de la protección de datos en línea adoptado el 21.11.2000.

[207] Apartado de Informes Jurídicos de la Agencia Española de Protección de Datos: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf>.

dirección IP. Ciertas herramientas existentes en la red permiten encontrar el enlace entre el nombre de dominio y la empresa o el particular.

A su vez, los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP. Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet, normalmente mantiene un fichero histórico con la dirección IP (fija o dinámica) asignada, el número de identificación del suscriptor, la fecha la hora y la duración de la asignación de dirección. Es mas, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica registrará el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación.

En estos casos, ello significa que, con la asistencia de terceras partes responsables de la asignación, se puede identificar a un usuario de Internet, es decir, obtener su identidad civil (nombre dirección, número de teléfono, etc), por medios razonables, con lo que no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 3 de la Ley 15/1999.

Advierte el Informe de la Agencia Española de Protección de Datos que, por otro lado, "*un tercero puede llegar a averiguar la dirección IP dinámica de un usuario pero no ser capaz de relacionarla con otros datos que le permitan identificarlo. Obviamente, resulta más sencillo identificar a los usuarios de Internet que utilizan direcciones estáticas Sin embargo, en muchos casos existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como cookies con un identificador único o sistemas modernos de minería de datos unidos a bases de datos con información sobre usuarios de Internet que permite su identificación*"[208].

Añade, además, que "*aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con*

[208] Ibídem, pág. 2.

independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos"[209].

Respecto a las medidas de seguridad a adoptar, el Informe 327/2003 indica que "*un fichero que contuviera únicamente las direcciones IP, en principio, resultaría de aplicación las medidas de seguridad nivel básico. Por el contrario, un fichero que contuviera la dirección IP asociada, por ejemplo, a los sitios web solicitados con la finalidad de elaborar un determinado perfil del usuario, si el mismo permite obtener una evaluación de la personalidad del individuo, se deberán adoptar las medidas de seguridad nivel medio. Con ello se pretende establecer que deberán implementarse sobre fichero los dispositivos técnicos que garanticen los niveles de seguridad regulados, atendiendo a la naturaleza de la información tratada, y en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información*"[210].

Termina con una referencia a los "log-in" de acceso a Internet o a páginas personales como datos de carácter personal, apuntando "*que si se identifica de forma directa al usuario, no hay duda de que estaremos ante un dato de carácter personal. Por el contrario, si este es anónimo, en principio no sería un dato de carácter personal, pero si, por ejemplo, el proveedor de servicios de Internet a través de ese "log in", puede identificar al usuario con el que tiene un contrato de acceso a Internet, sí será considerado como un dato de carácter personal*"[211].

3.2.1.9. La matrícula.

Sobre las matrículas de vehículos y concepto de dato de carácter personal, es el Informe 425/2006 de la Agencia Española de Protección de Datos[212] el que se encarga de analizar "*la naturaleza de los datos contenidos en la placa de matrícula de un vehículo y el nivel de protección exigido por la Ley de dichos datos*".

---

209 Ib., pág. 2.

210 Ib., pág. 3.

211 Ib., pág. 3.

212 Informe Jurídico de la Agencia sobre la matrícula como dato de carácter personal: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/index-ides-idphp.php>.

Para ello, indica el Informe Jurídico que "*exige fijarnos si los datos de la placa de matrícula de un vehículo han de ser considerados como datos de carácter personal, a tenor de lo dispuesto en la Ley Orgánica 15/1999. En este sentido, a tener en cuenta el artículo 2.1 de la LOPD, el artículo 3 a) de dicha Ley y, en ese mismo sentido, lo que dispone el artículo 2 a) de la Directiva 95/46/CE*"[213].

Para interpretar cuándo ha de considerarse que nos encontramos ante un dato de carácter personal, señala el Informe, "*la Agencia ha venido siguiendo el criterio sustentado por las distintas Recomendaciones emitidas por el Comité de Ministros del Consejo de Europa, en las que se indica que la persona deberá considerarse identificable cuando su identificación no requiere plazos o actividades desproporcionados*"[214]. En este sentido se pronuncia el e Reglamento de desarrollo de la Ley Orgánica 15/1999[215].

Sostiene, por tanto, que el tratamiento de los datos correspondientes a las placas de matrícula de los vehículos se encontrará sometido a lo dispuesto en la Ley Orgánica 15/1999 en caso de que se considere a los datos contenidos en dichas placas datos de carácter personal, para lo que sería preciso que esos datos pudieran permitir la identificación de un individuo sin que ello exija plazos o esfuerzos desproporcionados.

Se apoya, asimismo, en el artículo 5 h) del Texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por Real Decreto Legislativo 339/1990, de 2 de marzo, que establece que "*se atribuyen al Ministerio del Interior las siguientes competencias en el ámbito de esta Ley, sin perjuicio de las que tengan asumidas las Comunidades Autónomas en sus propios Estatutos (...) los registros de vehículos, de conductores e infractores, de profesionales de la enseñanza de la conducción, de centros de formación de conductores, de los centros de reconocimiento para conductores de vehículos a motor y de manipulación de placas de matrícula, en la forma que reglamentariamente se determine*"[216].

---

213 Ibídem.

214 Ib., pág. 1.

215 B.O.E., núm. 17, de 19/1/2008, págs. 4103-4136.

216 B.O.E., núm. 63, de 14/3/1990, págs. 7259-7270.

En consecuencia, dice la Agencia, el citado precepto reconoce la subsistencia del Registro de Vehículos, creado por el artículo 244 del Código de la Circulación, aprobado por Decreto de 25 de septiembre de 1934, habilitando expresamente al desarrollo reglamentario del Texto Refundido para establecer el régimen del citado Registro. Dicho desarrollo se produjo a través de la aprobación del Reglamento General de Vehículos, en virtud del Real Decreto 2822/1998, de 23 de diciembre, cuyo artículo segundo establece en su párrafo primero que "*la Jefatura Central de Tráfico llevará un Registro de todos los vehículos matriculados, que adoptará para su funcionamiento medios informáticos y en el que figurarán, al menos, los datos que deben ser consignados obligatoriamente en el permiso o licencia de circulación, así como cuantas vicisitudes sufran posteriormente aquéllos o su titularidad*"[217].

En cuanto a su finalidad, el párrafo segundo del precepto previene que "*estará encaminado preferentemente a la identificación del titular del vehículo, al conocimiento de las características técnicas del mismo y de su aptitud para circular, a la comprobación de las inspecciones realizadas, de tener concertado el seguro obligatorio de automóviles y del cumplimiento de otras obligaciones legales, a la constatación del Parque de Vehículos y su distribución, y a otros fines estadísticos*"[218].

Por último, y en lo atinente a la publicidad de sus datos, el párrafo tercero del citado artículo 2 añade que "*el Registro de Vehículos será público para los interesados y terceros que tengan interés legítimo y directo, mediante simples notas informativas o certificaciones*". En consecuencia, se establece el carácter público del Registro, bastando para la consulta de sus datos la alegación de la existencia de un interés legítimo y directo en la consulta.

De estas argumentaciones, afirma la Agencia, cabe desprender que la identificación del titular de los vehículos cuya matrícula sea conocida únicamente exigirá la consulta del Registro de Vehículos, cuya finalidad esencial es la identificación del titular, para lo cual únicamente será necesaria la invocación del interés legítimo del solicitante.

Por consiguiente, concluye la Agencia en el citado Informe Jurídico 425/2006, "*cabe considerar que la identificación del titular del vehículo no exige esfuerzos o plazos desproporcionados, por lo que el manejo del dato de la matrícula habrá de ser considerado como tratamiento de un*

[217] B.O.E., núm. 22, de 26/1/1999, págs. 3440-3528.

[218] Ibídem.

dato de carácter personal. De lo dispuesto en el artículo 2.1, ya citado, se desprende que para que el dato personal de la matrícula pueda considerarse sometido a la Ley Orgánica deberá encontrarse incorporado a un soporte físico que le haga susceptible de tratamiento"[219].

3.2.2. Definiciones y principios.

Es un aspecto, el de las definiciones, que con la Ley se amplió. Destaca la inclusión en la Ley 15/1999 de Protección de Datos del término consentimiento; el de fuentes accesibles al público enumerando expresamente qué tipo de ficheros debe considerarse como tales; así como la consideración del encargado del tratamiento como nuevo sujeto pasivo del régimen sancionador.

Consentimiento: una de las piedras angulares de la protección de datos, y que se refuerza en la LOPD. Para Yolanda Navaltropo[220], "*debe ser, tal y como indica la norma, inequívoco, requiriéndose por escrito en algunos supuestos, como los referidos a datos especialmente protegidos*."

Fuentes accesibles al público: como indica su nombre, son las que no ofrecen obstáculo para su acceso. Entre ellas, los repertorios telefónicos, así como las guías y listados de colegios y/o grupos profesionales. Destaca, en opinión de Navalpotro, "*el 'censo promocional', es decir, el censo electoral, que será creado por vía reglamentaria detallando la Ley los datos que lo constituirán. Sólo podrán ser utilizados siempre que su titular no se oponga. Podrán ser obtenidos por aquellos interesados que deseen desarrollar actividades de prospección comercial y les serán facilitados por el Instituto Nacional de Estadística. El Congreso aprobó en octubre de 2002 una enmienda a este punto, la exigencia del requisito previo de consentimiento expreso del titular de los datos para éstos formen parte del censo promocional*"[221]. Es necesaria desde entonces la expresión del consentimiento previo.

Principio de finalidad: la ley exige que sea determinada, explícita y legítima, indicando la prohibición de utilizar los datos para otras

[219] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/index-ides-idphp.php> , pág. 3.

[220] NAVALPOTRO NAVALPOTRO,Y.:'*Estudio práctico sobre la Protección de Datos de carácter persona'l. Capítulo I*, Lex Nova, (2ª edición), Valladolid, 2007, pág. 47.

[221] Ibídem, pág. 45.

finalidades que sean incompatibles con aquellas para las que se recabaron[222].

El encargado del tratamiento: figura diferente al responsable del tratamiento del fichero, aunque trata los datos por cuenta de éste y actuará directamente sobre el tratamiento. Pueden actuar como encargado del tratamiento no sólo personas jurídicas sino también físicas, así como autoridad pública. La LOPD (art.12) regula esta figura como acceso a datos por cuenta de terceros, indicando de forma expresa que dicho acceso no es considerado 'cesión' y la forma en la que ha de articularse entre las partes[223].

Derechos de los interesados: se trata del nuevo derecho de oposición. "*Implica la posibilidad del interesado de oponerse al tratamiento de sus datos en aquellos supuestos en que no sea preciso el consentimiento para proceder al tratamiento*"[224]. Además, se relacionan en la Ley los derechos de rectificación y cancelación de los datos por parte del responsable del fichero. Está también el derecho de impugnación de valores, para que pueda obtenerse información sobre los criterios de valoración. Destaca asimismo el derecho de consulta al Registro General de Protección de Datos por el titular de los datos.

Datos sensibles: son los datos especialmente protegidos. La LOPD incluyó como novedad los datos de afiliación sindical, si bien podrían considerarse en muchos casos incluidos dentro del grupo de ideología[225].

Documento de seguridad: documento a modo de informe de auditoría donde se refleja la forma de tratamiento de la información personal[226]. En él se relaciona la forma de entrada, la circulación y la forma de salida, así como la forma de destrucción o eliminación de datos de carácter personal de una entidad, sociedad o institución pública o privada. En el mismo se

---

222 Artículo 4, sobre la calidad de los datos, de la Ley15/1999. B.O.E., núm. 298, de 14/12/1999, pág. 43088.

223 NAVALPOTRO NAVALPOTRO,Y: Op. cit., pág. 47.

224 Ibídem, pág. 48.

225 Artículo 7 de la Ley 15/1999. B.O.E., núm. 298, de 14/12/1999, pág. 43088.

226 El Documento de Seguridad constituye la obligación material más importante que concierne a las empresas que manejen y/o traten datos de carácter personal en nuestro país. Su no elaboración es sancionada por la inspección de la Agencia de Protección de Datos. Debido a su relevancia práctica, dedicamos a él una mención aparte.

reflejan todas las incidencias que se produzcan en relación a los datos personales que se manejan. Es de obligado cumplimiento para protección de datos personales de todo tipo.

Aproximemos nuestra atención, ya en este punto, a otra serie de conceptos, denominaciones o figuras que van ir apareciendo con bastante asiduidad durante todo el repaso a la LOPD:

Fichero: "*Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*", según define el art. 3, b) de la Ley[227].

Tratamiento de datos: "*Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*", tal y como define el art. 3, c) de la Ley[228].

Responsable del fichero o del tratamiento: No tiene porqué ser el encargado, quien suele rendir cuentas al primero. "*Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*" (art. 3, d)[229].

3.2.2.1. La calidad de los datos.

Los tratamientos de datos de carácter personal deberán ser necesariamente exactos, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, según el art. 4.1 de la Ley Orgánica de Protección de Datos[230].

---

[227] B.O.E., núm. 298, de 14/12/1999, pág. 43088.

[228] Ibídem.

[229] Definiciones que ofrece la propia Ley Orgánica 15/1999, y que recogemos haciendo una aproximación lo más común posible a la variada interpretación que se da entre los autores. No obstante, la propia Agencia Española de Protección de Datos se ha ido encargando de aclarar esos conceptos en sus Resoluciones ya través de su página web.

[230] Artículo 4.1 de la Ley 15/1999. B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43088.

En casos como el de la relación contractual, relación empresario-empleado, se ha llegado a plantear qué tipo de datos pueden resultar necesarios para que el empresario pueda tratar información del empleado. Es decir, nos estamos refiriendo aquí a la relación entre la empresa editorial del periódico o compañía de televisión, así como sociedad de radiodifusión, en su relación con los periodistas, productores, realizadores, administrativos y todo el personal que, en general, presta sus servicios y, por tanto, concede sus datos personales.

Ya el propio art. 4 de la LOPD[231] señala que el empresario debe proceder a revisar los datos recabados del empleado para comprobar que no se manejan ni tratan datos excesivos, inadecuados o no pertinentes con la finalidad de la recogida, que es justo la relación contractual, el contrato, que se haya suscrito con el trabajador. Puede surgir aquí la incógnita del domicilio del empleado como dato a ser manejado por el empresario, sobre lo que ha habido pronunciamientos incluso del Tribunal Constitucional, indicando al respecto que "*no parece que la solicitud del dato del domicilio, con las matizaciones señaladas, de que sea información necesaria para el desempeño del puesto y de una buena relación contractual, contradiga la legislación vigente,*[…] *toda vez que la propia información personal se solicita en el medio laboral exclusivamente, en el marco de una relación contractual y para un fin tipo laboral*"[232].

Existen numerosas normas en el ámbito laboral que implican el conocimiento del dato del domicilio del empleado por parte del empresario, sin que plantee problemas.

El siguiente apartado del art. 4 señala que los datos de carácter personal objeto de tratamiento "*no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos*"[233].

El término de 'finalidad incompatible' ha sido opinado por la Audiencia Nacional siguiendo, además, la doctrina elaborada por la propia Agencia estatal de Protección de Datos. La sala de lo contencioso-

[231] Ibídem, pág. 43088.

[232] Sentencia del Tribunal Constitucional 94/1994, sobre relación laboral de trabajadores y empresa.

[233] Artículo 4.2 de la Ley 15/1999. B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43088.

administrativo dice en una sentencia[234], que la interpretación del término 'incompatible' deberá realizarse de forma sistemática poniendo en relación tal expresión con el principio de autodeterminación que inspira la ley. Una interpretación amplia lo vaciaría de contenido. Principio que implica, a juicio de la Audiencia Nacional, que el afectado conozca o pueda conocer, mediante el empleo de una diligencia razonable que los datos por él facilitados van a ser empleados con los fines para los que los facilita.

Es, para nosotros, de fundamental importancia este punto, que ha llegado a provocar pronunciamientos de la Agencia española de Protección de datos, como ha hecho en las Recomendaciones elaboradas para el ámbito de concursos, juegos y sorteos que tanto proliferan en las cadenas de televisión estatales, regionales y locales, efectuadas en *la Inspección Sectorial de Oficio relativa a 'Concursos, juegos y sorteos de televisión'*[235], indicando precisamente que no se pueden recabar datos personales cuyo conocimiento por parte del responsable no esté justificado por la finalidad para la que se recaban y de la cual el usuario no haya sido previamente informado.

En particular, dice la Agencia en esta Inspección, no se recabarán datos personales a través de líneas 906 (extensible esto a las líneas similares y de igual naturaleza que han ido apareciendo posteriormente) cuando éstos no vayan a ser utilizados para la finalidad comunicada y su recogida sólo esté movida por cuestiones promocionales.

Añade, además, la Agencia en este sentido que los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquella que haya justificado su recogida. A este respecto, ha de tenerse bien presente que la Sentencia 292/2000 del Tribunal Constitucional deja sentado que 'el derecho a consentir la recogida y tratamiento de los datos personales no implica en modo alguno consentir la cesión de tales datos a terceros'.

---

[234] Sentencia de la Audiencia Nacional emitida el 14 de junio de 2002 (núm. Rec. 650/2001).

[235] Informe de la Agencia de Protección de Datos '*Inspección Sectorial de oficio 'Concursos, juegos y sorteos de TV'* de octubre de 2002, disponible en: <https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/recomendaciones_concursos_tv.pdf>.

Nos parece de suma importancia lo que, ya en 2002, la Agencia Española estableció ante este tipo de producción audiovisual que, sobre todo en los últimos seis años, ha visto aumentar su presencia en las parrillas de programaciones televisivas de manera casi indiscriminada y repleta de dudas sobre la legalidad de cómo proceden.

Deja constancia la Agencia Española de Protección de Datos en su informe de Inspección Sectorial de oficio 'Concursos, juegos y sorteos de TV' en relación al cumplimiento que se da del artículo 4 de la LOPD en los espacios televisivos de selección de personas que se hacen a través de líneas telefónicas, que "*aún cuando parece justificada la recogida de datos identificativos en un proceso de selección, no resulta tan defendible que el interesado deba facilitar gran cantidad de estos datos (que a veces incluyen, aparte del nombre y apellidos, el número de D.N.I. o la profesión) cuando la finalidad inicial de una línea de votación es que la audiencia pueda manifestar una cierta preferencia*"[236].

De este modo, resulta llamativo que, aunque en estos casos se ofrezca como compensación la participación en un sorteo, sean diferentes los datos que se recaban a través de un número 906 ó 908 (ahora han aparecido además otras posibilidades de números) de los que se obtienen vía SMS, para una misma línea de votación. En este sentido, parece obvio que si en esta última vía de participación basta un número telefónico de contacto (que coincide con el que corresponde al terminal desde el que se envía el mensaje) para localizar al ganador del sorteo, también sería suficiente este dato para localizarlo entre los participantes que han llamado al número 906 ó 908. No se entiende así que sean precisos otros datos para la finalidad perseguida, aunque es evidente que su solicitud tiene como consecuencia una mayor duración de la llamada y así un mayor importe en la factura telefónica del participante y, consiguientemente, un mayor ingreso económico para la compañía de audiotex[237] y para la compañía contratante del servicio.

Sobre la el uso y la finalidad que en esos procedimientos televisivos se hace de los datos personales que son decepcionados, la Agencia Española de Protección de Datos no ha detectado hasta el momento ningún

[236] Ibídem, pág. 9.

[237] Son servicios de valor añadido. Las compañías que los ofrecen, y que suelen trabajar como especializadas junto a las productoras de programas de televisión, suelen ser las titulares de la línea telefónica a través de la cual se hace el concurso, el juego o el sorteo, y almacenan en sus propios servidores los datos de carácter personal que van siendo recabados telefónicamente. Suelen guardar por un tiempo las grabaciones de audio que reciben de los participantes que llaman.

caso en el que los datos recabados a través de un 906, 908 ó de SMS se hubiesen utilizado para otra finalidad que la que ocasionó su recogida. No obstante, sí se ha observado que alguna cadena de televisión había previsto añadir a los ingresos económicos que supone el servicio de valor añadido los que podrían resultar de la utilización comercial de los datos personales recabados.

Así, en los contratos firmados con la compañía de audiotex, relativos a los procesos de votación para medir el índice de popularidad de los concursantes de uno de los programas que más proyección pública han alcanzado, se recoge que "*los datos personales de los llamantes podrán ser utilizados para los fines comerciales que [la cadena de TV y la compañía de audiotex] estimen oportunos, siempre cumpliendo con la legislación vigente de protección de datos informatizados*". A pesar de ello, y de que en las correspondientes locuciones telefónicas ni siquiera se informaba a los participantes de la incorporación de sus datos a un fichero, no se ha obtenido constancia de que tales datos se hayan utilizado hasta la fecha con otros fines comerciales ni por la televisión ni por la compañía de audiotex.

En cuanto a los mensajes SMS, la Agencia constató en su inspección en las televisiones y productoras que "*no habían sido implantados aún procedimientos efectivos para el borrado periódico de los datos reflejados en cada envío una vez concluidas las actividades que los originan. Quedó verificado que alguna compañía especializada en estos servicios conserva en sus servidores prácticamente la totalidad de los mensajes recibidos desde el inicio de su actividad, lo que le aporta gran cantidad de información sobre el comportamiento de cada uno de los usuarios del servicio, identificados por su teléfono móvil, en relación a este tipo de eventos. No obstante, reconoce la Agencia que no ha habido constancia de que esa información haya sido tratada, hasta el momento, con otros fines*"[238].

Como nota curioso y a tener en cuenta para no perder de vista, respecto de las fichas manuales que elaboran las productoras de televisión durante los procesos de selección que hacen de concursantes, se ha observado que en ciertos casos son conservadas por éstas compañías para ser utilizadas, en algunos casos, en sucesivos procesos de "*casting*", al considerar que en determinados programas los interesados responden a una misma tipología, en lo relativo a sus aptitudes artísticas, aficiones y valores personales. Quede constancia de ello.

[238] Informe de la Agencia de Protección de Datos '*Inspección Sectorial de oficio 'Concursos, juegos y sorteos de TV'* de octubre de 2002: op. cit., pág. 10.

En todo caso, hay que estar atentos y cuidadosos con esto porque la finalidad comercial y el ánimo lucrativo de las empresas televisivas resulta a veces voraz y no importará cuando sea necesario esto de observar el cumplimiento de los derechos y las obligaciones de la Ley de Protección de Datos.

3.2.2.2. Derecho a información en la recogida de datos.

Junto al conocimiento de los ficheros personales existentes y sus características principales, que se articula a través del llamado 'Derecho de Consulta del Registro General de Protección de Datos', la LOPD ha establecido un derecho-deber de información particularizada a la persona cuyos datos se recogen o ceden.

En el caso del derecho a información en la recogida de datos, pueden distinguirse dos supuestos: cuando los datos son recabados del propio afectado, o cuando lo son de un tercero. Lo sintetiza, distinguiendo ambos supuestos, el estudio de Manuel Fernández Salmerón al analizar el problema en las Administraciones Púbicas, siendo válido para nuestro caso[239].

- Cuando los datos son recabados del propio interesado, "*éste deberá ser informado previamente y de modo expreso, precio e inequívoco de la existencia de un fichero o tratamiento de carácter personal, del carácter obligatorio o facultativo de su respuestas a las preguntas que le sean planteadas, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, también de la finalidad de la recogida de estos datos (…las fórmulas genéricas son nulas, según ha dejado establecido la Agencia Española de Protección de Datos…) y de los destinatarios de la información, en los casos en que los datos se recaban para un tercero por un encargado del tratamiento, así como de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante (la Agencia exige aquí como regla general una dirección postal u otro sistema que no suponga gastos ni incomodidades superiores, que puede además reforzarse con teléfono o e-mail. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español*

[239] FERNÁNDEZ SALMERÓN, Manuel: *La protección de los datos personales en las Administraciones Públicas*, Thomson Civitas y Agencia de Protección de Datos de la Comunidad de Madrileña, Madrid, 2003, pág. 85.

deberá designar, salvo que esos medios se utilicen con fines de trámite, un representante en España)"[240].

La Administración cumple su deber de informar en general de forma escrita, pudiendo satisfacerse este punto mediante la colocación de carteles en las dependencias administrativas e incluso de forma oral, como en servicios administrativos telefónicos, incluyendo grabación de conversación.

- Cuando los datos no han sido recabados del propio interesado, sino a través de un tercero, "*el afectado deberá ser informado de forma expresa, precisa e inequívoca por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, del contenido del tratamiento, de la procedencia de los datos así como el resto de extremos antes señalados. La gran excepción es cuando haya ley que lo prevea, o los casos de tratamientos con fines históricos, estadísticos o científicos, como tampoco será necesario ese deber de información en casos en que la información al interesado resulte imposible o implique esfuerzos desproporcionados y sin sentido (las relaciones en masa entre Administración e interesados en informaciones en materia tributaria o de seguridad social que han sido trasmitidas por los propios empleadores*)"[241].

En resumen, ha de informarse al titular-afectado de todos los extremos que le permitan decidir, con conocimiento de causa, sobre las consecuencias que puede tener la entrega de datos y sobre las facultades de control que conserva.

Ha sido muy útil, en este punto, la inspección de la Agencia española de Protección de Datos hecha en el sector de los concursos, juegos y sorteos de televisión. De hecho, puede afirmarse que quizá uno de los incumplimientos más generalizados de la LOPD que se han detectado consiste en la incompleta información que se facilita al ciudadano en el momento de recabar sus datos personales. Así, señala el documento que resume la inspección de la Agencia Española de Protección de Datos, "*las locuciones utilizadas en los sistemas audiotex no incluyen en muchos casos referencias a los extremos previstos en el apartado 1 del artículo 5 de la Ley Orgánica. De esta forma, las personas que facilitan sus datos al sistema automático no tienen conocimiento del destino final que se dará a*

[240] Ibídem, pág. 87.

[241] Ib., pág. 87.

los mismos, tanto si participan en un sorteo como si lo hacen en un proceso de selección de concursantes. A este respecto, hay que señalar que el hecho de grabar la voz de los interesados en el momento de facilitar sus datos personales ya constituye un tratamiento de los mismos. En este sentido, se ha observado que tales grabaciones se almacenan de forma automatizada constituyendo un conjunto organizado en los mismos términos en que el artículo 3 de la LOPD define el término "fichero", es decir, "cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso". A esta consideración se añade el hecho de que cuando los datos se recaban en el seno de un"casting" generalmente se transcriben luego sobre ficheros convencionales de texto, ya sea mediante métodos automáticos de reconocimiento de voz o con intervención humana"[242].

Al hilo de lo anterior, de la misma forma, puede decirse que los mensajes cortos remitidos por teléfono móvil, que se almacenan junto con el número llamante, constituyen en sí mismos datos personales. Basta con recordar lo aquí reflejado en Capítulos anteriores sobre definición de 'dato personal', o los numerosos pronunciamientos de la justicia española al respecto, como el de la sentencia de la Audiencia Nacional[243], que ratifica el criterio al afirmar que "*para que exista dato de carácter personal (en contraposición con dato disociado) no es imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados", y añade que "para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona*".

La información en la recogida de datos hay que ofrecerla en el mismo momento en que son recabados. En el ámbito de las televisiones, las compañías que prestan los servicios de audiotex en acciones comerciales que llevan asociado un sorteo suelen ser contratadas por las propias cadenas de televisión. Lo que ocurre es que no siempre queda claro al participante titular de los datos que se recaban a quién corresponde la responsabilidad del fichero al que se incorporará su información de carácter personal., debido a que las locuciones utilizadas no informan adecuadamente sobre lo establecido por el artículo 5 de la LOPD.

---

242 Informe de la Agencia de Protección de Datos '*Inspección Sectorial de oficio 'Concursos, juegos y sorteos de TV*' de octubre de 2002: op. cit., pág. 7.

243 Sentencia de la Audiencia Nacional de 8 de marzo de 2002. Procedimiento Ordinario 948/2000.

Establece la inspección de la Agencia Española de Protección de Datos más supuestos: "*Si la recogida de datos se realiza a través de mensajes cortos SMS, el participante no recibe en ningún caso la preceptiva información sobre protección de datos, que deberá ser facilitada en el instante justo en que se proporcionen al servicio, es decir, cuando se da publicidad en los Medios de Comunicación Social al número telefónico de cuatro cifras al que se remitirán los mensajes. Esto aplicable tanto en los sorteos, asociados generalmente a líneas de votación, como en los procesos de selección de concursantes, en los que los datos personales son más completos. Algo parecido ocurre cuando se solicita que los datos se envíen por vía postal, mucho menos utilizado porque, sencillamente, no generan los mismos beneficios económicos. Cuando la recogida de datos se realiza a través de Internet, la Agencia ha verificado que tampoco se suministra siempre la mencionada información, a pesar de que esta vía es la que más posibilidades ofrece y la que resulta menos onerosa para el ciudadano*"[244].

Lo que sí "*son escasas, (y esto ha de ser motivo para la preocupación), son las ocasiones en las que se informa, a través de las locuciones telefónicas, publicidad o Internet, de la posibilidad que tienen los participantes en esos espacios o eventos de ejercitar los derechos de acceso, rectificación, cancelación y oposición*"[245].

3.2.2.3. El consentimiento del titular de los datos.

El principio de consentimiento es uno de los pilares en los que se asienta las bases fundamentales de le regulación normativa de la protección de datos personales. Para un periódico, una emisora de televisión, o una de radio, resulta imprescindible preguntar por la voluntad del titular de los datos personas antes que proceder a manejar esa información. A esto se le denomina en el plano de la protección de datos solicitar el consentimiento, piedra angular del cuadro completo de derechos y obligaciones[246].

---

[244] Informe de la Agencia de Protección de Datos '*Inspección Sectorial de oficio 'Concursos, juegos y sorteos de TV'* de octubre de 2002: op. cit., pág. 8. Los subrayados son nuestros.

[245] Ibídem, pág. 9.

[246] Ib., pág 17.

Es el art. 6 de la Ley Orgánica de Protección de Datos el que lo define[247], anteponiendo ante todo que ha de ser inequívoco y señalando las excepciones, para cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas, cuando se refieran a partes de un contrato o precontrato de relación negocial, laboral o administrativa, cuando la cesión tenga por finalidad proteger un interés vital del interesado, cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés del responsable del fichero o del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Constituye de suma importancia para nuestro estudio tener bien claro que para los Medios de Comunicación Social, EN SU ACTIVIDAD NO EDITORIAL, solicitar 'permiso' a la hora de recabar y archivar para manejar y/o tratar los datos de lectores, suscriptores, televidentes llamantes a concursos, adquirentes de colecciones, etc. es vital para dar cumplida cuenta de la Ley española. Estamos, además, ante la principal fuente de sanciones impuestas por la falta de cumplimiento con este principio legal.

Este consentimiento podrá ser revocado en aquellos casos que pueda darse causa justificada. Es decir, cabe dar marcha atrás una vez aceptado que manejen nuestros datos.

---

247 "*Artículo 6. Consentimiento del afectado. 1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado. 3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. 4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado",* de la LOPD, Boletín Oficial del Estado de 14 de diciembre de 1999, op. cit., pág. 43088.

En casos en que no sea necesario el consentimiento del afectado para el tratamiento, éste podrá oponerse siempre que existan motivos fundados, salvo que una ley disponga lo contrario. Será el responsable del fichero el que excluya del tratamiento los datos del afectado que revocó.

La normativa básica en la materia, junto a otros pronunciamientos que han venido a reforzar el concepto, viene a sentar con rotundidad que el consentimiento ha de ser libre, inequívoco, específico e informado. Lo dice el artículo 3, h) de la Ley Orgánica de Protección de Datos[248].

En torno a la interpretación de este precepto hay que atender a diversas interpretaciones. Ya en su Memoria anual del año 2000, la propia Agencia Española de Protección de Datos quiso delimitar cómo ha de ser concebido el 'consentimiento' del titular de los datos de carácter personal, señalando que "*habrá de ser libre de intervenciones de vicio, para una finalidad determinada y explícita, dando cuenta precisa del tratamiento y finalidades del mismo, y sin que sea deducible de una acción o acto del titular, es decir, ha de ser puramente inequívoco*"[249].

Concretamente, si son datos referidos al origen racial, salud y a la vida sexual (de protección máxima, es decir, los del artículo 7 de la LOPD) deberá ser expreso, y si son los datos personales referidos a ideología, afiliación sindical, religión y creencias, el consentimiento deberá ser expreso y si los datos personales revelan ideología, afiliación sindical, religión y creencias, el consentimiento deberá ser expreso y por escrito.

El consentimiento para la cesión de datos por parte del titular de los mismos pueden establecerse tres modos básicos de manifestarse, según pronunciamientos de la propia Agencia Española de Protección de Datos: expreso, tácito o presunto. De hecho, ha emitido varios informes sobre el concepto de 'consentimiento'[250].

---

[248] "*Artículo 3, apartado h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen."*, de la LOPD. Boletín Oficial del Estado de 14 de diciembre de 1999, op. cit., pág. 43088.

[249] La Memoria de 2000, junto a las otras elaboradas cada año por la Agencia Española de Protección de Datos con las últimas cifras e incidencias, puede encontrarse en: <https://www.agpd.es/portalweb/canaldocumentacion/memorias/index-ides-idphp.php>.

[250] Informes Jurídicos sobre el concepto de consentimiento, disponibles en: <https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/consentimiento/index-ides-idphp.php>.

El consentimiento expreso se manifiesta mediante un acto positivo y declarativo de la voluntad.

El consentimiento tácito se produce cuando pudiendo manifestar un acto de voluntad contrario, ésta no se lleva a cabo, es decir, cuando el silencio se presume o interpreta como un acto de aceptación. (No se admite consentimiento tácito para aprobar el tratamiento de datos personales relativos a la ideología, la afiliación sindical, la religión y las creencias)[251].

El consentimiento presunto, que no se deduce ni de una declaración ni de un acto de silencio positivo, sino de un comportamiento o conducta que implica aceptación de un determinado compromiso u obligación.

Son numerosos los pronunciamientos que tiene la Agencia española de Protección de Datos para acotar y debilitar el concepto jurídico de un principio tan importante que, como aquí decimos, constituye el consentimiento en el mundo de la protección de datos de carácter personal, y de tanta incidencia para nuestro análisis mirando al modo de proceder de los Medios de Comunicación Social.

Son varios los Informes que la Agencia ha dedicado exclusivamente al concepto de consentimiento, para clarificar interpretaciones y ofrecer diferentes ángulos de vista sobre el consentimiento encarcelas que, en la actualidad, puede ofrecer alguna controversia o duda en torno a este principio tan destacado de la LOPD. En concreto, los realizados y publicados hasta la fecha[252], son los dedicados a especificar el consentimiento en los siguientes aspectos:

---

[251] A estos efectos, la Sentencia de la Audiencia Nacional del 31 de enero de 2003 confirma la sanción impuesta por la Agencia Española de Protección de Datos a la una empresa encargada de realizar la selección de participantes en un concurso de televisión por incurrir en infracción del art. 7 de la LOPD, al haber recabado datos sobre la ideología política y religiosa de los aspirantes sin informarles del precepto contenido en el art. 16 de la Constitución española, ni haberles informado debidamente, ni haber recabado su consentimiento expreso y por escrito, previamente al tratamiento. Para la Audiencia Nacional, el mero hecho de la participación en la selección y rellenar el formulario no implicaba el conocimiento, por los interesados, de que sus datos personales iban a ser sometidos a tratamiento.

[252] Puede accederse a cada uno de ellos en el siguiente sitio de web de la Agencia: <https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/consentimiento/index-ides-idphp.php>.

- Necesidad de obtención de consentimiento del empleado para utilizar fecha de nacimiento para felicitarle el cumpleaños.
- Comunicación de datos personales en procedimientos administrativos sancionadores.
- Formas de obtener el consentimiento mediante web. Consentimientos tácitos.
- Tratamiento de datos a través de páginas web.
- Tratamiento de datos para fines incompatibles.
- Tratamiento por abogados y procuradores de los datos de las partes en un proceso.
- Consentimiento otorgado por menores de edad.
- Caracteres del consentimiento definido por la LOPD.
- Tratamiento de la huella cibernética de los trabajadores.

3.2.2.4. Seguridad de los datos.

Corresponde al responsable del fichero y, en su caso, si lo hubiera, al encargado del tratamiento de los datos personales, "*el deber de adoptar medidas de índole técnica u organizativa necesarias que garanticen la seguridad de los datos y eviten así su pérdida, alteración, tratamiento o acceso no autorizado*"[253]. Esto habrá de ser inexcusable, siempre, en cualquier empresa dedicada a la actividad propia de los Medios de Comunicación.

Se entiende que el responsable del fichero "*es la persona física o jurídica, de naturaleza privada o pública, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento",* tal como señala exactamente la definición del apartado d) recogida en el artículo 3 de la Ley [254].

Se entiende que el encargado del tratamiento "*es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o*

[253] B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43090.

[254] Ibídem, pág. 43088.

conjuntamente con otros trate datos personales por cuenta del responsable del tratamiento" (art.3, apartado g)[255].

La Ley deja sentada la prohibición de registrar datos de carácter personal en ficheros que no reúnan las condiciones que se determinen con respecto a su integridad y seguridad, y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

La Agencia Española de Protección de Datos ha examinado el cumplimiento de este deber en las televisiones y productoras. En su inspección ha comprobado que, en general, las televisiones han elaborado e implantado su propia normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y al conjunto de los sistemas de información corporativos. No puede decirse lo mismo, sin embargo, de las productoras y de las compañías que prestan servicios de audiotex o de recepción de mensajes SMS.

En general, según indica la Agencia en un informe inspector de las televisiones[256], se trata de compañías que se hallan en aún proceso de implantación de las medidas de seguridad, por lo que los documentos de referencia, cuando existen, suelen tener carácter provisional. En este sentido, hay que recordar que, tanto si la compañía actúa como responsable del fichero como si lo hace en calidad de encargado del tratamiento, el artículo 9 de la LOPD establece que "*deberán adoptarse medidas*", como señalamos en el primer párrafo de este apartado.

Por otra parte, la Agencia española de Protección de Datos ha observado que es frecuente el intercambio a través de Internet de ficheros con datos personales entre las distintas compañías que participan en la realización de programas de televisión. Aunque puede decirse que la mayor parte de los ficheros analizados presentan una estructura de datos tal que, en aplicación del nuevo Reglamento, (tal y como exigía el anterior, en vigor en el momento de esa inspección), cabría exigir la adopción de las medidas de seguridad calificadas como de nivel básico, hay que incidir en los riesgos asociados al envío de esos datos a través de un medio que

[255] Ib., pág. 43088.

[256] Informe de la Agencia de Protección de Datos 'Inspección Sectorial de oficio 'Concursos, juegos y sorteos de TV' de octubre de 2002: op. cit., pág. 14.

ofrece tan pocas garantías de seguridad como es Internet. De hecho, se ha producido alguna sanción a productoras dedicadas a realizar concursos[257].

3.2.2.5. Datos especialmente protegidos (ideología, religión, creencias, afiliación sindical, origen racial, salud y vida sexual.

La normativa ha venido a distinguir tres niveles distintos de protección de datos atendiendo al tipo y naturaleza de los mismos y derivando en tres grandes conjuntos en los que se agrupan la totalidad de los datos de carácter personal, según importancia y alcance. Las emisoras de radio, los periódicos y las televisiones no están sabiendo aplicar siempre con precisión este ángulo de la Ley.

Vayamos a desglosar los niveles que clasifican a los datos personales.

El art. 7 de la LOPD dice que son datos especialmente protegidos (de Nivel Alto) los relativos a ideología, religión o creencias, (éstos están amparados además por precepto constitucional –art. 16.2 CE–). Para recabar estos datos es imprescindible solicitar consentimiento a su titular y informándole de la posibilidad a no prestarlo. Sólo con el consentimiento expreso y por escrito del titular de los datos podrán ser éstos objeto del tratamiento sobre información que revele ideología, religión o creencias, así como afiliación sindical (dato personal que se ha sumado a la luz de la jurisprudencia)[258].

La gran excepción a esta exigencia es para los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, si bien la cesión de esos datos requerirá en todo caso el previo consentimiento. Lógica excepción para estos ficheros que, por naturaleza y principios, se supone, no van a comercializar nunca con los datos que manejan.

---

[257] Sanción impuesta por la Agencia en el año 2000 a la productora de un concurso, al no haber estipulado contractualmente las medidas que debían adoptar todas las entidades colaboradoras con objeto de evitar que los datos recabados durante el proceso de selección de participantes llegasen a hacerse públicos a través de Internet, como finalmente ocurrió.

[258] Muchas Resoluciones acumula ya la Agencia española de Protección de Datos para delimitar este concepto. Disponibles en su página web, dedicando la mayoría de ellas a procedimiento sancionadores por incumplimiento del concepto de consentimiento, una de las principales infracciones que se dan en la práctica.

Son también datos que requieren especial protección los relativos "*al origen racial, a la salud y a la vida sexual, que sólo pueden ser recabados, tratados y/o cedidos cuando una ley lo disponga por razones de interés general o el propio titular lo consienta expresamente"* (art. 7.3 de la LOPD)[259]. Esto hace restringir y limitar bastante la posibilidad de que estos datos transiten.

Cuando el tratamiento de estos datos sean necesarios para la prevención o diagnóstico médicos, la prestación sanitaria, para la gestión de servicios sanitarios o para un tratamiento médico, podrán ser manejados dichos datos, si bien únicamente por el profesional sanitario sujeto al secreto profesional o persona equivalente. Igualmente, será posible tratar estos datos cuando sea necesario salvaguardar el interés vital del titular, si éste se muestra incapacitado para dar su consentimiento. La LOPD dedica su art. 8 a los datos relativos a la salud[260].

El Reglamento 1720/2007 de 21 de diciembre[261], que desarrolla la Ley de 1999, añade nuevos matices al respecto en su articulado y disposiciones. Además del nivel máximo de protección, los otros dos niveles son el medio y el básico:

De Nivel Medio son los datos relativos a "*comisión de infracciones penales, de infracciones administrativas, información de Hacienda Pública e información de servicios financieros como los relativos a la solvencia patrimonial y crédito, los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social*"[262]. Los recoge el art. 7.2, que también añade los que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

---

[259] Artículo 7.3. B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43090.

[260] El Reglamento 1720/2007 de 21 diciembre de 2007, que ha venido a desarrollar la Ley Orgánica de Protección de Datos, amplía en su Disposición Transitoria Segunda apartado 3, b), esa relación de datos que merecen protección de nivel alto a los ficheros que contengan datos derivados de actos de violencia de género.

[261] B. O. E., núm. 17, de 19/1/2008, págs. 4103-4136.

[262] Ibídem, pág. 4125.

De Nivel Básico son los datos relativos a nombre, apellidos, direcciones de contacto (tanto físicas como electrónicas), teléfono (fijo o móvil), número de cuenta corriente y otros, como recoge el art. 81.5.

El artículo 81 del nuevo Reglamento que desarrolla la LOPD, el Real Decreto 1720/2007, de 21 de diciembre, es clarificador de todo esto[263].

En la actividad no editorial de las televisiones, en su primera inspección de carácter sectorial, la Agencia estatal no obtuvo evidencia de que en los programas de televisión analizados se traten datos de los que el artículo 7 de la LOPD considera especialmente protegidos y que pueden ser manifestados en un momento dado, si no la ideología, o la afiliación sindical, que también, sí pueden ser expresados espontáneamente la religión, las creencias, el origen racial, la salud o la orientación sexual.

3.2.2.6 Deber de secreto.

Sin duda, uno de los ejes centrales del derecho de la protección de datos es el deber de secreto que la Ley extiende en su art.10 no sólo al responsable del fichero, sino también a quienes intervengan en cualquier fase del tratamiento durante el periodo de tiempo en que los datos almacenados en ficheros organizados y estructurados bajo su control. Estamos, junto al consentimiento que ha de solicitarse al titular de los

263 *"Artículo 81. Aplicación de los niveles de seguridad. 1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico. 2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal: a) Los relativos a la comisión de infracciones administrativas o penales. b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre. c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias. d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros. e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.*", del Real Decreto 1720/2007, de 21 de diciembre, B.O.E. núm. 17, de 19 de enero de 2008, págs. 4103-4136.

datos, ante otra de las piedras angulares de la protección de datos y los Medios de Comunicación Social.

El deber de secreto, afirma Y. Navalpotro, "*es una obligación que afecta tanto a personas que trabajan para el responsable del fichero como a aquellas que trabajan para terceros que acceden a los datos como consecuencia de un servicio prestado al responsable*"[264]. Están por tanto obligados al deber de guardarlos responsables y cualesquiera con acceso a los datos durante e incluso después de finalizar sus relaciones con el titular del fichero o con el responsable del mismo.

Sin embargo, tampoco puede darse una situación de descuido por parte del responsable del fichero debido a esta extensión de la obligación a otras personas. Deberá tomar las medidas adecuadas orientadas a garantizar la seguridad del tratamiento, es decir, la tutela de los datos.

Se establecen una serie de requisitos en el art. 12 en el que deben de incluirse obligatoriamente en el contrato que regula la relación entre responsable del fichero y encargado del tratamiento. Requisitos que han de cumplirse durante todo el periodo en que se esté accediendo a los datos.

Importante resulta establecer aquí la diferencia existente entre el deber de guardar secreto y la cesión de datos sin el consentimiento de los afectados, para lo cual, siguiendo a Y. Navalpotro, hay que considerar lo explicado por la Agencia Española de Protección de Datos en su Memorial anual de 1998, "*se considera que la diferencia radica en que la cesión es un comportamiento cualificado de la comunicación de datos, cualificación que no puede ser otra que la voluntad de que los datos sirvan para ser tratados de forma automatizada por parte del cesionario o se utilicen por éste para cualquier decisión posterior respecto de las relaciones que mantenga o pueda establecer con el afectado. Es decir, la cesión aparece como una conducta encaminada a la prestación de las funciones o actividades de los que intervienen en la comunicación, de modo que si la comunicación no se afecta a tales actividades, si no se dirige a satisfacer una demanda del cesionario, que se servirá de la cesión para el ejercicio de una actividad, la comunicación del contenido del fichero deberá ser calificada como una violación del deber de secreto*"[265].

[264] NAVALPOTRO NAVALPOTRO, Y: Op. cit., pág. 571.

[265] Ibídem, pág. 573.

3.2.2.7. La cesión o comunicación de los datos. Consentimiento previo y excepciones.

Considerada como revelación de datos realizada a una persona distinta del interesado, la cesión de datos es regulada en el art. 11 de la LOPD[266] .De la lectura del precepto se asienta la clara conclusión de que el consentimiento del interesado constituye el principal parámetro sobre el que pivota la cesión de datos personales.

A esa regla general de la obtención del consentimiento del interesado para la cesión o comunicación de datos, la ley coloca determinadas excepciones, entre las que destacan aquellas cesiones que sean necesarias para el desarrollo, cumplimiento y control de las relaciones laborales existentes entre el empresario y los trabajadores.

---

[266] "*Artículo 11. Comunicación de datos. 1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. 2. El consentimiento exigido en el apartado anterior no será preciso: a) Cuando la cesión está autorizada en una ley. b) Cuando se trate de datos recogidos de fuentes accesibles al público. c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica. 3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar. 4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable. 5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley. 6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores."*, B.O.E., núm. 298, de 14 de diciembre de 1999, pág. 43090.

Al margen de la necesidad u obligatoriedad del consentimiento para la cesión de datos a terceros, deberá cumplirse siempre y debidamente con el derecho de información establecido en el art. 5 de la LOPD.

Según Cristina Almuzara[267], "*para que no entre en juego el consentimiento como requisito previo, es necesario que las finalidades a las que se destinen los datos sean única y exclusivamente para el desarrollo, cumplimiento y control de las relaciones contractuales y precontractuales, (cesiones habituales a entidades bancarias y financieras para la tramitación de cobros y pagos de nóminas…) o que la misma sea exigida legalmente, como el típico caso de las cesiones a la Administración Tributaria para liquidaciones de IRPF o a la Seguridad Social del Ministerio para dar cumplimiento a las obligaciones laborales, como la tramitación de impresos TC1 o TC2, etcétera*".

En el resto de supuestos, y salvo ley que diga otra cosa, el consentimiento inequívoco del interesado debe ser recabado.

El más potente Medio de Comunicación de nuestra sociedad, la televisión, está incurriendo en cesiones irregulares de datos[268], al recogerlos para un sorteo o concurso y desviando esa información para actividades comerciales, de publicidad o marketing, que suelen ser realizadas por otras compañías, constituyendo por tanto comunicación de datos. Al tener presente lo que establece el art. 11 de la LOPD, esa comunicación o cesión de datos solo podrá efectuarse cuando el participante en el sorteo o concurso tenga conocimiento de la misma y la haya consentido previamente, lo que no suele ocurre en la práctica, a tenor de la Inspección que efectuó la Agencia Española de Protección de Datos.

De hecho, consta el caso de una cadena de televisión que ha llegado a comercializar datos personales de concursantes, ofreciéndolos a una compañía que los recopilaba con fines de marketing directo para alquilarlos a las empresas interesadas, actividad esta que suele conocerse como '*listbroking*'[269]. La compañía de marketing se comprometía a actuar como agente para la explotación comercial del fichero.

---

[267] ALMUZARA ALMAIDA, Cristina: '*Estudio Práctico sobre la Protección de Datos de Carácter Personal' .Capítulo XVII, Los Códigos Tipo*. Lex Nova, Valladolid, 2007, pág. 284.

[268] Informe de la Agencia de Protección de Datos sobre 'Inspección Sectorial de oficio 'Concursos, juegos y sorteos de TV' de octubre de 2002: op. cit., pág. 12.

[269] Ibídem, pág. 13.

Aunque hay bastante normativa que especifica la necesidad o no de consentimiento del interesado para hacer uso de sus datos personales, citemos aquí, como caso práctico de interés, el que utiliza C. Almuzara[270], aquel que se da cuando se produce cesión de datos personales con motivo de la realización de un programa formativo destinado a mejorar el nivel técnico del personal. Son programas de formación que suelen estar financiados en parte por la empresa y en parte por la Administración a través de subvenciones. Para que el centro o entidad formadora pruebe la participación de personas en los cursos se pide al trabajador que firme un cuestionario, normalmente impreso por la entidad o empresa desde su sistema de nómina, en el que aparecen los datos referidos a nombre y apellidos, DNI, número de Seguridad Social, sexo, fecha de nacimiento, teléfono particular, teléfono de la empresa y domicilio de residencia habitual. Supongamos que el trabajador se queja formalmente a sus directores sobre la cesión de datos personales (dirección y teléfono particular), siendo informado de que estos datos son imprescindibles para la solicitud de la subvención y que la alternativa pasa por renunciar al programa de formación.

Algunos de los datos solicitados pueden resultarnos excesivos, como el teléfono particular o el domicilio, para la realización de unos cursos que se circunscriben en el ámbito propio de la empresa donde trabaja, como indicó el Informe 161/2003 de la Agencia Española de Protección de Datos[271].

La cesión de los datos solicitados (no sólo teléfono y domicilio particular), para esta finalidad no se recoge de modo específico por las normas y, dado que de conformidad con el art. 4.2 apartado b) de la Ley de Estatuto de los Trabajadores[272], la formación profesional en el trabajo tiene carácter de derecho y no de obligación, se hace necesario solicitar el consentimiento del trabajador para la realización del curso y, en ese momento, se le deberá informar de que la aceptación implica automáticamente la cesión de sus datos a un tercer organismo.

---

270 ALMUZARA ALMAIDA, C.: op. cit., pág. 287.

271 Informe sobre cesión al INEM para la gestión de ayudas a planes de formación: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2003-0161_Cesi-oo-n-al-INEM-para-la-gesti-oo-n-de-ayudas-a-planes-de-formaci-oo-n..pdf>.

272 B.O.E., núm. 75, de 29/3/1995, pág. 9657.

Utilizamos este ejemplo gráfico porque numerosas empresas de Medios de Comunicación pueden caer en una práctica similar. A la hora de manejar datos personales obtenidos para un fin concreto, puede ser cedidos a otra sociedad del mismo grupo empresarial para una utilización distinta o desviada de la que inicialmente justificó la tenencia de aquellos datos de carácter personal.

En este sentido, y sabiendo que, según F. Coudert, "*los grupos de empresas son los grandes olvidados de la regulación en materia de protección de datos tanto a nivel internacional, comunitario y* nacional"[273], la LOPD no toma en cuenta la peculiaridad de la estructura de los grupos empresariales y exige a cada una de ellas lo mismo.

La cesión de datos por parte del empresario a las Administraciones Públicas constituye otro caso muy frecuente en la práctica que interesa tener bien presente. Tengamos en cuenta que por Administraciones Públicas se entiende, entre otras muchas instancias, el INEM, el nuevo SAE, la Tesorería de la Seguridad Social, la Hacienda Pública, etc., y están encuadradas en la excepción a la regla general del consentimiento del afectado. Sí conviene saber que el R.D. 214/1999, de 5 de febrero, por el que se aprueba el Reglamento del Impuesto sobre la Renta de las Personas Físicas (IRPF), establece la comunicación de determinados datos de los perceptores de rentas de trabajo a su pagador en los siguientes términos: "*Los contribuyentes deberán comunicar al pagador la situación personal y familiar que influye en el importe excepcionado de retener, en la determinación del tipo de retención o en las regulaciones de éste, quedando obligado, asimismo, el pagador a conservar la comunicación debidamente firmada. El contenido de las comunicaciones se ajustará al modelo que se apruebe por la Agencia Estatal de la Administración Tributaria*"[274].

En esos modelos de comunicación (Resolución de 28 de diciembre de 1999 del Departamento de Gestión Tributaria de la Agencia Tributaria)[275] de la situación personal y familiar del perceptor de rentas del trabajo, o de sus cambios, ante el pagador, se especifica la forma en que debe efectuarse

[273] COUDERT FANNY: *Estudio práctico sobre la protección de Datos de Carácter Personal. Capítulo* V, *Relaciones con otras Empresas*. Editorial Lex Nova, Madrid, Marzo 2007, pág. 316.

[274] B.O.E., núm. 60, de 10 marzo 2004, pág. 10670.

[275]<http://www.aeat.es/AEAT.internet/Inicio_es_ES/La_Agencia_Tributaria/Normativa/Normativa_reguladora_de_la_AEAT/Resoluciones/Resoluciones.shtml>.

dicha comunicación, estableciendo que se deben declarar como circunstancias personales el grado de discapacidad propia y/o de los hijos o descendientes (dato, éste último, que se considera como dato de salud, es decir, es un dato especialmente protegido).

Son, por tanto, cesiones de datos de carácter personal obligadas y reguladas por ley.

3.2.2.8. Acceso a los datos por cuenta de terceros.

El acceso a los datos por cuenta de terceros no se considera cesión de datos cuando se realiza para la prestación de un servicio. Al regularse, la figura del encargado del tratamiento como la persona física o jurídica que presta servicio al responsable del fichero o tratamiento, se está advirtiendo que todo lo que no sea responsable o persona autorizada, incurrirá en caso de incumplimiento.

Existe la posibilidad de que estemos ante una prestación de servicio. Es decir, los tratamientos de datos que no sean realizados por trabajadores al servicio del responsable del fichero, sino por terceras personas –normalmente empresas- que presten servicios que supongan el tratamiento de datos personales no se considerará acceso ilegal por cuenta de terceros. Los requisitos que deben contener los contratos de prestación de servicios son señalados en el art. 12 de la LOPD[276]. Lo más importante es que, teniendo en cuenta el análisis de C. Almuzara, "*el acceso a los datos por cuenta de terceros debe estar regulada en un contrato escrito o en alguna otra forma que permita acreditar su celebración y contenido*"[277].

El encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento y no los utilizará para fines distintos a los que figuren en el contrato. Una vez cumplida la prestación del acuerdo o contrato, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento. El encargado del tratamiento tendrá la misma responsabilidad que el responsable del fichero si los comunica o utiliza incumpliendo las estipulaciones del contrato.

El objetivo de estas medidas es garantizar que se está efectuando un tratamiento de datos seguro, así como conservar la confidencialidad de los

[276] Ley 15/1999, B.O.E., núm. 298 de 14/12/1999: op. cit., pág. 43091.

.

[277] ALMUZARA ALMAIDA, C.: op. cit., pág. 298.

datos prohibiendo al encargado del tratamiento su transmisión a un tercero ni siquiera para su conservación.

Es precisamente la necesidad de regularse en un contrato escrito donde muchas televisiones y también emisoras de radio están incurriendo en infracción por no respetar este punto.

En general, la productora de un formato televisivo y la cadena de televisión que lo emite están vinculadas contractualmente, aunque no se regula documentalmente el tratamiento que ambas realizan respecto de los datos personales de la audiencia. Estos contratos, sin embargo, cuando existen documentalmente, no siempre especifican quién es el responsable del fichero y en ocasiones sólo hacen una vaga referencia al carácter confidencial de la prestación del servicio, no detallando las condiciones en que debería realizarse ésta. En este sentido, no siempre se establece expresamente "*que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas*"[278], tal como prevé el apartado 2 del citado artículo 12. De la misma manera, tampoco siempre se estipulan contractualmente las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

Esta ausencia de normas documentadas es más frecuente en los servicios automáticos (906, 908, etc. o SMS) de recogida de datos que se prestan para la celebración de sorteos, aunque son éstos más numerosos que los que se prestan en los procesos de selección de concursantes. Además, tampoco en tales casos se estipula el destino de los datos una vez cumplida la prestación contractual, a pesar de lo que establece el apartado 3 del artículo 12 de la LOPD. Los datos recogidos a través de los 906 y similares no se conservan generalmente durante un largo período después del sorteo, aunque no ocurre lo mismo con los que se obtienen a través de mensajes SMS[279].

Una práctica muy común en el sector de audiotex y las televisiones es la compartición del tráfico de llamadas en situaciones de congestión de la red telefónica. Esta situación tiene graves consecuencias pues ocasiona

[278] Ibídem, pág. 298.

[279] Informe de la Agencia de Protección de Datos sobre 'Inspección Sectorial de oficio 'Concursos, juegos y sorteos de TV' de octubre de 2002: op. cit., pág. 10.

que, a veces, los interesados puedan creer que están facilitando sus datos a una compañía de televisión cuando, en realidad, los están recibiendo, a través de sus propios servidores, compañías que no están vinculadas contractualmente con ésta. Es más, según ha podido comprobar la Agencia española, las compañías que reciben las llamadas desviadas y, por tanto, los datos personales de los participantes, ni siquiera han suscrito contrato con la compañía a la que se encarga el servicio de audiotex. El resultado es que no existen garantías para los interesados respecto al tratamiento que se dará a los datos facilitados por teléfono.

3.2.3. Derechos de los ciudadanos.

3.2.3.1. El derecho de impugnación de valoraciones.

El art. 13 de la LOPD[280] recoge un derecho que se otorga a los ciudadanos "*a no verse sometidos a una decisión que tenga efectos jurídicos sobre sí mismos o que les afecte de alguna manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o de su personalidad"*. Este derecho les es reconocido a las Administraciones Públicas y a las entidades privadas.

El interesado en impugnar valoraciones tiene derecho a obtener información del responsable del tratamiento sobre los criterios que ha tenido para hacer la valoración y el programa que ha utilizado en el tratamiento que haya válido para tomar la decisión. No ha tenido mayor desarrollo este derecho recogido en la LOPD y por eso no se contemplan plazos ni requisitos más concretos para ejercitarlo.

Conviene enmarcar aquí una dinámica que suele darse con bastante frecuencia en la actividad bancaria en la que puede entrar en juego el derecho de impugnación de valores. Consiste en asignar una puntuación o un baremo por la que una entidad financiera califica la aptitud o capacidad crediticia de una persona, posible cliente, en base a unos criterios determinados previamente, como explica F. Coudert[281], la práctica que se da es que "*un operador facilita a otra entidad especializada una*

[280] Ley 15/1999, B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43091.

[281] COUDERT FANNY: op. cit., pág. 418

información sobre solvencia patrimonial y crédito en relación con sus propios o potenciales clientes, con información sobre capacidad crediticia de cada uno de esos clientes, lo que sirve al operador para poder rechazar o no la solicitud del servicio realizada por el potencial cliente. La Agencia Española de Protección de Datos estima que estos tratamientos permiten facilitar decisiones como el otorgamiento de créditos o tratamientos automatizados que, a partir de los datos del interesado, describen un perfil de su personalidad".

Estos datos, siempre que fundamenten una decisión sobre el interesado que desencadene consecuencias jurídicas, como conceder un préstamo hipotecario o un crédito personal, pueden ser impugnados en virtud del art. 13 de la LOPD.

3.2.3.2. La consulta al Registro General de Protección de Datos.

Es el art. 14 de la LOPD[282] el que refleja este derecho que tiene "*cualquier persona a conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos personales, sus finalidades y la identidad del responsable del tratamiento. El Registro General es de consulta pública y gratuita".*

Estamos, por tanto, ante un derecho abierto a todo ciudadano y sin ninguna limitación para ejercitarlo. De hecho, la Agencia Española de Protección de Datos publica todos los años un CD-Rom con la relación de todos los ficheros inscritos legalmente, con las direcciones a las que los interesados pueden dirigirse para ejercitar sus derechos de acceso, rectificación, cancelación y oposición. Suele haber dos tipos de consultas: las efectuadas para obtener la dirección del responsable del fichero en el que se encuentran sus datos para poder ejercitar sus derechos[283].

De otro lado, las efectuadas por los propios responsables de los ficheros, que suelen solicitar formularios de notificación de los ficheros en los que pueden comprobar los detalles que han sido incluidos. Copia ésta que sólo se concede a quienes acrediten un interés suficiente.

---

[282] B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43091.

[283] Disponibles todos ellos, actualizados, en la página web de la Agencia Española de Protección de Datos: <http://www.agpd.es/portalwebAGPD/ficheros_inscritos/index-ides-idphp.php>.

3.2.3.3. Los derechos de acceso, rectificación, cancelación y oposición.

El derecho de acceso a los datos personales es el principal de los derechos que asisten al afectado pues otorga la facultad para conocer la información que está siendo objeto de tratamiento y posibilita capacidad de control sobre los datos.

Tiene el interesado "*el derecho a solicitar y obtener gratuitamente información de sus datos personales sometidos a tratamiento, el origen de los mismos, y las comunicaciones que han sido efectuadas o están previstas hacer de los mismos",* según establece el art. 15 de la LOPD[284].

El responsable del tratamiento de datos dispone de un mes (a contar desde la recepción de la solicitud) para dar respuesta a esa petición de acceso, en caso de que no pueda disponer de los datos, tendrá el deber de hacérselo saber. Sólo puede denegarse el ejercicio de este derecho cuando el interesado haya intentado el acceso durante los doce meses anteriores a ese momento y no acredite interés legítimo que justifique le necesidad de volver a ejercer el derecho.

Una vez resuelta positivamente la petición, el acceso podrá realizarse efectivo en el plazo de diez días siguientes a su notificación. La información que se conceda deberá ser todos los datos de base del interesado, los resultantes de cualquier elaboración o proceso informático, el origen de los datos, los cesionarios de los mismos y la concreción de usos y finalidades para los que se almacenan.

Si la petición es denegada, el interesado puede interponer la reclamación prevista en el art. 18 de la LOPD[285] (tutela de los derechos), que veremos seguidamente.

El derecho de rectificación asiste al interesado a poder solicitar al responsable del tratamiento la rectificación de los datos personales que sean "*inexactos o incompletos. El plazo que tiene el responsable del tratamiento es de diez días*", como establece el art. 16 de la Ley[286], si bien en caso de ser imposible la rectificación deberá cancelar de oficio los datos tratados, por no ser actualizada ni responder a la situación real del afectado. Si los datos rectificados han sido antes comunicados a terceros, el

[284] B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43091.

[285] Ibídem, págs. 43091 y 43092.

[286] Ib. pág. 43091.

responsable deberá notificar en el mismo plazo de diez días la rectificación efectuada a quien se haya comunicado y el tercero deberá proceder a la rectificación de los datos.

El responsable del tratamiento tiene, no obstante, la facultad de rectificar, de oficio, a instancia propia, los datos que revelen ser incompletos, inexactos o no actualizados.

El derecho de cancelación es otro de los derechos que puede solicitar el interesado, bien porque haya decidido revocar el consentimiento que dio en el instante de la recogida de datos, o bien porque han podido manejarse sus datos sin su consentimiento y decide oponerse.

También dispone de diez días (siguientes a la recepción de la solicitud) el responsable del tratamiento para hacer efectiva la cancelación, si bien podrá no atenderla comunicándolo motivadamente dentro de ese plazo. Si los datos cancelados han sido comunicados antes a terceros, éstos deberán proceder a la cancelación a instancias del responsable del tratamiento.

La cancelación se concreta con el borrado físico de los datos personales. No basta con una marca o señalización, ni tampoco con el mantenimiento de otro fichero alternativo que registre bajas producidas.

Puede que se proceda sólo a su "*bloqueo*"[287], como expresa el art. 16.3 de la Ley, para que se conserven única y exclusivamente para su eventual uso por las Administraciones, jueces y tribunales. "*Se recomienda conservar los datos bloqueados durante los plazos de prescripción marcados por la LOPD para atender y depurar posibles responsabilidades surgidas del tratamiento de esos datos*", en opinión de F. Coudert[288], es decir, un año para infracciones leves, dos años para infracciones graves y tres años para las muy graves, que cuentan a partir del final del tratamiento.

Este bloqueo de datos en lugar de proceder a su eliminación física definitiva es una decisión que ha de tomar el responsable del tratamiento justificada bien en una disposición legal que así lo establezca, o bien en la existencia de una relación jurídica que le vincula al titular de los datos, legitimando el bloqueo y no eliminación ante la posibilidad de que puedan ser requeridos esos datos como medio de prueba a disposición de

[287] Ib. pág. 43091.

[288] COUDERT FANNY: op. cit., pág. 415.

Administraciones, jueces y tribunales. En ningún otro caso pueden ser bloqueados y no eliminados[289].

El derecho de oposición queda recogido en los artículos 6.4 y 30.4 de la LOPD. En el primero de los preceptos, se faculta al interesado a que podrá oponerse al tratamiento de sus datos si no ha sido necesario su consentimiento siempre y cuando una ley no disponga lo contrario y si se dan motivos fundados y legítimos.

En el segundo caso, que supone excepción a la exigencia de motivo fundado y legítimo, en tratamientos con fines de publicidad y de prospección comercial, los interesados tienen derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren, a su simple solicitud.

Sostiene F. Coudert que "e*l responsable del tratamiento de los datos, al recibir solicitud de ejercitar el derecho de oposición deberá comprobar la existencia de ese motivo fundado y legítimo relativo a una concreta situación personal, en caso de que proceda*"[290]. Dispone de un plazo de un mes para contestar al interesado, indicándole si acepta o deniega la solicitud así como para la adopción de medidas que oscilarán entre o bien abstenerse a realizar determinada acción, o bien cancelar los datos. Podrá bloquearlos por cierto tiempo si son necesarios para posibles responsabilidades, tal y como se ha indicado más arriba.

Requisitos. Para el ejercicio de estos derechos es necesaria una solicitud dirigida al responsable del tratamiento, que deberá contener, como mínimo: nombre, apellidos y fotocopia del DNI del interesado; petición concretando la solicitud; domicilio a efectos de notificaciones, fecha y firma del solicitante; documentos acreditativos de la petición que se formula (en la rectificación y en la cancelación).

Es importante atenerse en todo esto a lo establecido en la Instrucción 1/1998, de 19 de enero,[291] de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación que regula, entre otras cosas, los requisitos que acabamos de citar en la solicitud dirigida al responsable del fichero y establece la obligación a éste último de contestar la solicitud que se le dirija, con independencia de que

289 Ibídem, pág. 415.

290 Ib., pág. 416.

291 B.O.E., núm. 24, de 28/01/2002, Sec 3, pág. 3.468.

figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción.

3.2.3.4. Tutela de los derechos.

La tutela de los derechos que acabamos de enumerar queda en manos de la Agencia Española de Protección de Datos, o de los organismos competentes que haya en cada Comunidad Autónoma. Como establece el art. 18 de la LOPD, el interesado al que se deniegue total o parcialmente el ejercicio de los derechos de oposición, acceso, rectificación o cancelación podrá reclamarlo.

La resolución expresa debe dictarse, según indica el art. 18.3, en el plazo máximo de seis meses. A partir de la resolución de la Agencia de Protección de Datos, se pone fin a la vía administrativa y habrá que acudir a los tribunales de lo contencioso-administrativo. Es decir, contra las resoluciones de la Agencia, cabe interponer recurso contencioso-administrativo. La tutela de derechos es la principal fuente de motivos para la emisión de resoluciones por parte de la Agencia Española de Protección de Datos, como puede comprobarse en su página web[292].

3.2.3.5. Derecho a indemnización.

La ley reconoce el derecho de los interesados a recibir una indemnización por los daños o lesiones que sufran en sus bienes o derechos como consecuencia del incumplimiento de sus previsiones por el responsable o el encargado del tratamiento (art.19 LOPD). Este derecho a indemnización por daños es preexistente a la propia Ley de Protección de Datos pues deriva del sistema general del concepto de responsabilidad civil y administrativa.

Cuando este daño se invoca por el tratamiento de fichero público contradictorio con la ley de protección de datos, ese daño será antijurídico y deberá ser inmunizado, siendo jurisdicción competente la contencioso-administrativa (art. 9.4 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial)[293], y bajo los principios de la Ley 30/1992 de Procedimiento

[292] Resoluciones de la Agencia Española de Protección de Datos sobre la tutela de derechos: < https://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/index-ides-idphp.php>.

[293] B.O.E., núm. 157, de 02/07/1985, pág. 20632.

Administrativo Común. Si la cesión ilegal se ha hecho a otra Administración, podríamos estar ante un caso del que habrán de responder ambas Administraciones Públicas (art.140.2 Ley 30/1992)[294].

Si la cesión ilegal se ha hecho desde fichero de titularidad privada, la LOPD dice que se ejercitará la acción de reclamación de indemnización ante la jurisdicción ordinaria, pues parte del convencimiento tanto teórico práctico como de que el comportamiento implicará, cuando menos, una fuerte carga de culpa. Rige, por tanto, el principio de responsabilidad contractual de los artículos 1902 y siguientes del Código Civil[295].

3.2.4. Deberes y obligaciones de las empresas y entidades.

3.2.4.1. Notificación e inscripción de ficheros en el Registro General de la Agencia de Protección de Datos.

Al Registro General de Protección Datos le corresponde velar por la publicidad de la existencia de los ficheros y tratamientos de datos de carácter personal. El Registro General hace posible a los interesados ejercitar los derechos de información y los derechos fundamentales de a acceso, rectificación, cancelación y oposición. La instrucción de los expedientes de inscripción la lleva a cabo el Registro General expidiendo certificaciones de los asientos y con la publicación anual de los ficheros notificados e inscritos.

Están obligados a notificar la creación de ficheros para su inscripción en el Registro General, de acuerdo con lo dispuesto en la Ley Orgánica 15/99, aquellas personas físicas o jurídicas, de naturaleza pública o privada, u órgano administrativo, que procedan a la creación de ficheros que contengan datos personales.

La creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" (BOE) o diario oficial correspondiente.

---

294 B.O.E., núm. 285, de 27/11/1992, pág. 40300.

295 Real decreto de 24 de julio de 1889 por el que se publica el Código Civil. B.O.E., núm. 206, de 25/07/1889. Véase: <http://www.boe.es/datos/pdfs/BOE/1889/206/R00249-00312.pdf>.

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y "*se respeten las garantías establecidas*" expresamente en la Ley Orgánica de Protección de Datos, como recoge su art. 25[296].

Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección.

Cualquier modificación posterior en el contenido de la inscripción de un fichero en el Registro General de Protección de Datos, deberá comunicarse, por el responsable del mismo, a la Agencia mediante una solicitud de modificación o de supresión de la inscripción, según corresponda. En ambos casos será necesario citar el Código de Inscripción asignado al fichero por el Registro General. En el art. 39 de la LOPD se relacionan los ficheros susceptibles de inscribir[297].

La notificación y la correspondiente inscripción del fichero parece un mero trámite, pero puede aportar como efecto directo un clima de mayor confianza por parte de los titulares de los datos en aquellas empresas y/o entidades que mantengan inscritos debida y correctamente sus ficheros.

Para proceder a la notificación e inscripción de ficheros, la Agencia Española de Protección de Datos facilita desde su página web soportes con los distintos formularios, aprobados por la Resolución de 30 de mayo de 2000 (modelos normalizados en soporte papel, magnético y telemático) dirigidos a los responsables de los ficheros y que, por su importancia, fue publicada en el Boletín Oficial del Estado[298]. La no notificación de la existencia de un fichero supondría una infracción leve o grave.

3.2.4.2. Tratamiento legal y leal de los datos: respecto a los Principios y Derechos anteriores.

Como la LOPD recoge toda esta serie de principios, derechos y obligaciones que han de observarse en el tratamiento de datos de carácter

[296] B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43093.

[297] Ibídem, pág. 43096.

[298] B.O.E., núm. 153, de 27/6/2000, pág. 22624.

personal, se hace necesario establecer los mecanismos y procedimientos adecuados y necesarios, como remarca C. Almuzara, con el fin de llevar a cabo un tratamiento legal y leal de los datos personales[299].

Se trata de que el respeto a todos los principios que inspiran el espíritu de la ley sea la esencia de toda acción. Es importante que quien trate datos, responsable o encargado del tratamiento, observe todas las disposiciones en las diversas fases en las que se concreta: recogida, tratamiento y utilización o cesión o comunicación de los datos.

Implica todo ello la necesidad de adoptar los procedimientos necesarios con el fin de adecuar dichos tratamientos a la normativa vigente, en su caso mediante acciones como la adecuación de las cláusulas contractuales a dicha normativa; la suscripción de los correspondientes contratos de prestación de servicios; la elaboración del Documento de Seguridad que se prevé en el art. 88 del Reglamento 1720/2007 de desarrollo de la LOPD[300] y las medidas de seguridad que recoge; o el establecimiento de procedimientos que faciliten el ejercicio de los derechos de los afectados, y todo ello con el fin de garantizar al interesado un correcto tratamiento de sus datos.

En resumen, se trata de conocer el nivel de riesgo que corre el empresario, ejecutivo o la persona que toma decisiones en la empresa, con el tratamiento de datos de carácter personal, adoptando las medidas para minimizar riesgos.

3.3. El Reglamento de 2007 que desarrolla la L.O.P.D.

Tras ocho años de espera por parte de profesionales, especialistas, doctrina y tribunales, fue en diciembre de 2007 cuando, al fin, salió a la luz el esperado Real Decreto 1720/2007 por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (RLOPD)[301]. La nueva norma comparte con la LOPD la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de los datos personales.

---

299 ALMUZARA ALMAIDA, C.: op. cit., pág. 146.

300 B.O.E., núm. 17, de 19/1/2008, pág. 4126.

301 Ibídem, pág. 4103.

Llamada a clarificar conceptos y disposiciones, la norma pretende desarrollar la actual LOPD, tanto en su normativa jurídica como técnica, (ya que el anterior Reglamento de Medidas de Seguridad estaba desarrollando la antigua LORTAD de 1992) además de incorporar las subsistentes normas reglamentarias, las competencias en materia sancionadora y las instrucciones que la Agencia Española de Protección de Datos había publicado hasta el momento para la mejor interpretación de la LOPD 15/1999.

3.3.1. Novedades destacadas.

Las principales novedades que introdujo provienen tanto del ámbito legislativo como del ámbito de la seguridad, puesto que no sólo se ocupa del aspecto técnico, sino que desarrolla también el aspecto normativo de la LOPD, según recoge Mª Isabel Patón, abogada especializada en nuevas tecnologías y miembro del Servicio Jurídico de la Asociación para la Conciliación de las Libertades y la Información[302], que condensa lo nuevo que trajo esta norma advirtiendo que el Real Decreto 1720/2007 con el Reglamento (RLOPD), "*comprende tanto el tratamiento automatizado como el no automatizado de los datos personales. Amplía las definiciones y aparece como novedad, la definición de usuario. Fija el criterio en materia de cómputo de plazos, evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados. Da particular importancia a la regulación del modo de captación del consentimiento y cambia el nivel de protección de determinados datos personales. Además, establece que no es de aplicación a los tratamientos referidos a personas jurídicas, ni a los datos de personas físicas que presten sus servicios en aquellas, y los datos referidos a los empresarios individuales cuando hagan referencia a ellos en su calidad de comerciantes y ofrece un desarrollo de la forma de ejercitar los derechos de los afectados: derecho de acceso, rectificación, cancelación y oposición*".

Estas novedades se complementan con la inclusión de las medidas de seguridad en el Título VIII del propio texto normativo[303]. Se prevé, por primera vez, las medidas de seguridad en los ficheros no automatizados, es decir, los ficheros en papel que todavía, a fecha de 2007, seguían existiendo.

---

[302] < http://www.borrmart.es/articulo_redseguridad.php?id=1795>.

[303] B.O.E., núm. 17, de 19/1/2008, op. cit., pág. 4125.

Para poder desarrollar las medidas de seguridad y lo relacionado con el Documento de Seguridad y la Auditoría preceptiva, es necesario tener en cuenta las modificaciones y novedades que introduce este RLOPD en relación con el tratamiento de determinados datos, y que son dos fundamentales, según la abogada María Isabel Patón:

"*-Desaparece el nivel medio atenuado distinguiéndose ahora entre el nivel medio y el nivel medio con las excepciones del Art. 103 RLOPD.*

-La obligación establecida en la Disposición Adicional Única del Reglamento sobre los software destinados al tratamiento automatizado de datos personales, que deberían incluir en su descripción técnica el nivel de seguridad (básico, medio o alto). Según algunos, esta obligación es de difícil cumplimiento debido a la imposibilidad de conocer a priori de estimar la naturaleza de los datos que van a ser tratados con estas herramientas"[304].

3.3.2. Documento de Seguridad en el Reglamento.

Atención especial deberán prestar todas las empresas de Medios de Comunicación Social a lo que se establece ahora para el Documento de Seguridad, el cual es tratado con detalle en el nuevo Reglamento, comenzando desde el Art. 88 con normas generales como las de sus apartados 3 y 4[305]:

"*3. a) Ámbito de aplicación y recursos protegidos (medidas básicas).*
b). Medidas, normas, procedimientos y reglas (nivel básico).
c). Funciones y obligaciones del personal (nivel básico).
d). Estructura de los ficheros y sistemas (nivel básico).
e). Procedimiento sobre incidencias (nivel básico).
f). Procedimientos de copias de respaldo y recuperación (nivel básico).
g). Medidas a adoptar para la destrucción, reutilización y transporte de soportes y documentos (nivel básico). Esta es una novedad para el nivel básico puesto que antes se implantaban estas medidas sólo a los niveles medio y alto.
4. a). Identificación del Responsable de Seguridad (nivel básico y medio).

[304] <http://www.borrmart.es/articulo_redseguridad.php?id=1795>, op. cit.

[305] Artículo 88, apartados 3 y 4 del Real Decreto 1720/2007, B.O.E., núm. 17, de 19/01/2008, op. cit., pág. 4126.

b). Controles periódicos de verificación (nivel medio y alto)".

Hay obligación de incluir más aspectos en el Documento de Seguridad, contemplados en los artículos 90 al 94, entre los que destacan[306]:

1. El régimen de trabajo fuera de los locales del responsable o encargado: deberá autorizarse por el Responsable para un usuario o para un perfil de usuarios y deberá especificarse el período de validez de dicha autorización. Se incluyen de forma específica el trabajo en dispositivos portátiles.

2. Los controles de acceso que se deben conceder o no para acceder a los lugares donde se encuentren los equipos físicos.

3. La gestión de soportes y documentos, estableciendo y registrando al personal con acceso autorizado (no son válidos los usuarios genéricos), así como la salida de soportes y documentos.

4. El período de cambio de contraseñas.

5. El personal que debe controlar las copias de documentos.

3.3.3. Encargado de Tratamiento.

El RLOPD es un buen punto de partida para abarcar el ámbito tutelado anteriormente y para que los profesionales profundicen aún más en esta materia. Dentro del Documento de Seguridad aparecen con contenido específico y con especial relevancia el Encargado de Tratamiento (el "estatuto" del encargado de tratamiento), puesto que deberá contener lo que establece su art. 82[307]:

- la identificación de los ficheros o tratamientos que se traten en concepto de encargado;

- referencia expresa al contrato o documento de encargo;

- identificación del responsable;

- vigencia del encargo.

306 Ibídem, págs. 4127 y 4128.

307 Ib., pág. 4126.

3.3.4. Varias excepciones.

El R.D. 1720/2007 (RLOPD)[308] establece una serie de excepciones a la implantación de estas medidas dentro de su articulado:

A. En su art. 101 se establece que "*se hará constar motivadamente en el Documento de Seguridad el tratamiento de datos de carácter personal de ficheros de nivel alto automatizados en dispositivos portátiles que no permitan su cifrado y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos*".

B. La excepción de realización de registros de accesos en determinadas circunstancias enumeradas en el art. 103.6 del RLOPD en ficheros de nivel alto automatizados.

C. La excepción en la aplicación de medidas de nivel alto en ficheros no automatizados en el almacenamiento de la información establecida en el art. 111.2 del RLOPD.

3.3.4. Auditoría profesional.

En relación con la auditoría de medidas de seguridad, se especifica que puede ser interna o externa y abarca tanto a los ficheros automatizados como a los no automatizados (Art. 110 y 96 RLOPD) y "*deben estar a disposición de la Agencia Española de Protección de Datos o autoridades de control de la Comunidades Autónomas*", expresa el art. 96.3[309].

Sigue instaurándose la obligatoriedad de realizarla al menos cada dos años pero, además, la nueva norma establece una auditoría extraordinaria cuando se produzcan cambios relevantes, o sustanciales en:

a. El sistema de información e instalaciones.

b. El sistema de tratamiento y almacenamiento.

[308] Ib., pág. 4103.

[309] Ib., pág. 4128.

c. El la información incluida en el documento.

Podrá entenderse como cambio relevante todo aquél que pueda repercutir en el cumplimiento de las medidas de seguridad. "*Esta auditoría extraordinaria inicia de nuevo el cómputo de los dos años*", señala el art. 96.1, para la realización de la siguiente auditoría correspondiente[310].

3.3.6. Plazos de aplicación.

Para su aplicación, los plazos que se han estipulado son recogidos en la propia normativa. La entrada en vigor del Reglamento, RD 1720/2007, se estableció para pasados tres meses desde su publicación, y no tres días[311], y comenzó a partir del 19 de abril de 2008. A partir de esta fecha comenzaron a contar los cómputos de los plazos para la implantación de todos sus preceptos.

La indefinición jurídica del nuevo Reglamento ha planteado dudas. Deja aún muchos aspectos sin regular cuya interpretación deberá esperar a su clarificación por los tribunales y por la Agencia Española de Protección de Datos. Sin embargo, es un buen punto de partida para abarcar el ámbito tutelado anteriormente y para seguir profundizando más en el tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal.

Mención especial aparte merece la existencia aún de ficheros sobre datos personales en papel. Con motivo de la publicación RD 1720/2007, Landwell-PwC reeditó el informe publicado en 2008 sobre el tratamiento de los datos en papel en la empresa española. Entre las conclusiones del mismo destaca que el 63% de las empresas españolas no disponía de normas de seguridad específicas para proteger los datos de carácter personal en soporte papel[312].

El informe reveló que las empresas españolas no estaban en condiciones de cumplir el nuevo Reglamento y que tendrían que invertir entre 3.000 y 90.000 euros, si hacemos la suma del conjunto de todas, siempre según su tamaño y necesidades, para adaptar sus políticas a dicha normativa.

---

310 Ib., pág. 4128.

311 Ib., pág. 4106.

312 Informe completo en la página web de Xavier Ribas: <http://xribas.typepad.com/>.

El 27% de las empresas encuestadas dispone de una metodología para clasificar y almacenar los documentos con datos personales o con información confidencial. Tres de cada diez compañías no controlaban el acceso a los documentos en soporte papel y apenas un 18% de las mismas tenía un responsable de seguridad de los datos con competencias en materia de documentos en papel[313].

3.3.7. La adopción de medidas de seguridad: El Documento de Seguridad.

La adopción de medidas de seguridad sobre los datos de carácter personal supone la obligatoria elaboración de un Documento de Seguridad, cuyo contenido mínimo obligatorio viene establecido por el artículo 88 del Reglamento 1720/2007 de desarrollo de la LOPD[314] y que, por tanto, ha de tener elaborado y actualizado todo Medio de Comunicación.

La Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, establece que garantizada la seguridad de los datos, resulta legítimo el tratamiento de datos personales. Lo que, a sensu contrario, pone de manifiesto que, si no es así, no resultan legítimas las operaciones que se hagan con datos personales[315].

Deben poner en práctica tanto los responsables de los ficheros como los responsables del tratamiento de datos personales la adopción de medidas de carácter técnico y organizativo adecuadas para garantizar un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y atendiendo a la naturaleza de los datos que deban protegerse.

Se trata de tener preparada y lista una estructura organizativa que en el ámbito interno del responsable o del encargado del tratamiento debe existir para dar cuenta de las necesidades que conlleva la protección de datos personales. Todo ello en un Documento de Seguridad, así denominado por la nueva norma.

---

313 Ibídem, pág. 2.

314 B.O.E., núm. 17, de 19/1/2008, op. cit., pág. 4126.

315 STC 292/2000, de 30 de noviembre de 2000, que resuelve el recurso de inconstitucionalidad núm. 1463-2000 interpuesto por el Defensor del Pueblo contra los artículos 21.1 y 24.1 y 2 de la LOPD. B.O.E. Núm. 4, suplemento de 4/01/2001, pág.104.

La adopción de medidas de seguridad tiene como fin evitar, en especial, la comunicación o el acceso no autorizados, la destrucción accidental o ilícita, así como cualquier pérdida o alteración, o bien cualquier otra forma no permitida de tratamiento. Evitar, desde luego, que personas no autorizadas puedan acceder a los sistemas informáticos que traten o almacenen datos personales.

Según Ana Marzo, para poder llevar a cabo el tratamiento de datos personales y, con carácter general, para todos los niveles de seguridad, es necesario, como mínimo, adoptar las siguientes medidas:

- ✓ "*Los accesos a datos personales a través de redes de comunicación deberán garantizar el nivel de seguridad equivalente al correspondiente a los accesos en modo local.*
- ✓ *La ejecución de tratamiento de datos personales fuera de los locales de ubicación del fichero debe ser autorizada expresamente por el responsable del fichero y, en todo caso, debe garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.*
- ✓ *Los ficheros temporales deben cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el Reglamento, siendo borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación*"[316].

- Medidas de seguridad para el nivel básico de protección:

Para poder llevar a cabo el tratamiento de datos personales es necesaria la adopción previa de una serie de medidas de seguridad, en atención a lo que relaciona A. Marzo:

- ➢ "*Elaborar e implantar un Documento de Seguridad con las normas y estándares de obligado cumplimiento para la entidad y/o empresa y el personal con acceso a los datos personales y a los sistemas de información, que habrá de tener como contenido mínimo: el ámbito de aplicación; las normas y reglas a proceder; las funciones y obligaciones del personal; la estructura de los ficheros; medidas para el transporte de documentos, etc*".
- ➢ *Relación actualizada de usuarios con acceso automatizado al sistema de información, estableciéndose modo de identificación y autenticación para tal acceso. Debe existir una política de gestión*

[316] MARZO PORTERA, A.: *Estudio Práctico sobre la Protección de Datos de Carácter Personal*. *Capítulo XIII, Medidas de Seguridad*: op. cit., pág. 604.

y cambios de contraseñas. Con identificación inequívoca y autenticación de los usuarios (RD 1720/2007), debiendo existir un procedimiento de asignación, distribución y almacenamiento que garantice la confidencialidad e integridad de las contraseñas. El Documento de Seguridad recogerá la periodicidad con la que tienen que ser renovadas y cambiadas las contraseñas, como mínimo una vez al año, según novedad introducida por el RD 1720/2007.

- *La salida de datos mediante correo electrónico deberá ser autorizada*"[317].

Destacan, a continuación, las medidas que han de establecerse para el control del acceso a la información. El hecho de que los soportes informáticos que contengan datos personales deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado, la salida de soportes informáticos con datos personales fuera de los locales donde se ubica normalmente el fichero sólo podrá ser autorizada (por escrito) por el responsable del fichero, así como medidas para impedir el acceso, perdida o robo de soportes con datos en su traslado. De igual modo, la obligación de realización de copia de seguridad previa a las pruebas con datos reales[318].

- Medidas de seguridad para el nivel medio de protección:

Para poder llevar a cabo el tratamiento de datos personales relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos relacionados con la solvencia patrimonial y el crédito de las personas y con el cumplimiento o no de sus obligaciones dinerarias (art. 29 LOPD), aquellos de los que sean responsables las entidades y servicios de la Seguridad Social, o bien aquellos que contengan un conjunto de datos que permitan evaluar aspectos de la personalidad de su titulares, es necesaria la adopción de otras medidas de seguridad, según el estudio hecho por Ana Marzo, entre las que destacan, además de todas las relacionadas para el nivel básico, "*la realización, al menos cada dos años, de una auditoria interna o externa sobre los sistemas de información e instalaciones de tratamiento de datos personales, reflejar en el Documento de Seguridad, además de lo exigible para el nivel básico, la*

317 Ibídem, pág. 605.

318 Ib., pág. 606.

identificación del responsable (s) de seguridad, la designación de una o varias personas en la organización y/o empresa (Responsable de Seguridad, según define el Reglamento) que controlen y coordinen las medidas, así como el establecimiento de un sistema de control de acceso físico a las instalaciones donde se encuentren los sistemas de información de forma que sólo tenga acceso el personal autorizado en el Documento de Seguridad"[319]. Además, se obliga a controlar la restricción de acceso a los lugares donde se ubiquen los servidores, y a tener registro de salidas y entradas de soportes y documentos.

- Medidas de seguridad para el nivel intermedio de protección:

Para proteger datos de un nivel entre el básico y el medio (muy común en la práctica) es necesario adoptar las medidas previstas para el nivel básico y además las recogidas antes relativas a auditoria bienal de los sistemas de información; control de acceso físico; identificación y autenticación de usuarios; gestión de soportes y reutilización y desechado de soportes.

- Medidas de seguridad para el nivel alto de protección:

Para asegurar los datos de nivel alto o máximo de protección hay que adoptar las medidas exigidas para los niveles anteriores y son una combinación de las existentes hasta 2007 más las introducidas por el R.D. 1720/2007 en los artículos 101 y siguientes[320], y que podemos resumir en las siguientes:

- Cifrado de telecomunicaciones. Es decir, la transmisión de los datos a través de redes públicas o redes inalámbricas de comunicaciones electrónicas deberá efectuarse cifrando los datos o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

- Registro de accesos. Que relacione cada acceso a la información, guardando como mínimo la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Para el caso en que el acceso haya sido autorizado, será preciso que el registro guarde la información que permita identificar el registro accedido. El periodo mínimo de conservación de los datos registrados es de dos años.

---

[319] Ib., pág. 608.

[320] B.O.E., núm. 17, de 19/01/2008, op. cit., pág. 4129.

- Los mecanismos que permitan el registro de los datos detallados han de estar bajo el control directo del responsable de seguridad quien, además de no permitir en ningún caso la desactivación de los mismos, debe encargarse de revisar periódicamente la información de control registrada y elaborar un informe, al menos una vez al mes, de las revisiones realizadas y los problemas detectados. El RD 1720/2007 introduce que la limitación de acceso a datos mediante llave o sistema equivalente así como el establecimiento de medidas de identificación de accesos a documentos cuando accedan varios usuarios.

- Seguridad en la distribución de soportes. Si la transmisión se hace mediante la distribución de soportes, de igual modo que en el cifrado de redes, los datos contenidos en ellos deberá ser cifrada o salvaguardada para que no sea inteligible ni manipulada durante su transporte.

- Medidas adicionales de copias de respaldo. Una copia de respaldo y de los procedimientos de recuperación de datos debe ser conservada en un lugar diferente de aquel en que se encuentren los equipos informáticos que tratan la información. Cifrado de dispositivos portátiles para el tratamiento de datos fuera de las instalaciones. Destrucción de soportes o documentos de copias desechadas (art. 101. 2 del RD 1720/2007)[321].

El 17 de julio de 2010, el Tribunal Supremo[322] dio a conocer tres sentencias (sobre los recursos contenciosos administrativos 23/2008, 25/2008 y 26/2008) en que se declaran nulos, por ser contrarios a derecho, los artículos 11, 18, 38. 2, y 123.2 así como de la última frase del artículo 38.1.a), del Real Decreto 1720/2007 de 21 de diciembre (RLOPD).

El Tribunal Supremo considera que el artículo 11 del RLOPD[323] que permitía la verificación por las Administraciones Públicas de datos en solicitudes formuladas por los ciudadanos sin requerir consentimiento de estos, habilita una cesión de datos al margen de los supuestos autorizados por los artículos 6 y 11 de la LOPD. La declaración de nulidad del precepto conlleva una garantía de protección de los datos de personas físicas ante la

321 Ibídem, pág. 4129.

322 B.O.E., núm. 259, de 26/10/2010, sec. I, pág. 90213. Véase: <http://www.boe.es/boe/dias/2010/10/26/pdfs/BOE-A-2010-16300.pdf>.

323 B.O.E., núm. 17, de 19/01/2008, op. cit., pág. 4112.

gestión de las Administraciones Públicas, pero también una incomodidad para el ciudadano, que deberá volver a declarar los datos personales de que se trate o acreditar su autenticidad. Este problema podría resolverse incorporando en los formularios que rellenen los ciudadanos una autorización expresa para la verificación o comunicación de datos por parte de la Administración correspondiente.

El Supremo declara nulo el artículo 18 del RLOPD ("Acreditación del cumplimiento del deber de información") por imponer al responsable del fichero, ilegítimamente y sin respaldo en la LOPD, la obligación de la constancia documental o acreditación del deber de información al afectado. El Supremo expresa que la LOPD "*ninguna referencia contiene a la forma, abriendo así múltiples posibilidades (escrita, verbal, telemática, etc.) (...). En consecuencia, debe considerarse que el legislador ha optado por la libertad de forma*"[324]. La Sentencia suprime, con este artículo, dos obligaciones: la de informar por un medio que permita acreditarlo, y la de conservar el soporte en el que conste el cumplimiento del deber de informar.

En el artículo 38 (sobre requisitos para la inclusión de los datos en ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado) se expresa que es requisito para esa inclusión la "*existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada*". Se elimina la frase "*y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero*"[325]. La supresión de esta frase, por defectuosa redacción y falta de concreción de su contenido (ya que permite considerar que incluso cuando la reclamación se formule por el acreedor exista la imposibilidad de inclusión de los datos en el fichero), afecta a la defensa del ciudadano ante las prácticas de empresas que ante una deuda incluyen los datos de sus "deudores" en un fichero de morosos por deudas sobre cuya existencia o cuantía puede haber discrepancia.

[324] Los señala así expresamente la Sentencia de la Sección Sexta de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, pág. 54.

[325] Ibídem, pág. 4.

La declaración de nulidad del artículo 38.2 beneficia a las empresas y demás responsables de fichero, ya que este párrafo trasladaba a estos la carga de la prueba de la concurrencia de los requisitos del artículo 38.1 en términos que originan una inseguridad jurídica que podría dar lugar a apertura de expedientes sancionadores. Sin embargo, para el ciudadano aumenta la desprotección, ya que no puede combatir la presunción del declarante.

La Sala de lo Contencioso-Administrativo acepta así una de las peticiones planteadas por la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)[326], que en colaboración con Equifax, una agencia estadounidense de control de crédito, gestiona el mayor fichero de morosos de España.

Los magistrados del Tribunal Supremo entienden que el RD 1720/2007 que desarrolla la Ley de Protección de Datos sólo permite que los ficheros de morosos traten y comuniquen datos que sean públicos, si no tienen el consentimiento de los afectados. "*A juicio de esta Sala, esa restricción erige un obstáculo a la libre circulación de los datos de carácter personal no querido, en principio, por la norma comunitaria*", señala el auto, que añade que el único obstáculo europeo es "*el interés de los derechos y las libertades fundamentales del titular de los datos*"[327].

El Supremo recuerda, no obstante, que la Directiva 95/46/CE prohíbe a los Estados miembros restringir de forma generalizada el tratamiento de los datos personales atendiendo, en particular, al derecho a la intimidad.

Tras concluir que "*no cabe que los Estados miembros impongan mayores restricciones que las previstas por el legislador comunitario*", los magistrados concluyen que procede plantear la cuestión prejudicial ante el Tribunal de Justicia de las Comunidades Europeas.

3.3.8. Deber de secreto profesional respecto a los datos de carácter

[326] La Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) es una Organización Empresarial creada en 1957, regulada por la Ley 19/1977 de 1 de abril sobre regulación del derecho de asociación sindical. Se presenta como enlace indispensable entre las entidades de crédito especializadas en España en financiación al consumo y las Administraciones Públicas, otras asociaciones profesionales españolas y europeas y los usuarios de productos financieros. <http://www.asnef.com/>.

[327] Sentencia de la Sección Sexta de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, pág. 15.

personal.

El deber de secreto profesional es otra de las piedras angulares de la protección de datos personales, llegando a constituir su incumplimiento no ya sólo una infracción administrativa grave, sino también la comisión de un delito, puesto que la revelación de secreto es una de las figuras delictivas contempladas en nuestro Código Penal.

Cabe decir aquí lo expuesto en el apartado anterior sobre 'deber de secreto', aunque dirigido a profesionales que tienen y tratan los datos personales con motivo de su trabajo. Es muy destacado este deber de secreto en ámbitos como el de la medicina o en la abogacía, para los que se establecen normas específicas que regulan estos supuestos cuyo incumplimiento va siempre asociado a una infracción que, en ocasiones puede llegar a conllevar hasta penas de prisión para quien reveló el secreto.

Veamos primero que la Ley Orgánica de Protección de Datos, en su art. 10[328], habla de la obligación de mantener secreto sobre los datos objeto de tratamiento, aplicable al responsable del fichero, encargado del tratamiento y todas las personas que participen en alguna fase del mismo, es decir, las personas que trabajen para los primeros, lo que, a tenor de los artículos 1902 y 1903 del Código Civil[329] hace generar la duda de si el responsable del fichero responde o lo hace el encargado del tratamiento de los datos, si hubiera éste incurrido en el incumplimiento. Lo recomendable es que establezca un acuerdo o contrato entre responsable y encargado para delimitar responsabilidades y adopción de medidas de seguridad. Es decir, dejarlo claro mediante un contrato de confidencialidad.

La Audiencia Nacional, en una de sus últimas sentencias sobre este aspecto, ha ratificado que no se puede vulnerar el "deber de secreto" colgando datos personales en Internet. Se reafirma así el tribunal al desestimar en 2010 un recurso contencioso-administrativo interpuesto por el Gobierno cántabro contra la resolución de la Agencia Española de Protección de Datos, en la que se consideraba que el servicio regional de Salud cometía "infracción" al difundir datos personales de los pacientes a través del programa de intercambio de archivos eMule[330].

---

328 B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43090.

329 Real decreto de 24 de julio de 1889 por el que se publica el Código Civil. B.O.E., núm. 206, de 25/07/1889, op. cit., pág. 310. Véase en base de datos del Boletín Oficial: <http://www.boe.es/datos/pdfs/BOE/1889/206/R00249-00312.pdf>.

330 "*El País*", edición digital, 8 de marzo de 2010:

El archivo contenía los nombres, apellidos, fechas de nacimiento, direcciones, teléfonos, sexo y, en algún caso, datos de salud asociados (tales como hipertensión o diabetes) de 1.748 pacientes de varias localidades de la comunidad cántabra.

La Audiencia dice en sentencia, según recogió la Agencia Española de Protección de de Datos en un comunicado[331], que existió una revelación de datos "*efectiva*" e "*innegable*", puesto que la información personal de los pacientes quedó a disposición del público en la Red y, por tanto, "*impone la obligación de adoptar las medidas necesarias para evitar que los datos se pierdan, extravíen o caigan en manos de terceros*".

A principios de 2009, la Agencia Española señaló en la resolución R/00340/2009[332] una infracción por parte del citado servicio de Salud de Cantabria, al constatar la existencia de un archivo accesible desde el programa eMule. La resolución de la Agencia instó al servicio cántabro de Salud a adoptar las medidas internas oportunas para impedir que volviera a repetirse una situación similar en el futuro. Según la Agencia, queda inutilizado el argumento de que fuera un trabajador quien llevara a cabo los actos que derivaron en la divulgación de los datos a través de eMule, ya que "*dicha hipotética actuación no deja sin efecto el hecho de que la entidad debía haber adoptado las medidas*".

Hasta finales de 2010, la Agencia Española de Protección de Datos había resuelto ya una treintena de procedimientos sancionadores vinculados al mal uso de programas de intercambio de archivos, al utilizar programas como eMule o similares, que han permitido la difusión a través de Internet de 11.300 historias clínicas de una clínica ginecológica, datos de pacientes de una clínica psiquiátrica, adoptantes, o miembros de sindicatos, entre otros[333].

En el ámbito del derecho laboral, algunas empresas empiezan a adoptar este tipo de compromisos o contratos de confidencialidad con sus

<http://tecnologia.elpais.com/tecnologia/2010/03/08/actualidad/1268042468_850215.html>.

331 Comunicado disponible en la web de la Agencia Española de Protección de Datos: <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/marzo/03_08_2010_NP_AN_EMULE.pdf>.

332 Resuelve el procedimiento nº AP/00053/2008. Véase: <http://www.boletindintel.es/BoletinesAyS/B100309/Docs/resolucion.pdf>.

333 Ibídem, pág., 2.

empleados, al margen de la relación contractual que les liga, para dejar bien sentadas las obligaciones de deber de secreto.

A pesar de todo, muchos autores terminan afirmando que el deber de secreto profesional es, por encima de todo, una cuestión ética que se regula para proteger los derechos de las personas al honor y la privacidad.

De otro lado, el hecho de que el Código Penal contemple penas por infringir este derecho es ya muy significativo, pues constata la importancia que tiene tutelar el derecho de las personas a mantener la privacidad de sus datos y el derecho al honor que puede resultar vulnerado por comunicar datos o información sobre la vida privada. Se dedican a ello los artículos 197, 198 y 199 del Código Penal de 1995[334].

3.3.9. Facilitar el manejo de los derechos por los titulares de los datos.

Existe la obligación para el responsable del tratamiento de habilitar procedimientos que permitan y faciliten a los interesados el ejercicio de sus derechos de acceso, rectificación, cancelación y de oposición. Lo dejó así establecido la Instrucción 1/1998[335], disponiendo que "*el responsable del tratamiento deberá adoptar las medidas pertinentes que garanticen que todas las personas de su organización u entidad que tienen acceso a datos personales puedan informar del procedimiento a seguir por el afectado-interesado para el ejercicio de sus derechos, facilitándole el manejo de los mismos*".

Hay, además, en la Ley Orgánica de Protección de Datos[336] un artículo, el número 17.2, que prohíbe cualquier posibilidad de que el responsable del tratamiento pueda exigir contraprestación alguna por el ejercicio de los derechos por los titulares de los datos. Es decir, es una conminación a facilitar el manejo de los derechos por los titulares de los datos.

---

[334] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. B.O.E., núm. 281, de 24/11/1995, pág. 33987.

[335] Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación. B.O.E., núm. 25, de 29/1/1998, pág. 3058.

[336] B.O.E., núm. 298 de 14/12/1999, pág. 43091.

Esta obligación de facilitar el ejercicio de derechos implica el establecimiento de cauces de información que permitan fácilmente al afectado-interesado conocer quién es el responsable del tratamiento, la dirección en la que puede ejercer sus derechos y la documentación que deberá aportar para que su solicitud pueda llevarse a cabo. Lo normal y típico es que esa información pueda aparecer en la parte de política de privacidad de la página web del responsable del tratamiento.

3.4. Ley de Economía Sostenible.

La Ley 2/2011, de 4 de marzo, de Economía Sostenible[337], fue promovido por el Gobierno español con el objetivo de introducir en el ordenamiento jurídico las reformas estructurales en un momento muy marcado por la crisis financiera y económica necesarias para crear condiciones que favorezcan un desarrollo económico sostenible, con una nueva Estrategia para una Economía Sostenible, según argumentó el Ejecutivo central en su preámbulo, en el que califica la Ley como "*una de las piezas más importantes de la Estrategia ya que aborda, transversalmente y con alcance estructural, muchos de los cambios que, con rango de ley, son necesarios para incentivar y acelerar el desarrollo de una economía más competitiva, más innovadora, capaz tanto de renovar los sectores productivos tradicionales como de abrirse decididamente a las nuevas actividades demandantes de empleos estables y de calidad*"[338].

Ampliamente anunciada por el Gobierno de José Luis Rodríguez Zapatero, la Ley de Economía Sostenible enumeró como principios inspiradores para impulsar una actividad basada en nuevos pilares, "*la mejora de la competitividad; la estabilidad de las finanzas públicas; la racionalización de las Administraciones Públicas, el fomento de la capacidad innovadora de las empresas; el ahorro y eficiencia energética; la promoción de las energías limpias y la racionalización de la construcción residencial*"[339].

337 B.O.E., núm. 55, de 5/03/2011, sec. I, pág. 25033.

338 Ibídem, pág. 25032.

339 Ib., pág. 25033.

La nueva norma modifica toda una serie de leyes de los ámbitos de la economía, las finanzas, las energías y la Administración. Entre los cambios, el régimen sancionador previsto en la Ley de Protección de Datos de carácter Personal al que están sujetos los responsables de los ficheros y los encargados de los tratamientos. Para ello, la Ley 2/2001 introduce su Disposición final quincuagésima sexta, titulada "*Modificación de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal*"[340].

Modifica cinco artículos de la Ley de Protección de Datos, referidos al régimen sancionador, recogiendo en gran medida la experiencia acumulada, según estimó en marzo de 2011 la Agencia Española de Protección de Datos, "*con el objetivo de conseguir mayor seguridad jurídica y mayor precisión en la aplicación de la norma, así como ampliar los criterios de modulación y adecuación de las sanciones*"[341].

Los cambios van dirigidos a mejorar la tipificación de las infracciones de la Ley de Protección de Datos para no sólo modular y adecuar la imposición de sanciones, sino incorporando novedades como la posibilidad de "*valorar la diligencia profesional sobre el tratamiento de datos exigible al infractor, pues no es lo mismo una gran compañía o corporación que una pyme, su volumen de negocio y el tipo de actividad que desarrolle*"[342].

Nos ocuparemos con más detalle del análisis de las modificaciones que introduce la Ley de Economía Sostenible en el régimen sancionador de la protección de datos y los cambios en las cantidades de las sanciones en el Capítulo 4 de nuestro estudio.

3.5. Directiva europea de Privacidad y Comunicaciones de 2002.

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección

340 Ib., pág. 25231.

341 Valoración de la Ley de Economía Sostenible hecha por la Agencia Española de Protección de Patos, disponible su resumen en: <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2011/notas_prensa/common/marzo/NP_modificacion_LOPD.pdf>.

342 Ibídem, pág. 2.

de la intimidad en el sector de las comunicaciones electrónicas, es conocida como la Directiva europea de Privacidad y Comunicaciones[343].

Viene a definir, tal y como recoge en su síntesis de presentación la página europea sobre legislación comunitaria[344] cinco grandes cuestiones sobre la confidencialidad de los datos en las comunicaciones electrónicas, la retención de datos, los mensajes electrónicos no solicitados, los cookies y las guías públicas.

En primer lugar, la confidencialidad de los datos, debido a que las comunicaciones realizadas a través de las redes públicas de comunicaciones electrónicas han de tener reserva confidencial. En particular, han de prohibir que personas distintas de los usuarios escuchen, intercepten o almacenen comunicaciones sin el consentimiento de los usuarios.

Destaca, en segundo lugar, la retención de datos, para lo que la Directiva establece que los Estados miembros solamente pueden limitar las disposiciones en materia de protección de datos para que puedan llevarse a cabo investigaciones de actividades delictivas o para garantizar la seguridad nacional, la defensa y la seguridad pública. Una medida de este tipo sólo podrá adoptarse cuando "*constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática*"[345].

Aborda también el envío de comunicaciones o mensajes electrónicos comerciales no solicitados (Spamming), para lo cual, establece que los usuarios han de dar su consentimiento previo antes de recibir este tipo de mensajes (enfoque «opt-in»). Este sistema abarca asimismo los mensajes de SMS y los demás mensajes electrónicos recibidos en cualquier equipo terminal, fijo o móvil.

---

[343] Diario Oficial de las Comunidades Europeas L 201/37, de 31/07/2002, op. cit., pág.37: < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF>.

[344] Página web sobre legislación comunitaria: <http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm>.

[345] Ibídem.

Contempla el problema de los «chivatos» (Cookies)[346], que son datos ocultos intercambiados entre un usuario de Internet y un servidor web que quedan archivados en el disco duro del usuario. Su finalidad inicial era conservar datos entre dos conexiones, aunque también constituyen un medio de control de las actividades del internauta que ha sido objeto de muchas críticas. La Directiva prevé que los usuarios deben tener la posibilidad de impedir que se almacene en su equipo terminal un «chivato» o dispositivo semejante. A tal fin, también se deberá facilitar a los usuarios información clara y precisa sobre la finalidad y la función de los «chivatos»[347].

Sobre las guías públicas, prevé que los ciudadanos europeos han de dar su consentimiento previo para que su número de teléfono (fijo o móvil), su dirección electrónica y su dirección postal pasen a figurar en las guías públicas.

En sus '*Considerandos*' preliminares, advierte sobre las necesidades específicas de proteger los datos personales que han ido surgiendo merced al avance de las nuevas tecnologías. Alude a Internet señalando que está revolucionando las estructuras tradicionales del mercado con sus aportaciones, indicando que los servicios de comunicaciones electrónicas

[346] Cookies, según la definición aceptada y consolidada desde hace algún tiempo en Wikipedia, (http://es.wikipedia.org/wiki/Cookie) son pequeños ficheros de datos que se generan a través de las instrucciones que los servidores web envían a los programas navegadores, y que se guardan en un directorio específico del ordenador del usuario. Dicho de otra forma, fragmentos de información que se almacenan en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas. Al ser el protocolo HTTP incapaz de mantener información por sí mismo, para que se pueda conservar información entre una página vista y otra como *login* de usuario, preferencias de colores, etc, deberá ser almacenada, ya sea en la página, en el propio servidor, o en una *cookie* en el ordenador del visitante. No obstante, una cookie no identifica a una persona, sino a una combinación de computador y navegador y consigue información sobre los hábitos de navegación del usuario, lo que puede causar problemas de privacidad. Lo que sí puede reflejar es el país donde vive el usuario de Internet, el dominio en la red que tiene, el sector de la actividad de la empresa donde trabaja, la función y el puesto que el usuario ocupa en la empresa donde trabaja, el proveedor de acceso a Internet e incluso puede conocerse hasta el volumen de la empresa, es decir, pistas significativas de la personalidad. Muchas empresas de cibermarketing –algunas al servicio de Medios de Comunicación--, han adoptado este proceso invisible de elaboración de perfiles.

[347] Considerando 25 de la Directiva 2002/58/CE. Diario Oficial de las Comunidades Europeas L 201/37, de 31/07/2002, op. cit., pág.39.

disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad.

Establece, de la misma manera, que "*deben elaborarse disposiciones legales, reglamentarias y técnicas específicas con objeto de proteger los derechos y libertades fundamentales de las personas físicas y los intereses legítimos de las personas jurídicas, en particular frente a la creciente capacidad de almacenamiento y tratamiento informático de datos relativos a abonados y usuarios*"[348].

Hace referencia directa a la relación entre un abonado y un proveedor de servicios, y dedica unas líneas importantes en su Considerando 15[349], para señalar que "*una comunicación puede incluir cualquier dato relativo a nombres, números o direcciones facilitado por el remitente de una comunicación o el usuario de una conexión para llevar a cabo la comunicación. Los datos de tráfico pueden incluir cualquier conversión de dicha información efectuada por la red a través de la cual se transmita la comunicación a efectos de llevar a cabo la transmisión. Los datos de tráfico pueden referirse, entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión*".

Estima esta Directiva que la información que forma parte de un servicio de radiodifusión suministrado en una red pública de comunicaciones y está dirigida a una audiencia potencialmente ilimitada no constituye una comunicación con arreglo a sus preceptos. No obstante, añade que en casos en que se pueda identificar al abonado o usuario individual que recibe dicha información, por ejemplo con servicios de vídeo a la carta, la información conducida queda incluida en el significado del término "*comunicación*" a efectos de lo que pretende regular.

Aclara que el consentimiento de un usuario o abonado, independientemente de que se trate de una persona física o jurídica, debe tener el mismo significado que el consentimiento de la persona afectada por los datos tal como se define y se especifica en la Directiva 95/46/CE.

---

348 Ibídem, pág.37.

349 Ib., pág. 38.

3.6. Directiva europea de acceso a Internet de 2009.

Varios de los artículos de la Directiva 2002/58/CE han sido modificados por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009[350], que lo primero que hace es reescribir el apartado 1 del artículo 1, para dejarlo de la siguiente forma: "*La presente Directiva establece la armonización de las disposiciones nacionales necesaria para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad y la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad*".

Añade una letra al art. 2, en concreto el apartado h), para definir legalmente que es una violación de los datos personales: "*violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público en la Comunidad*"[351].

Especialmente significativa es la modificación que hace del art. 4, para referirlo expresamente a la seguridad en el tratamiento de datos en las comunicaciones electrónicas, estableciendo tres nuevas exigencias a los proveedores de servicios de comunicación, centradas en garantizar que sólo el personal autorizado disponga de acceso a los datos personales, que se protejan de la posible destrucción accidental o ilícita, así como de la pérdida, alteración o revelación no consentida, y "*garantizarán la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales*"[352].

---

[350] Diario Oficial de las Comunidades Europeas L 337 de 18.12.2009, pág. 11. Véase: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:FULL:ES:PDF>

[351] Ibídem, pág. 29.

[352] Ib., pág. 29.

Introduce, además, la posibilidad de que las autoridades nacionales competentes puedan examinar las medidas adoptadas por los proveedores de servicios de comunicaciones electrónicas disponibles al público y puedan formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad.

Asunto controvertido y que supuso buena parte del Dictamen 1/2009 emitido por el Grupo de Trabajo comunitario en febrero de 2009[353] ha sido el de las notificaciones de las violaciones de datos personales. Estableciendo, para ello, que el proveedor de los servicios de comunicaciones electrónicas disponibles al público notificará, sin dilaciones indebidas, la violación de datos a la autoridad nacional competente. Propone, además, nuevas exigencias de notificación de violaciones de datos, que han sido trasladas a la legislación española por el Real Decreto-Ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas[354].

El Título II lo dedica a '*Modificaciones relativas a la transposición de Directivas en materia de Telecomunicaciones y Sociedad de la Información*' y redacta el nuevo Artículo 3. *Modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones*[355]. Cambia la redacción del artículo 34 de la citada Ley, el dedicado a la *Protección de los datos de carácter personal*, pata referirse al caso de violación de los datos personales, e imponer que "*el operador de servicios de comunicaciones electrónicas disponibles al público notificará sin dilaciones indebidas dicha violación a la Agencia Española de Protección de Datos. Si la violación de los datos pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el operador notificará también la violación al abonado o particular sin dilaciones indebidas. La notificación de una violación de los datos personales a un abonado o particular afectado no será necesaria si el proveedor ha probado a satisfacción de la autoridad competente que ha aplicado las medidas de protección tecnológicas convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad*"[356].

[353] < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_es.pdf>.

[354] B.O.E., núm. 78, de 31/03/2012, sec. I. pág. 26876.

[355] Ibídem, pág. 26923.

[356] Ib., pág. 26933.

Prosigue este R.D. Ley 13/2012, que traslada lo que establecía el Dictamen 1/2009 comunitario y transpone la Directiva 2009/136/CE señalando que, "*si el proveedor no ha notificado ya al abonado o al particular la violación de los datos personales, la Agencia Española de Protección de Datos podrá exigirle que lo haga, una vez evaluados los efectos adversos posibles de la violación. En la notificación al abonado o al particular se describirá al menos la naturaleza de la violación de los datos personales y los puntos de contacto donde puede obtenerse más información y se recomendarán medidas para atenuar los posibles efectos adversos de dicha violación. En la notificación a la Agencia Española de Protección de Datos se describirán además las consecuencias de la violación y las medidas propuestas o adoptadas por el proveedor respecto a la violación de los datos personales*"[357].

La nueva normativa obliga a los operadores a tener que llevar un inventario de las violaciones de los datos personales, incluidos los hechos relacionados con tales infracciones, sus efectos y las medidas adoptadas al respecto, que resulte suficiente para permitir a la Agencia Española de Protección de Datos verificar el cumplimiento de estas obligaciones de notificación.

La Directiva 2009/136/CE se refiere también al problema de los cookies que se dirigen de manera invisible a nuestra computadora, y establece la obligatoriedad de informar al usuario de manera "clara y completa" de manera previa a la utilización de cookies con fines publicitarios. La modificación de 2009 señala que "*se permitirá el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines de tratamiento de datos*".

Es en el '*Considerando 66'* de la Directiva 2009/136/CE[358] donde el legislador comunitario incide en el régimen de los cookies, subrayando que "*puede que haya terceros que deseen almacenar información sobre el*

[357] Ib., pág. 26934.

[358] Diario Oficial de las Comunidades Europeas L 337, de 18.12.2009, op.,cit., pág. 20. El subrayado es nuestro. Véase: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:Es:PDF>.

equipo de un usuario o acceder a información ya almacenada, con distintos fines, que van desde los fines legítimos (como algunos tipos de cookies) hasta aquellos que suponen una intrusión injustificada en la esfera privada (como los programas espía o los virus). Resulta, por tanto, capital que los usuarios reciban una información clara y completa cuando realicen una acción que pueda dar lugar a dicho almacenamiento u obtención de acceso. El modo en que se facilite la información y se ofrezca el derecho de negativa debe ser el más sencillo posible para el usuario. Las excepciones a la obligación de facilitar información y proponer el derecho de negativa deben limitarse a aquellas situaciones en las que el almacenamiento técnico o el acceso sean estrictamente necesarios con el fin legítimo de permitir el uso de un servicio específico solicitado específicamente por el abonado o usuario. Cuando sea técnicamente posible y eficaz, de conformidad con las disposiciones pertinentes de la Directiva 95/46/CE, el consentimiento del usuario para aceptar el tratamiento de los datos puede facilitarse mediante el uso de los parámetros adecuados del navegador o de otra aplicación".

Define, de otro lado, la cuestión de las 'comunicaciones no solicitadas' estableciendo (como nuevo art. 13), que la utilización de sistemas de llamada automática y comunicación sin intervención humana (aparatos de llamada automática), fax o correo electrónico con fines de venta directa solo se podrá autorizar respecto de aquellos abonados o usuarios que hayan dado su consentimiento previo. Pese a ello, añade que cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico, en el contexto de la venta de un producto o de un servicio de conformidad con la Directiva 95/46/CE, esa misma persona física o jurídica podrá utilizar dichas señas electrónicas para la venta directa de sus propios productos o servicios de características similares, a condición de que se ofrezca con absoluta claridad a los clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse a dicha utilización de las señas electrónicas en el momento en que se recojan y, en caso de que el cliente no haya rechazado inicialmente su utilización, cada vez que reciban un mensaje ulterior[359].

La Directiva 2009/136 conmina a lo los Estados europeos a que tomen las medidas adecuadas para garantizar que no se permitan las comunicaciones no solicitadas con fines de venta directa en casos que no sean los anteriormente mencionados, bien sin el consentimiento del

[359] Ibídem, pág. 31.

abonado o el usuario, bien respecto de los abonados o los usuarios que no deseen recibir dichas comunicaciones[360].

En España, el Interactive Advertising Bureau (IAB Spain)[361], que es la Asociación que representa al sector de la publicidad digital en nuestro país, se muestra de acuerdo con la necesidad de que exista un consentimiento informado por parte del usuario para la utilización de cookies publicitarias, y prefiere, según sostiene, el establecimiento de un sistema de información claro y preciso a los internautas. De hecho, una de las opciones por las que aboga IAB Spain es, en este sentido, la adopción de una solución internacional que implique el uso de un icono común para todo el sector de la publicidad digital, siguiendo la iniciativa adoptada por la industria estadounidense en enero de 2010.

3.6.1. La Directiva 2006/24/CE sobre la conservación de datos en las comunicaciones electrónicas y la transposición española.

La Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE con el objetivo de garantizar los datos para que estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves[362].

Su transposición a la legislación española es publicada en el 19 de octubre de 2007 en el Boletín Oficial del Estado, se trata de la Ley 25/2007 de 18 de octubre[363], de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Un tanto criticada por algunos autores, al ampliar el campo de las posibles infracciones, si bien hay que tener en cuenta que la naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos.

---

360 Ib., pág. 31.

361 Véase la web de la Asociación de Publicidad Digital: <http://www.iabspain.net/>.

362 Diario Oficial de la Unión Europea. L 105/54, de 13/04/2006, pág. 54.

363 B. O. E., núm. 251, de 19/10/2007, pág. 42517. Véase: <http://www.boe.es/boe/dias/2007/10/19/pdfs/A42517-42523.pdf>.

La Ley 25/2007, que viene a reflejar los preceptos de la Directiva 2006/24/CE, obliga a los operadores a conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones durante un plazo no superior a 12 meses computados desde el momento en que se haya producido la comunicación. Reglamentariamente, según señala su art. 5, previa consulta a los operadores, "*se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores, y sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de* cancelación"[364].

En lo que a Internet y el correo electrónico se refiere, destaca el hecho de los plazos temporales que se implantan: desde noviembre de 2007 deben conservarse los siguientes datos personales:

> "- *La identificación de usuario asignada.*
>
> - *La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.*
>
> - *El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono*"[365].

Relaciona, a continuación, los datos a conservar necesarios para la identificación del destino de una comunicación por correo electrónico y mediante la telefonía por Internet: "*La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet. Y los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación*".

---

[364] Ibídem, pág. 42519.

[365] Ib., pág. 42518.

Deben conservarse, también, datos necesarios para determinar la fecha, hora y duración de una comunicación y, en este sentido, con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet, la Ley 25/2007 indica en su art. 3.c) : "*La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo de Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado. La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet, o del servicio de telefonía por Internet, basadas en un determinado huso horario*"[366].

Para identificar el tipo de comunicación, con respecto al correo electrónico por Internet y a la telefonía por Internet, deberá conservarse "*el servicio de Internet utilizado*", según el art. 3 d) de la Ley 25/2007.

Para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación, con respecto al acceso a Internet, correo electrónico por Internet y telefonía a través de la Red, deberán conservarse, según el art. 3.e): "*El número de teléfono de origen en caso de acceso mediante marcado de números, y la línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación*"[367].

Esta detallada lista tiene que ser completada para los servicios de telefonía fija y móvil.

3.6.2. Otras normas comunitarias.

- Decisión de la Comisión 2008/49/CE, de 12 de diciembre de 2007, relativa a la protección de los datos personales en la explotación del Sistema de Información del Mercado Interior (IMI)[368].

---

366 Ib., pág. 42519.

367 Ib., pág. 42519.

368 Diario Oficial L 13, 16/01/2008. El IMI es una aplicación web segura concebida para que las autoridades nacionales, regionales y locales puedan comunicarse de forma rápida y sencilla con sus homólogas de otros países. La aplicación es accesible a través de internet y no requiere la instalación de software adicional. El sistema IMI se desarrolló con cargo al programa IDABC de prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los

- Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países[369].

- Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE[370]. Esta Decisión define las cláusulas contractuales tipo que garantizarán un nivel adecuado de protección de los datos personales que se transfieren desde la UE a terceros países. La decisión obliga a los Estados miembros a reconocer que las sociedades u organismos que utilicen esas cláusulas tipo en contratos relativos a transferencias de datos personales a terceros países garantizan un «nivel adecuado de protección» de los datos.

- Reglamento 45/2001/CE del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos[371]. Este Reglamento se propone garantizar la protección de los datos personales en el marco de las instituciones y organismos de la Unión Europea. El texto contempla disposiciones que garantizan un nivel de protección elevado para los datos personales tratados por las instituciones y los organismos comunitarios y la creación de una instancia de vigilancia independiente encargada de controlar la aplicación de dichas disposiciones.

3.7. Constitución Española de 1978 y la protección de datos.

Más allá de la protección administrativa, existe la protección constitucional de este derecho: el artículo 18.4 de la Constitución española

ciudadanos y gracias a él, pueden encontrar la autoridad con la que deben ponerse en contacto en otro país y entablar una comunicación mediante el uso de listas estructuradas de preguntas y respuestas estándar ya traducidas.

[369] Diario Oficial de la Unión Europea L 385, de de 29/12/2004.

[370] Diario Oficial de la Unión Europea L 181, de de 04/07/2001.

[371] Diario Oficial de la Unión Europea L 8, de 12/01/2001.

de 1978[372] establece que "*la ley limitará el uso de la informática para garantizar el honor y la intimidad personal*". Puesto que no cabe duda de que es posible incurrir en una intromisión ilegítima en la intimidad cuando se accede ilegalmente a datos de carácter personal.

No ha sido frecuente observar artículos como éste de la Constitución española, ya que el reconocimiento internacional al derecho a la intimidad no se ve reflejado en textos constitucionales europeos occidentales al ser coetáneos o posteriores a éstas. Sólo existía el precedente destacado de la Constitución de Portugal.

Hacer una valoración y establecer la naturaleza y justificación de la protección del derecho fundamental de la protección de datos personales desde el marco del Estado social y democrático de Derecho en el que nos movemos se complica al no existir aún mucha dogmática constitucional en la materia.

Lo complicado de esto que afirmamos se acentúa aún más, en opinión de María Rosa Abad Amorós, en el caso de Constituciones estatales "*que se encuentran redactadas a modo de clasificación de numerus clausus de derechos fundamentales. Esto hace que nos debamos preguntar si, realmente, los Estados democráticos que se estructuran constitucionalmente con declaraciones cerradas de derechos, como el caso de la española de 1978, impiden a las personas la posibilidad de disfrutar de otros nuevos derechos no reconocidos expresamente o si queda abierta la opción de ver ampliada esa declaración*"[373].

La Constitución Española vigente es de las que tienen un *numerus clausus* de derechos fundamentales, luego no recoge ni reconoce el nuevo derecho fundamental a la protección de datos personales. Tenemos que situarnos en el año 1993 para que, merced a la sentencia del Tribunal Constitucional número 254/1993[374], adquiera tal rango este derecho, y que le otorga similar constitucionalidad a los reconocidos expresamente.

Estamos ante un derecho que tiene una naturaleza mixta, basada en la dignidad de la persona, que es un derecho inherente reconocido en el art. 10.1 de la Constitución española de 1978: "*la dignidad de la persona, los*

[372] B.O.E., núm. 311, de 29/12/1978, pág. 29317.

[373] ABAD AMORÓS, Mª R.: '*La Protección de Datos Personales' en 'Derecho de la Información*'. Ariel, Barcelona, 2003, pág. 349.

[374] Sentencia del Tribunal Constitucional de 20 de julio de 1993, B.O.E. de18 de agosto de 1993.

derechos inviolables que le son inherentes al libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social"[375].

El que fuera presidente del Tribunal Constitucional español, Manuel Jiménez de Parga, sostiene que lo anterior son principios constitucionales y todo el ordenamiento jurídico español ha de interpretarse conforme a esos principios que, en su opinión, son directamente vinculantes por la fuerza normativa de la Constitución[376].

Principios constitucionales que están claramente constitucionalizados y que están dotados de la fuerza vinculante de las normas jurídicas. Son, por tanto, fuente normativa inmediata, es decir, no necesita de la interposición de regla o circunstancia alguna para alcanzar su plena eficacia.

Con estos principios, pues, constitucionales y de aplicación directa, junto al apoyo de determinados derechos expresamente reconocidos en la Constitución de 1978, así como en textos internacionales, es más fácil entender la tutela de ciertos derechos de singular relieve e importancia en el actual momento de la historia. Tal es el caso del derecho fundamental a la protección de datos personales. Su naturaleza puede estar, además, en el espíritu de otros como el derecho al honor, a la intimidad, y a la propia imagen. Las consideraciones que puedan hacerse sobre el contenido propiamente jurídico del derecho de la protección de datos personales puede encontrar, de esta manera, una directa coparticipación de otros derechos, especialmente, del derecho a la intimidad o del derecho a la información, en su facultad de acceso o investigación de informaciones.

Siguiendo a G. Peces Barba, en uno de sus variados estudios sobre derechos fundamentales, "*la condición jurídica propia del derecho fundamental a la protección de datos se retrotrae a la concepción genérica de todo derecho de libertad que, en última instancia, utilizando cualquier tendencia jurídica, facilita y hace posible, como así ha ocurrido con los*

[375] Uno de los preceptos que recogen derechos básicos en nuestra Carta magna, y que plasma uno de los de los mandatos enunciados y promulgados tres décadas antes por la Declaración Universal de los Derechos Humanos de 1948.

[376] Voto particular formulado por el magistrado Manuel Jiménez de Parga a la sentencia dictada en los recursos de inconstitucionalidad acumulados números 201/1993, 219/93 y 236/93, al que se adhiere el magistrado Rafael de Mendizábal Allende.

tradicionales derechos reconocidos y consolidados, el desarrollo integral de la persona"[377].

Con la promoción del poder público es como este derecho fundamental alcanza trascendencia real para toda persona que es sujeto de derechos. Estamos ante un nuevo derecho de libertad que se incorpora al decálogo de derechos reconocidos a la persona por su simple naturaleza racional, pero cuyo ejercicio real y su plena efectividad social demanda la promoción del poder público y, a la postre, de todos los poderes del Estado.

Nos apoyamos en el catedrático sevillano A. E. Pérez Luño para remarcar que el de la protección de datos personales "*es un derecho individual en cuya naturaleza confluyen, por tanto, el derecho clásico a la intimidad de la persona y, a su vez, la facultad de acceso a la información como parte integrante del contenido de otros derechos fundamentales, cual es el derecho a la información. Fueron derechos de clásica apropiación social burguesa. En el siglo XVIII la persona titular los defendía para sí con carácter excluyente y autónomo a toda intromisión del poder público. No era aquel más que un derecho individual que la doctrina inscribe en la denominada primera generación de los derechos fundamentales*"[378].

Ocurre que el derecho a la protección de datos personales comprende, además del sentido negativo del derecho a la intimidad, el sentido positivo o dinámico del mismo derecho, entendido como garantía individual de controlar las posibles variables que afecten a la intimidad. La conciencia social de finales del siglo XIX exigirá el desarrollo participativo del Estado y la paulatina incorporación constitucional de los denominados derechos de tipo social, explica Abad Amorós, "*la insuficiencia de aquellos primeros derechos, meramente sociales, movidos por una conciencia de clase y el nuevo pensamiento políticos de finales de siglo deriva en la necesidad del hombre no sólo de defenderse del Estado, sino de hacerle partícipe de la promoción y otorgamiento de unas prestaciones que hagan reales y efectivos de unos derechos de tipo social, que residían en las desigualdades y la ausencia de solidaridad*"[379].

---

[377] PECES BARBA, G. '*Derechos Fundamentales'*. Universidad Complutense, Facultad de Derecho, Madrid, 1986, pág. 74.

[378] PÉREZ LUÑO, A.E. '*Encuentros sobre Informática y Derecho 1990-1991*'. Aranzadi, Pamplona, 1992, pág. 173.

[379] ABAD AMORÓS, Mª R.: op. cit., pág. 351.

Es entonces, a tenor de esas premisas históricas y la evolución de las demandas sociales en materia de protección jurídica, cuando tiene entrada la segunda generación de derechos fundamentales de carácter social, del bienestar, de la igualdad real, que exigen la participación del Estado. No estamos ya ante valores, sino ante derechos innatos de la persona. Sólo con la intervención de los poderes públicos y su compromiso de promoción por el poder económico, administrativo y jurídico que le asiste, será posible establecer las condiciones idóneas para garantizar, en el seno de un Estado social y democrático de Derecho, la incorporación de derechos prestacionales.

En un Estado social y democrático de Derecho, los derechos individuales y sociales se anidan, se complementan para la persona titular de los mismos, al tiempo que el factor población de los Estados crece y progresa intelectual, científica y tecnológicamente, sostiene Abad, "*de ahí que ahora, sin diferenciaciones sustentadas en sustratos de clase, sino bajo el principio de la universalidad, todos nos autocreamos necesidades de nuevos derechos para defendernos de nuestras propias creaciones. Es la evolución tecnológica la que, e finales de los años sesenta y comienzos de los setenta la que crea para las personas la tercera generación de derechos fundamentales de perfil bien distinto a los anteriores*"[380].

Entre ellos, el derecho a la protección de datos, aún con el núcleo anclado en el derecho a la intimidad. A partir de esas décadas de los sesenta y, sobre todo, de los setenta, las modernas teología, la informática, agreden o solucionan desde el exterior a los tradicionales derechos fundamentales, como señalan, entre otros, los profesores Pérez Luño y Frossini, de ahí que el sujeto titular de derechos evolucione también y reaccione ante esas nuevas agresiones demandando mantener las garantías de su inherente derecho a la intimidad. Pero además de este sentido negativo de la intimidad, apostando por el control de la misma en todo momento, que será el control de sus datos de carácter personal.

Llegados a este punto es cuando el derecho a la protección de datos personales o derecho a la libertad informática adquiere un aspecto de ejercicio de libertad positivo y dinámico. Para ello se requieren nuevos instrumentos reales y efectivos de garantía. La sofisticación de las nuevas agresiones va exigiendo mayor complejidad jurídica, porque desafiar y controlar su extensión no es más que controlar al extensivo e imparable mundo de la sociedad tecnológica de este transformador siglo XXI, que tan fácil hace la invasión de nuestra intimidad.

380 Ibídem, pág. 352.

Las libertades se han ido contaminando por agresiones bien diferentes que, a su vez, han concienciado incluso radicalmente a puntuales o generales sectores sociales. Según Pérez Luño[381], "*si las guerras atómicas impulsaron los movimientos pacifistas, la agonía medioambiental la recoge el movimiento ecologista, la medicina o la biología se conmueven por los avances genéticos. Y si la Humanidad reivindicó primero libertad, paz, justicia y bienestar social después junto a calidad de vida, ahora en la era de las nuevas tecnologías y la Sociedad de la Información, cuando es mayor la amenaza sobre las tradicionales libertades se reclaman facultades para la protección de los datos personales ante cualquier forma de tratamiento, y todos recogemos el testigo de su control*". Un fenómeno que, en opinión de Pérez Luño, es simplemente '*una nueva concreción histórica de los valores básicos de la libertad, la igualdad y la dignidad de la persona humana*'.

Puede decirse que estamos ante una relectura de los valores de la humanidad. Siendo el bien jurídico a proteger el mismo, es decir, el reconocido como inherente derecho a la intimidad y en el modelo de Estado social y democrático de Derecho, ya garantizado y superado el sentido negativo de la intimidad más propio del siglo XVIII, "*se está evaluando y procediendo al reconocimiento del sentido positivo de la libertad informática. Esto sólo se alcanzará con el ejercicio dinámico de una serie de facultades que dan contenido al nuevo derecho fundamental, permitiendo a la persona disponer del control, en todo momento, de sus datos personales. Es, en última instancia, conseguir el control de su intimidad*", según Pérez Luño[382].

La libertad informática no es, por consiguiente, tan sólo el derecho a negar cualquier información individual que posee toda persona en su esfera de lo íntimo y que, en la actualidad, ya no encuentra suficiente tutela e incluso protección por las leyes y las aportaciones jurisprudenciales, sino que además es el derecho a la libertad para poder controlarlos en todo instante y bajo cualquier circunstancia.

Es, ésta última concepción descrita, *el habeas data*, según expresión acuñada por el italianoVittorio Frosini[383], inseparable en la protección de

[381] PÉREZ LUÑO, A.E.: '*Nuevas tecnologías, Sociedad y Derecho. El impacto sociojurídico de las NT de la Información*'. Fundesco, Madrid, 1987 pág. 125.

[382] Ibídem, pág. 125.

[383] Frosini Vittorio: '*La protezione della riservatezza nella società informatica*'. Bolonia. 1981, pág. 44.

los datos personales y que implica no sólo el simple acceso a los mismos, sino su posible cancelación, rectificación y oposición a su tratamiento, según la voluntad y consentimiento del interesado.[384] La compleja naturaleza del nuevo derecho le hace ser tanto inherente para la persona, como objeto de prestación para el Estado.

Evidentes resultan las diferencias entre la protección de la intimidad y la protección de datos personales. Las resume Álvarez Cienfuegos Suáres: '*La primera tiene un carácter defensivo, excluyendo del conocimiento ajeno a la vida personal y familiar, vetando incluso las intromisiones de terceros contra la voluntad del titular. En el caso de la protección de datos personales, aún reconociendo la dinamicidad de su contenido objetivo derivado de los cambios tecnológicos, este derecho fundamental garantiza a la persona un poder de control, de contenido positivo sobre la captura, uso, destino y posterior tráfico de los datos de carácter personal*'[385].

El derecho fundamental a la protección de datos, por plasmación constitucional y por construcción jurisprudencial, ha pasado a formar parte de los derechos de la persona. Desde el Derecho Privado, todo sujeto que se desarrolla en sociedad se comunica, se relaciona con el mundo de los demás y mantiene relaciones jurídicas que el conjunto de la doctrina define como cualquier tipo de relación entre seres humanos que se encuentra regulada por el Derecho o que, sin estarlo, produce consecuencias jurídicas. El ejercicio de todo derecho fundamental, su puesta en práctica, se proyecta hacia el exterior y crea situaciones sociales, necesidades y relaciones con el resto del mundo que son susceptibles de ser analizadas jurídicamente.

3.7.1. Elementos del derecho fundamental a la protección de datos personales.

Partamos de la base de que toda relación jurídica tiene una estructura básica que comprende distintos elementos que le caracterizan, como son el objeto, el contenido o los sujetos de la relación. Si delimitamos estos elementos en la estructura del nuevo derecho fundamental a la protección de datos, podremos llegar a la conclusión de su trascendencia jurídica.

---

[384] Conceptos los de cancelación, rectificación y oposición que son convertidos en derechos de los titulares de los datos personales por el Derecho Comunitario europeo, y que plasma la Directiva 95/46/CE abordada en el capítulo 3.1 de este estudio.

[385] ALVAREZ CIENFUEGOS SUARES, J.Mª.: *´La libertad informática, un nuevo derecho fundamental en nuestra Constitución*'. Diario La Ley, Madrid, 22 de enero de 2001. Nº 5.230.

Se abre el riesgo nuevamente de insertar racionalmente la protección de datos personales en los ya conocidos esquemas jurídicos de los derechos de la personalidad, una misión que posibilitan las propias fuentes del Derecho.

3.7.2. Función del derecho fundamental a la protección de datos.

Hallar la función que para la persona tiene el derecho fundamental a la protección de datos es buscar una derivación de la función que ha tenido y mantiene la protección de la intimidad. La jurisprudencia se ha posicionado entendiendo el distanciamiento generacional entre ambos derechos, y así lo ha señalado al abordar el mecanismo concreto de la función de este derecho.

La función del derecho fundamental de la protección de datos, como describe E. Suñe Llinas[386], "*es garantizar a toda persona el poder de control sobre sus datos personales, tanto su uso como su destino, con el propósito de impedir su tráfico ilícito y la posible vulnerabilidad del afectado. Eso lleva implícito el poder de disposición sobre sus datos. Por el contrario, la función del derecho fundamental a la intimidad es proteger de cualquier invasión los reductos de vida personal o familiar que la persona desea mantener fuera del saber de terceros o de evitar intromisiones contra su propia voluntad*".

La realidad social y jurídica viene a confirmar la función más amplia del derecho a la protección de datos frente al derecho a la intimidad. "*Una amplitud que se proyecta en sus caracteres más particulares*"[387].

3.7.3. El objeto.

Son los propios datos personales el objeto de protección de este nuevo derecho fundamental. La definición que de los mismos están dando los ordenamientos jurídicos europeos son ramificaciones del tronco

386 SUÑE LLINAS, E.: '*Tratado de Derecho Informático, Introducción y Protección de Datos personales*'. Facultad de Derecho de la Universidad Complutense, Madrid, 2000, pág. 56.

387 Ibídem, pág. 56.

jurídico del Convenio 108 del Consejo de Europa[388] que hemos analizado aquí al hablar de los antecedentes de la Directiva 95/46/CE, que definía a inicios de los años ochenta los datos personales como cualquier información relativa a una persona física identificada o identificable.

Más tarde, y aportando más elementos a esta definición, la propia Directiva 95/46/CE[389] dice que 'datos personales' son toda información sobre una persona física identificada o identificable (el 'interesado'), considerando identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

El dato personal es, en efecto, información, pero no en el sentido de libertad informativa, tal y como se interpreta el objeto del derecho a la información, afirma J. Mª. Desantes[390], "*sino como hechos que podrían ser conocidos, tratados e incluso difundidos como resultado de la decisión del interesado que consiente en su conocimiento por terceros, y que en cualquier caso su tratamiento no ha de lesionar su intimidad*".

Son estas definiciones conceptos tan amplios que de entrada no admiten distinciones en la calidad de la información a proteger. "*Pero la información positiva ya consolidada coincide en la superprotección jurídica de una tipología de datos denominados sensibles, denotando cierta relajación con respecto a los demás*", según J. Pérez[391]. En el ordenamiento jurídico español, esta antigua protección se ha fortalecido porque así lo ha hecho la jurisprudencia del Tribunal Constitucional español con respecto al objeto de protección del derecho fundamental a la protección de datos.

---

[388] Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal. Estrasburgo, 28 de enero de 1981. B.O.E., núm. 274, Madrid, 15 de noviembre de 1981, op. cit.

[389] Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. Diario Oficial de las Comunidades Europeas, núm. L 281, de 23 de noviembre de 1995, págs. 31-50.

[390] DESANTES GUANTER, J. Mª.: '*Información y Derecho*'. Colección Actualidad e Información, Santiago de Compostela, 1990, pág. 38.

[391] PÉREZ MAÑA, JORGE: '*Bases de datos jurídicos. Características, contenido, desarrollo, marco legal*'. Centro Superior de Investigaciones Científicas, Madrid, 1994, pág. 49.

Lo que hace el alto Tribunal es interpretar que el objeto de protección son, además de los datos íntimos individuales y fundamentales, como pudieran ser entre otros los relativos al honor, la intimidad personal o familiar, la propia imagen, la ideología o las creencias, salud, afiliaciones sindicales, raciales o sexuales, también lo son cualquier otro tipo de datos, cuyo conocimiento por terceros pueda afectar a sus derechos, sean o no fundamentales. Por tanto, su objeto excedería de la esfera meramente privada para alcanzar también a los datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos[392].

Deriva esta cualidad del objeto del derecho a la protección de datos en el incuestionable resultado de que los datos personales a proteger son todos aquellos que, puestos de forma adecuada, permitan identificar a la persona y confeccionar un perfil de cualquier naturaleza que pueda llegar a constituir una amenaza para el desarrollo del individuo, tanto en sociedad como en su estricta vida. Si nos alejamos del frío concepto jurídico que aporta el Derecho y entramos en la meditación que asiste a la Filosofía, ya en los años ochenta, J. María, entre otros, anticiparon reflexiones acerca de la automatización del saber que "*los datos no son nunca saber; sino que son elementos para el saber. Únicamente en conexión articulada, componiendo una figura, proporcionan conocimiento*"[393].

Los datos aislados, disociados de su titular son, en efecto, sólo una sombra, un reflejo de un poder ser, pero convenientemente insertados o acoplados en torno a un individuo dan un perfil perfecto del mismo, dejando al descubierto su lado oculto, con la indefensión que produce el desconocimiento de su destino.

3.7.4. El contenido.

Contar el derecho a la protección de datos personales como parte del catálogo de los derechos fundamentales implica la inserción en el mismo de todos los elementos propios de un derecho subjetivo. Ésta es la pretensión iniciada, de ahí que el contenido del derecho a la protección de

[392] Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Fundamento Jurídico 6.

[393] MARÍA, JULIÁN: '*Cara y cruz de la Electrónica'*. Espasa Calpe, Madrid, 1985, pág. 56.

datos debe albergar para la persona, como el resto de sus derechos, posibilidades de actuación que, técnicamente, se denominan facultades.

El Tribunal Constitucional español ha puesto de manifiesto que el derecho a la protección de datos atribuye al titular un haz de facultades que consisten en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicas, que sirven a la función capital que desempeña este nuevo derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, el derecho a saber y el deber de recibir la completa información sobre el destino y uso de esos datos, quién dispone y qué uso reciben tales datos para, en todo caso, proceder al ejercicio de oponerse a la posesión y al uso.

El conjunto de facultades primarias que adquiere el sujeto de derecho a la protección de datos pueden incluso independizarse a modo de derechos instrumentales para el ejercicio del derecho principal. Son el derecho de acceso, de rectificación, de oposición y cancelación de datos personales, que en un todo, recuerda Pérez Luño, constituye el *habeas data*, '*la facultad de las personas de conocer y controlar las informaciones que les conciernen procesadas en bancos de datos informatizados*'[394]. Una definición que es necesario actualizar, pues no es sólo ya el derecho al control de los datos personales procesados de forma automatizada, sino el control, tal y como dispone por transposición de la Directiva comunitaria reguladora de la protección de datos la LOPD española, de los datos insertados en ficheros o bancos de datos susceptibles de ser tratados tanto informática como manualmente.

El *habeas data*, que no estaba no tan siquiera implícito en el Convenio 108 de Roma, adoptado, según ha quedado aquí reflejado, como norma primaria supranacional para la protección de los datos personales, los define el Tribunal Constitucional español en su sentencia de 1993[395]. Trata de derechos y facultades que, observa Abad, "*complementan y desarrollan el derecho a la intimidad, imponiendo cargas a los poderes públicos, y en concreto a la Administración, y cuya imposición necesita una regulación legal de carácter sustantivo y procesal, y sin la cual el derecho no alcanza su plena efectividad*"[396].

394 PÉREZ LUÑO, A.E.: op. cit., pág. 175.

395 Sentencia del Tribunal Constitucional 254/1993. B.O.E., de 18/08/1993.

396 ABAD AMORÓS, Mª R.: op. cit., pág. 359.

Apuntalado el carácter sustantivo conviene fijar el significado como cauce procesal del habeas data interpretado como salvaguarda de la libertad de la persona en la esfera informática. La doctrina aquí está adoptando como paralelismo la función, que correspondió al *habeas corpus* para los derechos de la primera generación respecto a la libertad física o de movimientos de la persona. Ambos conceptos garantizan derechos fundamentales: el *habeas corpus* defiende y protege la libertad física de la persona, y el *habeas data* la libertad interna. El histórico *habeas corpus* se regula con independencia formal legislativa en un trámite procesal rápido y ágil, que permite la inmediata puesta en libertad de aquella persona que ha sido objeto de una detención ilegal. El habeas data es el resultado de la sucesiva ampliación de la teoría de los estatus de George Jellinek[397], y se concreta en las normas de protección de datos en las garantías de acceso y control de las informaciones insertas en programas o ficheros de datos personales y que conciernen a cualquier sujeto.

3.7.5. El sujeto titular de los datos.

El sujeto titular es elemento crucial en toda relación jurídica. Los derechos y deberes sólo pueden atribuirse a las personas. Por tanto, resulta imprescindible esa componente personal. A tenor de los principios civiles, la capacidad para ser sujeto de derechos y obligaciones se adquiere con la personalidad. Esta capacidad es referida tanto a la persona física como a la persona jurídica.

Vista la construcción jurisprudencial hecha del objeto del derecho a la protección de datos, el sujeto titular de los mismos tiene control y disponibilidad tanto de los datos más mínimos o sensibles como sobre sus datos hechos públicos.

Ahora bien, ateniéndonos y acotándonos al escaso marco positivo referido aquí, y considerando la definición de persona que reza en el Código Civil español, cabe plantearse quién es el sujeto titular del derecho fundamental a la protección de datos, siguiendo a Abad[398].

La Ley española de Protección de Datos dice que el titular de los datos personales es el afectado o interesado, y que éste sólo puede ser la persona física titular de los datos que sean objeto del tratamiento. De igual

[397] Ibídem, pág. 360.

[398] Ib., pág. 361.

modo, aún con mayor amplitud, se había pronunciado la Directiva comunitaria 95/46/CE, estableciendo que lo será "*el interesado que pueda ser identificado o identificable*", y parece claro que identificable es toda persona cuya identidad pueda determinarse directa o indirectamente, en concreto, mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

Con estas definiciones en la tipología de personas que regulan el Derecho, "*sólo la persona física o natural es titular de sus datos personales, asumiendo los derechos y deberes que esto implica*"[399].

En cuanto a lo relativo a las personas jurídicas, éstas asumen competencias y responsabilidades en diferentes momentos y en las normas que aquí se han citado en dos figuras permanentes en todo proceso de tratamiento del dato: el responsable del fichero o tratamiento y el encargado del mismo. Así lo establece expresamente el art. 3 de la LOPD de 1999 en su apartado d)[400]. Pueden ser ambos personas físicas o jurídicas. El primero será quien decida sobre la finalidad, contenido y uso del tratamiento, mientras que el segundo se ocupará de tratar los datos personales, pero por cuenta del responsable del tratamiento.

3.7.6. Los límites del derecho fundamental a la protección datos.

La doctrina viene manteniendo la tesis del Tribunal Constitucional español, que ha declarado que no existe ningún derecho absolutamente ilimitado. También los derechos fundamentales, cuando se delimitan en los ordenamientos jurídicos, asumen restricciones y límites que, en cualquier caso, deben respetar su contenido esencial.

Una de las bases interpretativas supranacionales del Título I de la Constitución española de 1978 es el Convenio de Roma suscrito en 1950, y cuyo Instrumento de Ratificación se firmó en Madrid en noviembre de

---

399 Ib., pág. 361

400 Ley Orgánica de Protección de Datos Personales 15/1999, art. 3, "*d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento*".

1977[401]. El Tribunal Europeo de Derechos Humanos, cuando dicta sentencias sobre las garantías y límites de la intimidad individual y familiar se remite al artículo 8 de su texto normativo[402]. Ahora también lo hace pero con respecto a la protección de los datos de carácter personal y aplica las mismas garantías y límites. Las restricciones alcanzarán, materialmente a todos los aspectos del contenido del derecho a la protección de datos y, en consecuencia, a todas sus facultades. Un asunto que merece análisis aparte.

El artículo 105, apartado b), de la Constitución española de 1978 ordena la regulación del derecho de acceso de los ciudadanos a los archivos y registros administrativos. Es la constitucionalización de la facultad del sujeto de acceder a las informaciones. El límite deviene impuesto por la seguridad y defensa del Estado, la averiguación del delito y la intimidad de las personas. La jurisprudencia añade que la persecución del delito, la distribución equitativa del sostenimiento del gasto público y las actividades de control en materia tributaria son bienes y finalidades constitucionales legítimas capaces de restringir el derecho al honor, a la intimidad personal y familiar y a la propia imagen, así como el uso de la informática.

En el caso específico del derecho a controlar los datos personales, los límites que se fijan recaen en la forma de ejercer el conjunto de facultades que conforman su contenido, como analiza Pablo Lucas Murillo de la Cueva[403].

El primer derecho para el control de nuestros datos es el acceso a los mismos allí donde se encuentran. El acceso no es indiscriminado, tiene

[401] Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. B.O.E., núm. 243, de 10/10/1979, pág. 23564.

[402] Convenio de Roma de 1950, articulo 8. 'Derecho al respeto a la vida privada y familiar' *1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*.

[403] MURILLO DE LA CUEVA, P. '*Informática y Protección de Datos Personales'. Centro de Estudios Constitucionales*'. Madrid. 1993, pág. 136.

restricciones para quien accede y para quien permite el acceso. Tras ello, se abre paso la posibilidad de ejercer el resto de facultades: la cancelación, la rectificación o la oposición a su tratamiento. Todos esos derechos que recoge con claridad la Ley española de Protección de Datos Personales.

Fijar los límites lo hace la ley, pero siempre en el estricto margen constitucional, sin salirse de las paredes que marca el texto de 1978. Por ello, el tratamiento de datos, ya sea desde los sectores privados o por el poder público, sólo se justifica en los Estados democráticos en aras a la protección o coexistencia con otros derechos de idéntica tutela.

La protección de los datos de carácter personal constituye en auténtico *habeas data*, como se ha encargado de dejar claramente sentado la decisiva STC 254/1993 aquí citada.

3.7.7. Concreción del derecho a proteger nuestros datos.

A modo de concreción, puede afirmarse, siguiendo a I.C. Del Castillo, que "*el derecho a la autodeterminación informativa es el derecho fundamental que toda persona ostenta para decidir por sí misma, en qué momento y qué datos propios desea dar a conocer a terceros para revelar situaciones o aspectos de su vida privada, y qué utilización de dichos datos autoriza*"[404].

Significa el derecho a conocer qué datos relativos a su persona obran en los ficheros públicos o privados, con la posibilidad añadida de modificar o cancelar tal información.

La concepción de este derecho como fundamental encuentra arraigo en lo más cierto de la dignidad humana, puesto que el *habeas data* es el conjunto de referencias por el cual un individuo se define, de tal suerte que la conjunción de todos sus datos personales conforma su identidad, con las distintas expresiones de su personalidad.

La peculiaridad de este derecho fundamental en nuestro ordenamiento jurídico radica en su creación y configuración jurisprudencial, al margen de la tabla de derechos reconocida en el texto constitucional de 1978, y sustentada sobre una exquisita elaboración doctrinal que flexibilizó la letra del artículo 18.4 de la Constitución española para dar cobertura positiva a

[404] DEL CASTILLO VAZQUEZ, Isabel Cecilia*: Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*. Thomson Civitas., Pamplona, 2007, pág. 621.

este nuevo derecho. Todo ello perfila su especial atractivo para quien dedica sus esfuerzos al estudio de la ciencia jurídica. Es, en efecto, "*un derecho fundamental de nueva generación y signo de los tiempos que corren, surgido a partir de la intimidad, sus inicios son fruto de la toma en consideración del peligro que entraña el manejo de las nuevas tecnologías en el trasiego de datos de carácter personal*"[405].

3.8. En el Código Penal.

En el Código Penal español vigente, de 1995[406], se pretendió por vez primera otorgar protección a los datos personales y, en consecuencia, tipificar las conductas consistentes en el acceso indebido a los mismos, su utilización, cesión, etc. A ello dedica el Título X de su Libro II[407] (artículos 197 a 201), bajo el enunciado de '*Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*'. El primero de sus artículos protege diversas manifestaciones de la intimidad, entre las que se encuentra la libertad informática, así como la privacidad.

El Código Penal castiga acciones como el apoderamiento, utilización o modificación, en perjuicio de tercero de datos reservados de carácter personal, el acceso no autorizado y su alteración o utilización en perjuicio del titular de los datos personales, la difusión y revelación o cesión a terceros de datos o hechos descubiertos o imágenes grabadas, así como la revelación de secretos ajenos descubiertos por otros. Regula en su art. 199 la revelación de secreto profesional[408].

El dedicado al secreto profesional cobra especial relevancia en el ámbito de los Medios de Comunicación para todo lo que es la actividad editorial de un periódico, una televisión o una emisora de radio. No obstante, ceñimos nuestro análisis a lo que es la actividad no editorial de los Medios, que también exige el cumplimiento de lo que recoge el Código Penal español (CP)[409], el cual establece pena de prisión de uno a tres años y

405 Ibídem, pág. 622.

406 Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, B.O.E., núm. 281, de 24/11/1995, págs. 33987-34058.

407 Ibídem, pág. 34010.

408 Ib., pág. 34011.

409 Ib., pág. 34011.

multa de seis a doce meses para el que revele secretos ajenos de los que tenga conocimiento por razón de su oficio o sus relaciones laborales. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión de dos a seis años.

Como puede deducirse, la revelación de secreto profesional tiene aparejados castigos más que significativos en la legislación española.

El art. 197 del Código Penal (modificado en 2010 como se lee en párrafos siguientes) está dedicado a la revelación de secretos por personas autorizadas para manejar los datos como por aquellas que no lo están y habla de penas de prisión de uno a cuatro años y multa de 12 a 24 meses para quien se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, con el objetivo de descubrir los secretos o vulnerar la intimidad del otro sin su consentimiento.

En su apartado 2 establece las mismas penas para quien, "*sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado*"[410]. Iguales penas se impondrán a quien, sin estar autorizado, aceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

Las penas de prisión van de dos a cinco años si se difunde, revela, o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los dos apartados anteriores.

Se contemplan estas penas en su mitad superior para las personas encargadas o responsables de los ficheros, soportes, archivos o registros que cometan los hechos señalados. Las penas de prisión pueden ser de entre cuatro a siete años si con la revelación del secreto se ha perseguido un beneficio económico.

El art. 198 CP contempla penas de prisión e inhabilitación absoluta para la autoridad o funcionario público que cometa los hechos arriba descritos, sin que medie causa legal y prevaliéndose de su cargo. Como

[410] Ib., pág. 34010.

también lo hace el art. 417 CP[411], que castiga a la autoridad o funcionario público que revele secretos o informaciones que no deban ser difundidos y que tengan por razón de su oficio o cargo.

En 2010 ha visto la luz una reforma del Código Penal que hace incidencia en varias materias relacionadas con una realidad que siempre avanza por delante del Derecho. La reforma representa una respuesta penal ante nuevas formas de criminalidad, como las derivadas, entre otras cuestiones, de las nuevas tecnologías.

En el mes de junio de 2010 se publica la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, para su entrada en vigor a los seis meses desde su publicación, es decir, en plena vigencia desde 23 de diciembre de 2010[412].

En relación a los delitos informáticos, se han modificado varios artículos, que inciden en el objeto de nuestro estudio, como el art. 197, referido al '*descubrimiento y revelación de secretos*' El nuevo artículo 197 introduce un nuevo apartado 3, pasando los actuales apartados 3, 4, 5 y 6 a ser los apartados 4, 5, 6 y 7, y se añade un apartado 8, con la siguiente redacción: "*3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años*"[413].

Para continuar con el establecimiento de penas mayores en función de la gravedad de la vulneración y la pertenencia a grupo organizado. Hasta ahora, el Código Penal no había previsto las modalidades comisivas consistentes en el uso de las tecnologías de la información para invadir la intimidad de las personas o para violar, acceder o descubrir sus secretos. Es el llamado "mero acceso no consentido", conocido como hacking directo (acceso indebido o no autorizado con el único ánimo de vulnerar el password sin ánimo delictivo adicional).

411 Ib., pág. 34034.

412 B.O.E., núm. 152, de 23/06/2010, sec. I., pág. 54811.

413 Ibídem, pág. 54844.

Con esta reforma, se castigará a quien acceda a un sistema informático sin haber obtenido consentimiento, independientemente de si lleva a cabo algún tipo de daño en el sistema o algún perjuicio al propietario del equipo.

Se modifica el artículo 248, el dedicado al '*delito de estafa*', que queda redactado de forma que introduce la manipulación informática y la idea de emplear programas informáticos para estafar: "*1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. 2. También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo*"[414].

Con lo la incorporación de es forma más moderna de la estafa, el nuevo texto de nuestro Código Penal se decanta por dar coherencia a la posibilidad de que esas nuevas formas den lugar a daños sufridos a través de nuevos canales, y provocando perjuicios. De acuerdo, con esto, cambia el artículo (264) dedicado al 'delito de datos'[415]: "*1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.*

2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años", para continuar con una relación de las penas que llevan aparejadas los diferentes niveles de daños causados por estas conductas.

Otra de las novedades que introduce la nueva reforma del Código Penal es la inclusión de la responsabilidad penal de la empresa, una cuestión que puede afectar sensiblemente a las empresas de Medios de

414 Ib., pág. 54846.

415 Ib., pág. 54848.

Comunicación, pues supone regular, por primera vez, la responsabilidad penal de las personas jurídicas, es decir, de las propias empresas frente a sus actos y los de sus empleados. Una responsabilidad por no vigilar; por negligencia, que puede ser más difícil de atajar o limitar por parte de las sociedades.

Queda por comprobar si a los Medios de Comunicación se les va a propinar mayor carga de posible responsabilidad penal por las acciones de sus profesionales que puedan suponer infracción de los nuevos preceptos penales en el ordenamiento jurídico español.

Glosando el nuevo artículo 31 bis del Código Penal, que establece la responsabilidad penal de las personas jurídicas[416], se concluye que la empresa, a partir de ahora, no solo es culpable si se beneficia de un hecho delictivo cometido por el administrador o representante, sino también si no ha establecido un código deontológico y un adecuado seguimiento de este, independientemente de la responsabilidad penal del representante, que es individual. La reforma impone, pues, un claro deber de autorregulación.

La inclusión de esta nueva figura jurídica es el resultado de adaptar el Derecho Penal español a las Directivas comunitarias que emanan del Tratado de Lisboa, y que ya fueron puestas en marcha en países como Francia, Holanda, Italia o Bélgica.

El Ministerio de Justicia ha publicado un resumen general de las modificaciones introducidas en el Código Penal, en formato que puede ser descargarlo por cualquier interesado[417].

[416] Ib., pág. 54825.

[417] Disponible en la página web del Ministerio de Justicia: <http://www.mjusticia.gob.es/cs/Satellite/es/1215197775106/Medios/1215327152743/Detalle.html >.

4. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y SUS INCIDENCIAS

4.1 Estructura de la Agencia Española de Protección de Datos.

La Agencia Española de Protección de Datos (AEPD) está concebida para asumir, en su conjunto, la defensa y protección de datos de carácter personal, atendiendo a los preceptos establecidos en la LOPD (Título VI, con rango de ley ordinaria). También encuentra su base legal en una norma más antigua, el Real Decreto 428/1993, de 26 de marzo[418], por el que se aprueba el Estatuto de la Agencia. La Ley la configura como "*un ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Nace y existe para hacer efectivo el derecho a la autodeterminación informativa, libertad informática o derecho a la intimidad*", según define Murillo de la Cueva[419].

Para llevar a cabo esa misión general protectora de derechos, la Agencia está estructurada orgánicamente por un Director, un Consejo Consultivo, el Registro General de protección de datos, la Inspección de datos y la Secretaría General.

El Director de la Agencia es nombrado por el Gobierno a propuesta del titular del Ministerio de Justicia de entre los miembros del Consejo Consultivo y no recibe instrucciones de autoridad alguna, por lo que desarrolla su cargo con independencia y objetividad. Desde enero de 2007 hasta 2011 ha sido Artemi Rallo, Catedrático de Derecho Constitucional de la Universidad Jaume I. En junio de 2011, José Luis Rodríguez Álvarez tomó posesión del cargo, tras la aprobación de su nombramiento por el Real Decreto 853/2011, previa deliberación del Consejo de Ministros el viernes 17 de junio de 2011[420].

El nuevo director de la Agencia es licenciado en Derecho y Profesor de Derecho Constitucional en la Facultad de Derecho de la Universidad Complutense de Madrid. En febrero de 2009 fue nombrado director del Gabinete del ministro de Justicia, cargo que ha desempeñado hasta la

418 B.O.E., núm. 106, de 4/5/1993, pág. 13244.

419 LUCAS MURILLO DE LA CUEVA, P.: "*Las funciones de la Agencia de Protección de Datos*". Agencia de Protección de Datos. Madrid, 1996, pág. 265.

420 B.O.E., núm. 145, de 18 de junio de 2011, sec. II.A, pág. 62954.

actualidad. También fue director gerente de la Fundación Democracia y Derecho Local entre los años 2002 y 2004.

Entre sus funciones, destacan las de "*resolver sobre si se procede o no a una inscripción que deba practicarse en el Registro General; requerir a los responsables de ficheros privados a que subsanen deficiencias de sus códigos tipo; resolver, previo informe del responsable del fichero, sobre si procede o no la denegación, total o parcial, del acceso a los ficheros policiales o tributarios automatizados*" tal y como recoge el art. 12 del Estatuto de la Agencia[421].

Siendo las citadas en primer término las de mayor trascendencia, el Director de la Agencia tiene también, y según recoge a continuación el art. 12 de su estatuto, la potestad de "*adoptar las medidas cautelares y provisionales que requiera el ejercicio de la potestad sancionadora de la Agencia con relación a los responsables de los ficheros privados; iniciar, impulsar la instrucción y resolver los expedientes sancionadores referidos a los responsables de los ficheros privados; iniciar la incoación de expedientes disciplinarios en casos de infracciones cometidas por órganos responsables de ficheros de Administraciones Públicas; autorizar la entrada en los locales con ficheros a fin de proceder a las inspecciones pertinentes, asegurando siempre las garantías legales de inviolabilidad del domicilio*". Su potestad sancionadora es conforma una de sus principales misiones, sostiene M. Fernández Salmerón[422].

Tiene, además, las funciones de gestión de la Agencia, recoge el art. 13 del Estatuto, como aprobación de la Memoria anual, formalización de contratos, cuentas…etc.

El Consejo Consultivo es un órgano colegiado de asesoramiento del Director de la Agencia sobre todas las cuestiones pudiendo además formular propuestas. Su composición la forman un Diputado del Congreso; un Senador; un representante de la Administración Central, designado por el Gobierno; un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias; un miembro de la Real Academia de la Historia; un experto en la materia, propuesto por el Consejo Superior de Universidades; un representante de los usuarios y consumidores; un representante de cada Comunidad Autónoma que haya creado una Agencia de Protección de Datos territorio (Madrid, Cataluña y

421 B.O.E. , núm. 106, de 04/05/1993, pág. 13246.

422 FERNANDEZ SALMERON, M.:"*Potestad sancionadora de la Agencia Española de Protección de Datos*. Aranzadi, 2008, págs. 33 y ss.

País Vasco cuentan con sus Agencias autonómicas), y un representante del sector de ficheros privados, propuesto por el Consejo Superior de Cámaras de Comercio, Industria y Navegación, mediante terna, según establece el art. 19 del Estatuto de la Agencia[423].

La Secretaría General es el órgano de la Agencia que desempeña funciones de apoyo y ejecución como son las relativas a notificación de Resoluciones del Director (artículos 30 y 31)[424]; se encarga de la elaboración de informes y propuestas que le solicite el Director; gestionar los medios personales y materiales de la Agencia; organizar conferencias y seminarios; facilitar información a las personas sobre los derechos que la Ley les reconoce en relación con el tratamiento de sus datos personales, para lo cual promueve campañas de difusión valiéndose de los Medios de Comunicación Social.

4.2.1. El Registro General de Protección de Datos.

El encargado, fundamentalmente, de "*velar por la publicidad de la existencia de los ficheros y tratamientos de datos de carácter personal con el objetivo de que puedan ejercitarse los derechos*" de los titulares de los datos, según el art. 23[425].

Le corresponde al Registro General de Protección de Datos la instrucción de los expedientes de inscripción, expedir certificaciones de los asientos y publicar la relación anual de los ficheros notificados e inscrito, recoge el art. 26 del Estatuto de la Agencia[426].

Es muy común que el Registro reciba solicitudes de información por parte de responsables de ficheros referentes a copia del contenido de la inscripción que tienen declarada, bien porque luego puede venir una modificación, o bien por atender las peticiones de una auditoría relacionada con el Documento de Seguridad de la entidad. Son comunes también las solicitudes de información de los órganos judiciales requiriendo copias y certificaciones de un tratamiento en relación al responsable del mismo.

---

423 B.O.E., núm. 106, de 04/05/1993, op. cit., pág. 13247.

424 Ibídem, pág. 13249.

425 Ib., pág. 13248.

426 Ib., pág. 13248.

En el Registro General consta la historia de todas las operaciones de inscripción efectuadas en la vida de un fichero o tratamiento, desde que se inscribe al inicio hasta que se suprime y elimina, con constancia de cada una de sus modificaciones.

4.2. Funciones de la Agencia Española de Protección de Datos.

La principal función de la Agencia Española de Protección de Datos, además de las ya relacionadas, es la de inspección e instrucción de expedientes, que deriva en la potestad sancionadora (residida en el art. 40 de la Ley Orgánica de Protección de Datos[427]) y la tramitación de los expedientes administrativos iniciados como consecuencia de las reclamaciones o denuncias recibidas.

Además, también ha pasado a ser competente para sancionar por incumplimientos en materia de Servicios de la Sociedad de la Información y Comercio Electrónico, como son los casos, cada vez más frecuentes, del envío, no solicitado, de comunicaciones comerciales por correo electrónico o cualquier otro medio, como recalca Ana Marzo[428].

Las medidas que la inspección conlleva engloban actuaciones de examen, análisis y prueba de sistemas, ficheros, documentos, dispositivos y, en general, de todos aquellos elementos relacionados con los posibles tratamientos de datos personales objeto de investigación.

La potestad sancionadora consiste en efectuar inspecciones periódicas o espontáneas, de oficio o a instancia de algún afectado, de cualquier fichero (público o privado), en los locales donde estén los ficheros y los equipos informáticos correspondientes del responsable o del encargado del tratamiento. Para todo ello, se le otorgan una serie de prerrogativas que enumera el art. 28 del R.D. 428/1993:

"- *Examinar los soportes de información que contengan los datos de carácter personal.*

- *Examinar los equipos físicos.*

- *Requerir el pase de programas y examinar la documentación pertinente al objeto de determinar, en caso necesario, los algoritmos de los procesos de que los datos sean objeto.*

[427] B.O.E. Núm. 298, de 14/12/1999, op. cit., pág. 43096.

[428] MARZO PORTERA, A.: op. cit., pág. 634.

- Examinar los sistemas de transmisión y acceso a los datos.

- Realizar auditorías de los sistemas informáticos con miras a determinar su conformidad con las disposiciones de la Ley Orgánica 5/1992.

- Requerir la exhibición de cualesquiera otros documentos que sean pertinentes.

- Requerir el envío de toda información precisa para el ejercicio de las funciones inspectoras"[429].

A fin de allanar el camino a la Agencia Española de Protección de Datos en la realización de esas atribuciones, se establece en la norma que los responsables de cada fichero quedarán obligados a permitir el acceso a los locales en los que se hallen los ficheros y los equipos informáticos con los datos de carácter personal, siempre previa acreditación de la autorización expedida por el Director de la Agencia, y salvaguardando y garantizando la inviolabilidad del domicilio particular, en su caso, como deja señalado el final del art. 28 del R.D. 428/1993 que se cita.

4.3. Las sanciones que contempla y aplica.

Las sanciones que aplica la Agencia en su tarea sancionadora e instructora en defensa de los derechos de los ciudadanos titulares de datos personales son establecidas por la Ley Orgánica de Protección de Datos (LOPD) en su art. 45, previa relación, en el art. 44[430], de una serie de infracciones que clasifica como leves, graves y muy graves, considerando que los infractores pueden ser tanto los responsables de los ficheros como los encargados de los tratamientos, estando ambos sujetos al régimen sancionador establecido por la norma.

Contempla de igual modo el caso de que se trate de ficheros o tratamientos cuyos responsables sean las Administraciones Públicas, para lo que la Ley dispone que podrá dictar una resolución el Director de la Agencia Española de Protección de Datos con las medidas disciplinarias y las sanciones a aplicar.

Hay que acudir al Reglamento que desarrolla la LOPD, al R.D. 1720/2007, para encontrar cómo la Agencia ha de articular la iniciación del

[429] B.O.E., núm. 106, de 04/05/1993, pág. 13249.

[430] B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43097.

procedimiento instructor, antes de sancionar. Para ello, ha de identificar al infractor, describir los hechos y calificarlos, indicar al presunto infractor de que puede allanarse o que puede formular alegaciones, y establecer, en su caso, medidas de carácter provisional. Lo recoge el art. 127 del R.D. 1720/2007[431].

Están establecidas las sanciones en el Título VII de la LOPD para cada una de las infracciones relacionadas en el art. 44 en función de su gravedad, si bien permite que sea la Agencia Española de Protección de Datos la que pueda graduar cada sanción a tenor de cada caso y circunstancias.

La Ley no consagra nuevos tipos delictivos, ni define supuestos de responsabilidad penal para la eventualidad de su incumplimiento, "*puesto que la sede lógica para tales cuestiones no es la LOPD, sino sólo el Código Penal, que sí lo hace. Sin embargo, atribuye a la Administración la potestad sancionadora*", apunta Ana Marzo[432].

Tras la aprobación del Reglamento de 1720/207, no fue hasta 2011, cuando se decidieron nuevos cambios en la normativa española de protección de datos de carácter personal, momento en el que se modifican ciertos aspectos del régimen sancionador de la LOPD.

Se llevan a cabo por medio de la Ley 2/2011[433], de 4 de marzo, de Economía Sostenible, que persigue, por un lado, incrementar la seguridad jurídica, así como modular la imposición de sanciones económicas a la trascendencia de la infracción cambiando la calificación de algunas infracciones antes tipificadas como muy graves, que pasan a ser consideradas graves, ampliando y sistematizando los criterios de graduación o atenuación que han de ser tenidos en cuenta por la Agencia.

Pero, sobre todo, la modificación legislativa permitirá aplicar la figura del apercibimiento, de forma que aquellas empresas que cometan una infracción leve o grave por primera vez, en lugar de ser sancionadas con una multa, la Agencia de Protección de Datos les advertirá de la irregularidad cometida y les requerirá la adopción de las medidas adecuadas que permitan, en cada caso, corregir la situación o evitar la repetición de la conducta infractora.

---

[431] B.O.E., núm. 17, de 19/01/2008, op. cit., pág. 4132.

[432] MARZO PORTERA, A.: op. cit., pág. 662.

[433] B.O.E., núm. 55, de 05/03/2011, sec. I, pág. 25033.

Respecto a la cuantía de las sanciones en sí, la normativa reguladora de la Protección de Datos, teniendo en cuenta los cambios introducidos por la Ley de Economía Sostenible, establece que:

- ✓ Las infracciones leves son sancionadas con multa de 900 euros a 40.000 euros (modificado por la Ley 2/2011, de 4 de marzo, de Economía Sostenible[434])
- ✓ Las infracciones graves son sancionadas con multa de 40.001 a 300.000 euros
- ✓ Las infracciones muy graves son sancionadas con multa de 300.001 a 600.000 euros.

El 15 de febrero de 2011, el pleno del Congreso de los Diputados aprobó, definitivamente, la reforma del Título VII, infracciones y sanciones, de la LOPD.

En concreto, son objeto de reforma por parte de la Ley 2/2011, de Economía Sostenible los artículos 43, 44, 45, 46, y 49 de la LOPD. Del examen de las modificaciones más importantes, es necesario destacar lo suprimido y lo que se añade.

En primer lugar, el artículo 44 de la LOPD. Contiene todo el elenco de infracciones por lo que se trata de artículo es muy importante al establecer qué conductas son constitutivas de infracción y su grado (leve, grave o muy grave). En relación a las infracciones leves, lo más relevante es que desaparecen dos infracciones: en primer lugar, dejará de considerarse infracción "*No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda*".

Y, en segundo lugar, desaparece la posibilidad de incumplir el deber de secreto como infracción leve. A partir de ahora, toda infracción del deber de secreto pasará a ser "*grave*", así que tampoco será posible vulnerar el deber de secreto de forma 'muy grave', a tenor del nuevo art. 44.3.d) de la Ley de Economía Sostenible[435].

Se añade una nueva infracción leve: *"La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de esta Ley*". Lo que puede entenderse como la materialización de los criterios que ha venido manteniendo la Agencia

[434] Ibídem, pág. 25232.

[435] Ib., pág. 25231.

Española de Protección de Datos. Esta infracción supone penalizar la conducta consistente en facilitar datos de carácter personal a un encargado del tratamiento por parte del responsable del fichero sin que medie el contrato y forma que exige el artículo 12 de la LOPD. Lo recoge el nuevo art. 44.2.d) de la Ley de Economía Sostenible[436].

Por tanto, si no existe el contrato mencionado, "*se entiende que lo que se ha producido es una cesión de datos de carácter personal, y como no va a existir el consentimiento para la cesión, al cedente (responsable del fichero) se le imputa una infracción muy grave, pero además, al cesionario una infracción grave por tratar los datos personales cedidos sin consentimiento (claro, si el que tiene el deber de obtener el consentimiento no lo hace, cuando los ceda llegarán ya intoxicados)*", según sostiene Samuel Parra[437]. A partir de la reforma introducida por la Ley de Economía Sostenible, se castiga expresamente el hecho de no firmar ese contrato del artículo 12.

Respecto a las infracciones graves, lo más relevante es el hecho de considerar que las cesiones de datos serán castigadas como infracción grave y no como muy grave, dejando la calificación de "muy grave" para casos muy concretos. Hasta la modificación, toda cesión de datos sin consentimiento se ha considerado una infracción muy grave.

Se añade una nueva infracción grave: "*El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por esta Ley y sus disposiciones de desarrollo*" donde podrán encajar diversas conductas desobedientes.

En relación a las infracciones muy graves, se simplifican y reducen significativamente y han pasado a cuatro: La recogida de datos en forma engañosa o fraudulenta; tratar o ceder los datos de carácter personal calificados de especial protección; no cesar el tratamiento ilícito cuando así lo ha requerido la autoridad; y transferir datos a países sin adecuado nivel de protección, como recoge el art. 44 en su nuevo apartado 4[438].

---

[436] Ib., pág. 25231.

[437] < http://www.samuelparra.com/2011/01/30/ley-economia-sostenible-podria-reformar-lopd/>.

[438] B.O.E., núm. 55, de 05/03/2011, op. cit., pág. 25032.

Han sido reformados y añadidos nuevos criterios para graduar las sanciones. Así, ahora se tendrá en cuenta, y según el tenor del nuevo art. 45.4 introducido por la Ley 2/2011 de Economía Sostenible:

"*a) El carácter continuado de la infracción.*

b) El volumen de los tratamientos efectuados.

c) La vinculación de la actividad del infractor con la realización de datos de carácter personal.

d) El volumen de negocio o actividad del infractor.

e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

f) El grado de intencionalidad.

g) La reincidencia por comisión de infracciones de la misma naturaleza.

h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.

i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.

j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora"[439].

De todas las modificaciones, probablemente la más relevante es la relativa a la adición de un nuevo apartado 6 en el artículo 45. Añade este precepto, que introduce la figura del 'apercibimiento': *"Excepcionalmente, el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que los hechos fuesen constitutivos de infracción leve*

[439] Ibídem, pág. 25232.

o grave conforme a lo dispuesto en esta Ley, y que el infractor no hubiese sido sancionado o apercibido con anterioridad. Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento"[440].

Este nuevo art. 45.6 deja en manos de la propia Agencia Española de Protección de Datos castigar las infracciones leves y graves, dejando como único límite que el infractor no hubiese sido sancionado o apercibido con anterioridad, aunque no indica el precepto si esa sanción o apercibimiento anterior debe ser de la misma naturaleza que la infracción de la que se pretenda no iniciar procedimiento sancionador.

Por último, la facultad prevista en el artículo 49 relativa a la posibilidad de inmovilizar ficheros, se extiende a los casos de infracciones graves. Recordemos que en la actualidad sólo es de aplicación para infracciones muy graves.

A la hora de graduar las sanciones en sus expedientes y resoluciones, la Agencia Española de Protección de Datos, hasta 2011, ha venido teniendo en cuenta una serie de criterios que resume A. Marzo:

"- *La naturaleza de los derechos personales afectados*

- *El volumen de los tratamientos efectuados*

- *Los beneficios obtenidos*

- *El grado de intencionalidad*

- *La reincidencia*

- *Los daños y perjuicios causados*

- *Y cualquier otra circunstancia relevante*"[441].

La labor de la Agencia Española de Protección de Datos se ha traducido en numerosas actividades para facilitar el cumplimiento de la Ley. En la última Memoria presentada por su director en el Congreso de los Diputados, celebrada en diciembre de 2010[442], se recoge, a modo de

[440] Ib., pág. 25233.

[441] MARZO PORTERA, A.: op. cit., pág. 670.

[442] Disponible en el canal de documentación de la Agencia de Protección de Datos: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/comparecencias/index-ides-idphp.php>.

balance, que la Agencia ha ampliado el catálogo de guías prácticas dirigidas a los usuarios de Internet, al sector de la videovigilancia y a la protección de datos en las relaciones laborales, y que atendió, sólo en 2009, cerca de 100.000 consultas (un 34% más que en 2008) a través del servicio de Atención al Ciudadano y cerca de 700 consultas de mayor complejidad ha atendido mediante informes del Gabinete Jurídico de la Agencia.

Destaca el hecho de que han sido informados preceptivamente por parte de la Agencia Española de Protección de Datos hasta 100 proyectos de disposiciones generales entre las que destacan: la normativa reguladora del acceso electrónico de los ciudadanos a los servicios públicos; la prevención del blanqueo de capitales y la financiación del terrorismo; diversas normas relacionadas con el tratamiento de datos en el sistema nacional de salud; el Anteproyecto de Ley Orgánica de Salud Sexual y Reproductiva y de la Interrupción voluntaria del embarazo; y el intercambio de información e inteligencia entre los servicios de seguridad de los Estados de la Unión Europea.

Y durante el año 2009, "*ha impulsado la notificación de ficheros al Registro General de Protección de Datos a través de Internet (utilizándose ya en el 90% de los casos). Casi 100.000, son notificaciones firmadas con certificado electrónico. Todo ello ha supuesto la inscripción de casi 400.000 nuevos ficheros, con un incremento del 50% sobre 2008, alcanzando una cifra total de casi 1.650.000 al cierre de 2009*"[443], según ensalza la Agencia. Esta cifra ascendía ya a finales de 2010 a más de 2.076.000 ficheros notificados en España.

Otro dato significativo es que la Agencia ha incorporado una nueva herramienta, por medio del programa '*EVALÚA*', que permite a las empresas y a las Administraciones Públicas analizar gratuitamente su nivel de cumplimiento de la LOPD de forma anónima y gratuita.

Por último, la Agencia destaca el hecho de que "*ha promovido, con la Federación Española de Comercio Electrónico y Marketing Directo la puesta en marcha de un fichero de exclusión, conocido más coloquialmente como Lista Robinson, para evitar que quienes no quieren recibir publicidad puedan evitarlo*"[444]. Este Servicio permite a los ciudadanos gestionar la publicidad que reciben y, muy especialmente, posibilita a los padres o tutores solicitar que no se traten datos de menores para el envío de

[443] Ibídem, pág. 5.

[444] Ib., pág. 6.

publicidad. También permite seleccionar los canales a través de los que no se desea recibir publicidad.

Prioriza, en resumen, políticas preventivas dirigidas a ampliar la información, conocer cómo se cumple la norma y cómo mejorar su cumplimiento, facilitar la inscripción de ficheros, impulsar la autorregulación y a ofrecer nuevas herramientas para evitar la publicidad no deseada.

4.4. Sede electrónica de la Agencia Española de Protección de Datos.

Ha sido emitida la Resolución de 18 de marzo de 2010[445], de la Agencia Española de Protección de Datos, por la que se crea la Sede Electrónica de la Agencia.

La dirección de referencia de la nueva sede electrónica de la AEPD es <https://sedeagpd.gob.es>. También se podrá acceder a través del portal de Internet <http://www.agpd.es>.

Los canales de acceso a los servicios disponibles en la sede electrónica de la AEPD son enumerados en el art.5 de la Resolución:

"*a) Acceso electrónico, a través de Internet.*

b) Atención presencial en las oficinas de la AEPD, sin perjuicio del acceso a través de los registros regulados en el artículo 38 de la Ley 30/1992.

c) Atención telefónica. Los teléfonos actuales son: 901 100 099 y 91 266 35 17"[446].

Para la formulación de quejas y sugerencias. Los medios disponibles son los que relaciona la Resolución de 18 de marzo de 2001 en su art. 6:

"*a) Presencial o por correo postal en la dirección de la Agencia Española de Protección de Datos, calle Jorge Juan, 6, 28001 Madrid, o a través de otro órgano administrativo, conforme al art. 38 de la Ley 30/1992, y*

[445] B.O.E., núm. 72, de 24/03/2010, sec. I, pág. 28401.

[446] Ibídem, pág. 28402.

b) Presentación telemática a través de la sede electrónica de la AEPD"[447].

La sede electrónica de la AEPD dispondrá del contenido y de los servicios a disposición de los ciudadanos previstos expresamente en el artículo 6 del Real Decreto 1671/2009, de 6 de noviembre por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos[448].

4.5. Fundación Española para la Protección de Datos.

La Fundación Española para la Protección de Datos es una entidad sin ánimo de lucro de referencia en el sector, surgida en 2009 para la difusión y promulgación de estos derechos, que pone a la disposición de los ciudadanos sus recursos para la adaptación de las empresas a la LOPD, y la formación de sus trabajadores. Según los estudios realizados por la Fundación, la inmensa mayoría de las empresas españolas no cumplen con la legalidad en materia de protección de datos por lo que tienen escaso control de los datos que manejan, "*comprometiendo la seguridad e integridad de los datos de sus clientes, personal y proveedores*", según reseña en la presentación de su página web[449].

Con el objetivo de fomentar la cultura de protección de datos y facilitar mejores prestaciones a las empresas, la Fundación firma convenios con asociaciones empresariales, federaciones, gestorías, asesorías y otras entidades. Con ello trata de poner al alcance de empresas y organizaciones un nuevo servicio que ofrecer a sus clientes, actuando como proveedor en la adaptación de las empresas a la LOPD y en la formación de personal. Trata así de conseguir que las empresas españolas den por cumplidos los requisitos exigidos legalmente en materia de protección de datos.

La Fundación ofrece un dossier con datos para aquellas empresas que quieran adherirse a la misma, en el que advierte que "*la vulnerabilidad de la información y el impacto de un ataque cibernético puede ir más allá*

[447] Ib., pág. 28402.

[448] B.O.E., núm. 278, de 18/11/2009, sec. I, pág. 97921.

[449] Véase: <http://www.fundacionprotecciondedatos.es/index.php>.

de la pérdida de datos y afectar a la confianza del cliente, la reputación de la empresa y la marca, y acarrear sanciones"[450].

Mediante su servicio de adaptación, persigue que la empresa esté en condiciones de, entre otras cosas, poder efectuar todos los tratamientos establecidos por la LOPD.

La Fundación ofrece un servicio orientativo y de asesoramiento avalado por el más alto nivel de calidad, pues ostenta certificaciones ISO 27001 e ISO 20000[451]. La norma ISO 27001 permite a las empresas certificar su Sistema de Gestión de Seguridad de la Información (SGSI). Se da un paso más en la madurez y gestión de la empresa certificándola en ISO 20000, una norma que muestra el compromiso con la buena gestión de los servicios de tecnologías de la información (TI). Implantar estas normas ofrece garantías de seguridad y formas de trabajo.

[450] Dossier de adhesión a la Fundación Española de Protección de Datos, pág. 19: <http://www.fundacionprotecciondedatos.es/UNETE-A-LA-FUNDACION/index.php>.

[451] Normas con estándares internacionales emitidas por ISO, la Organización Internacional para la Estandarización a fin de mejorar un Sistema de Gestión de Seguridad de la Información.

5. LA PRENSA ESCRITA Y EL USO DE DATOS

5.1. La publicación de datos personales.

La protección de los datos personales cede, como han defendido nuestros tribunales de justicia, entre ellos el Tribunal Constitucional, en la mayoría de los casos, ante el derecho a la información, y como señala el *Considerando 37* de la Directiva 95/46 de Protección de Datos Personales[452], tal y como hemos visto en el Capítulo 6, a la libertad de expresión o la libertad de recibir o comunicar informaciones.

Ha quedado establecida por nuestra jurisprudencia la prevalencia de las libertades que se asientan en el art. 20 de la Constitución Española[453], aunque en esa confrontación ante el derecho de protección de datos de carácter personal, el de la libertad de información transmitida sea veraz, y esté referida a asuntos públicos que son de interés general por las materias a que se refieren y por las personas que en ellos intervienen, contribuyendo, en consecuencia, a la formación de la opinión pública.

Otra variante puede llegar a tener el dato referido a la imagen, es decir, la publicación de fotos de personas en la prensa escrita. Como ha quedado explicado en Capítulos anteriores, las imágenes son datos personales siempre que sean identificables y ha sido objeto de pronunciamientos por parte de la Agencia Española de la Protección de Datos, como el Informe 0624/2009, sobre protección de datos y libertad de expresión e información[454], emitido por una consulta que se plantea sobre si para la publicación de la fotografía ganadora de su concurso de fotografía en una revista de eventos sobre las fiestas de moros y cristianos de la ciudad de la persona reclamante, en la que figure la imagen de personas físicas o menores, necesita la obtención del consentimiento informado de los afectados, y si éste debería recabarlo de quien presenta a concurso dicha fotografía ganadora.

---

[452] Diario Oficial de la Unión Europea, núm. L 281, de 23/11/1995, op. cit., pág. 34.

[453] B.O.E., núm. 311, de 29/12/1978, op. cit., pág. 29317.

[454] Informe Jurídico de la Agencia Española de Protección de Datos sobre la publicación de fotografías, basado en que la imagen es un dato personal. Véase: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdfs/2009-0624_Publicaci-oo-n-en-revista-de-foto-ganadora-de-concurso-con-im-aa-genes-de-personas.-No-necesidad-de-consentimiento.pdf>.

La Agencia vuelve a decantarse por la prevalencia del derecho a la libertad de información consagrado en el artículo 20 de la Constitución Española al entrar en colisión con el derecho a la intimidad y a la protección de datos de los afectados, y recuerda en su argumentación que la jurisprudencia del Tribunal Constitucional tiende a otorgar una posición preferente a la libertad de información frente a otros derechos constitucionales, "*siempre y cuando los hechos comunicados se consideren de relevancia pública (STC 105/1983, STC 107/1988) y atendiendo a la veracidad de la información facilitada (STC 6/1988, STC 105/1990, STC 240/1992)*", argumenta el Informe de la Agencia[455]. También es recordado aquí el art. 9 de la Directiva 95/46 para la argumentación.

En consecuencia, por tanto, para admitir la publicación de videos y fotos en la revista de la entidad consultante, sin recabar el consentimiento de los ciudadanos afectados, es preciso que la información publicada tenga relevancia pública, es decir, que se den las circunstancias constitucionalmente previstas para que la libertad de información prevalezca sobre el derecho a la protección de datos de carácter personal, como resulta ser el caso analizado del citado Informe Jurídico 0624/2009, en el que la publicación se refiere a acontecimientos festivos y culturales de la ciudad donde la revista tiene difusión.

5.1.2. Las Cartas al Director.

El caso de las cartas al director del periódico también ha motivado algún pronunciamiento de la Agencia Española de Protección de Datos, como la Resolución que dicta en el procedimiento TD/01161/2008[456]. El 2 de junio de 2008, tuvo entrada en la Agencia una reclamación de un ciudadano contra un diario escrito, en concreto, contra La Nueva España, Diario Independiente de Asturias, por no haber sido debidamente atendido su derecho de cancelación. El reclamante pedía que se eliminaran de la publicación los detalles de su identificación personal, es decir, nombre y dos apellidos junto a la carta. La Agencia recuerda en su Resolución, que la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de

[455] Ibídem, pág. 3.

[456] Resolución R/01827/2008 de la Agencia Española de Protección de Datos: <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2009/common/pdfs/TD-01161-2008_Resolucion-de-fecha-13-01-2009_Art-ii-culo-16-LOPD.pdf>.

acceso, rectificación y cancelación[457], establece que el responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción, dando así la razón al reclamante para que se procediera a cancelar el nombre y los apellidos de la publicación, recordando, al respecto, la infracción que recoge el art. 44 de la LOPD.

De igual modo, la R/01567/2008[458], en la que la Agencia atiende una reclamación contra el buscador Google, que no adoptó las medidas técnicas pertinentes para que no aparecieran en su memoria 'caché' datos referidos a la sección de 'cartas al director' del Periódico de Extremadura.

5.1.2. El caso de "Abc" de Sevilla y Google.

El caso de una reclamación cursada ante la Agencia Española de Protección de Datos por parte de una ciudadana que solicitó el derecho de oposición al tratamiento de sus datos personales ante la hemeroteca del periódico "Abc" de Sevilla mediante escrito de fecha 18 de enero de 2010 contra la reproducción telemática de una noticia ocurrida en el año 1975 en la que aparecía la identidad de la reclamante, que demandó también a Google Spain SL, ante quién solicitó el derecho de cancelación de sus datos personales mediante escrito de fecha 28 de octubre de 2009, es ejemplarizante.

La reclamación da lugar a la Resolución de 24 de mayo de 2010, dictada en el procedimiento nº TD/00030/2010[459], en la que la Agencia Española de Protección de Datos da la razón a la ciudadana en su reclamación de derecho de cancelación ante Google, pero no en su pretensión de derecho de oposición ante "Abc" de Sevilla.

En concreto, como contestación al derecho de cancelación ejercido por la reclamante contra Google Spain, esta empresa señaló que no podía proceder a lo solicitado, debido a que las informaciones de los resultados

[457] B.O.E., núm. 25, de 29/1/1998, pág. 3058.

[458] Véase:< http://www.agpd.es/portalwebAGPD/resoluciones/index-ides-idphp.php>.

[459] Véase: <http://www.agpd.es/portalwebAGPD/resoluciones/recursos_reposicion/rr_sobre_tutela_de_derechos/common/pdfs/REPOSICION-TD-00030-2010_Resolucion-de-fecha-03-09-2010_Art-ii-culo-16-LOPD.pdf>.

de búsqueda se encuentran en páginas web de terceros cuyo acceso es público, y que para eliminar contenido de los resultados necesitan la colaboración del webmaster, es decir, el sitio web donde se incluye la información.

Respecto a los argumentos de "Abc" de Sevilla, con fecha 18 de enero de 2010, la reclamante ejercitó el derecho de oposición de sus datos personales que aparecen digitalizados por una noticia publicada en el diario "Abc" el día 5 de septiembre 1975, manifestando que existen motivos fundados y legítimos relativos a su situación personal, para evitar la difusión pública desproporcionada de unos datos de carácter personal debido a la naturaleza de la noticia. "Abc" de Sevilla le manifestó "*la imposibilidad de hacer efectiva la oposición solicitada basándose en que es una empresa que se encarga de digitalizar el diario ABC, y por tanto, es un medio de comunicación que realiza su actividad amparados en el derecho a informar reconocido en el artículo 20 de la Constitución Española*"[460].

En su Resolución, la Agencia señala en relación a este derecho de informar, y ante la ausencia de Exposición de Motivos de la Ley Orgánica de la Protección de Datos, que cabe acudir a los *Considerandos* de la Directiva 95/46/CE, de la que aquella trae causa, cuyo número 45 señala que "*cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la autoridad pública, o en interés legítimo de una persona física, cualquier persona deberá, sin embargo tener derecho a oponerse a que los datos que le conciernan sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; que los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales contrarias*"[461].

Recuerda los preceptos de la LOPD sobre consentimiento del afectado para el tratamiento de sus datos de carácter personal y sobre el ejercicio del derecho de oposición para afirmar que la propia Constitución Española reconoce la libertad de expresión y le otorga una posición prevalente, en el caso de que se trate de información veraz de relevancia pública, como ha sido desarrollado en múltiples sentencias del Tribunal Constitucional.

---

460 Ibídem, pág. 1.

461 Diario Oficial de la Unión Europea n° L 281, de 23/11/1995, op. cit., pág. 35.

Con estas argumentaciones, la Agencia Española de Protección de Datos decide proceder a desestimar la reclamación de Tutela de Derechos contra "Abc" Sevilla, dando la razón al periódico, aunque dejando escrito que "*no obstante, los medios de comunicación deberían valorar la necesidad de que su actuación se dirija a conciliar, en mayor medida, el derecho a la libertad de información con la aplicación de los principios de protección de datos personales. En primer lugar, debiera ponderarse escrupulosamente la relevancia pública de la identidad de las personas afectadas por el hecho noticiable para, en el caso de que no aporte información adicional, evitar la identificación mediante la supresión del nombre e incluso, si fuera necesario, de las iniciales o cualquier referencia suplementaria de la que pueda deducirse la identificación, en el caso de que el entorno sea limitado. Junto a ello, no cabe duda de que el desarrollo de Internet y la implantación generalizada de los motores de búsqueda suponen una actualización y divulgación exponencial y permanente de la información en prensa así como de los datos personales incluidos en la misma como la identidad de las personas. Deberían por ello los medios de comunicación reflexionar sobre la trascendencia que tiene mantener de manera permanente una absoluta accesibilidad de los datos contenidos en noticias cuya relevancia informativa probablemente es inexistente en la actualidad. Y tener en cuenta la trascendencia sobre la privacidad de las personas que puede derivar de ello*"[462].

Ante esta consideración tan importante, en la que la Agencia Española de Protección de Datos tiene en cuenta que la divulgación de datos de carácter personal cobra una nueva dimensión con el desarrollo de las nuevas tecnologías de la comunicación, lanza un mensaje dirigido a las nuevas cautelas que habrán de adoptarse para la difusión de información, indicando que "*los medios de comunicación debieran usar medidas informáticas para que, en el caso de que concurra interés legítimo de un particular y la relevancia del hecho haya dejado de existir, se evite desde su webmaster la indexación de la noticia por los motores de búsqueda en Internet. De esta forma, aún manteniéndola inalterable en su soporte –no se borraría de sus archivos ni de sus históricos- se evitará su divulgación indiscriminada, permanente y, en su caso, lesiva. Por contra, la libertad de información no impone que los datos personales de la reclamante figuren en los índices que utiliza Google para facilitar al usuario el acceso a determinadas páginas, ni tampoco preceptúa que figuren en las páginas que Google conserva temporalmente en memoria 'caché'. Es decir, no es una actividad amparada por la libertad de información, sin que exista, una*

[462] Resolución de 24/05/2010, del procedimiento nº TD/00030/2010, pág. 7.

disposición legal o constitucional en contra del ejercicio del derecho de cancelación frente a Google"[463].

De acuerdo con lo expuesto, la Agencia Española de Protección de Datos decide que se proceda a la exclusión de los datos personales de la reclamante de los índices elaborados por Google, estimando en este sentido la petición de tutela de derechos. En la misma línea, la Resolución nº R/00898/2010 interpuesta contra Google y la versión digital del diario "La Vanguardia"[464]. En este caso, la Resolución deja sentado que Google obtiene en España datos personales que afectan a la dignidad de la persona y puede lesionar derechos de un tercero, por lo que es la Agencia Española de Protección de Datos la competente para velar por el cumplimiento de la normativa.

E insiste en su consideración de que "*cabe proclamar que ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la Red sin poder reaccionar ni corregir la inclusión ilegítima de los mismos en un sistema de comunicación universal como Internet*"[465].

Nos remitimos al Capítulo dedicado a las páginas y/o sitios webs, en el que analizamos la indexación de datos en las versiones digitales de los Medios de Comunicación, especialmente utilizadas cada vez más amplia e intensamente por los periódicos.

5.2. Creación de ficheros de datos inscritos por los periódicos.

Centramos nuestro estudio de campo en los periódicos "Abc" de Sevilla, perteneciente al Grupo Vocento, "Diario de Sevilla", del Grupo Joly, y "EL Correo de Andalucía", antes del Grupo Prisa, posteriormente vendido al Grupo Alfonso Gallardo, al ser los tres diarios de referencia

[463] Ibídem., pág. 8.

[464]<http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-01887-2009_Resolucion-de-fecha-24-05-2010_Art-ii-culo-6.4-LOPD_Recurrida.pdf>.

[465] Ibídem, pág. 20.

tradicional y de claro arraigo en la provincia sevillana al hablar de prensa escrita.

5.2.1. Ficheros declarados por "Abc".

Un total de once ficheros tiene inscritos en el Registro de la Agencia Española de Protección de Datos el diario "Abc" de Sevilla, vinculados a su dirección postal de la isla de la Cartuja.

Se trata de un inventario directivo para la gestión de recursos humanos, los acreedores y deudores, listado de personas a invitar en actos sociales, para gestionar las nóminas, seguimiento de los programas de formación, datos de los suscriptores, sobre los puntos de venta para la distribución del periódico, y los relacionados al registro de entrada en las instalaciones y para la prevención de riesgos laborales. Son todos ellos ficheros con datos vinculados directamente a la gestión administrativa y económica del periódico. Quedan relacionados en el Anexo que dedicamos a los ficheros inscritos por el diario "Abc" de Sevilla.

5.2.2. Ficheros declarados por "El Correo de Andalucía".

También once ficheros tiene declarados ante la Agencia el diario "El Correo de Andalucía". Todos adscritos a su dirección sevillana de Américo Vespucio, salvo el fichero de la hemeroteca, que lo tiene con dirección en la Avenida de la Prensa, antigua sede de sus instalaciones.

En concreto, el fichero que denomina 'Hemeroteca' tiene como fin recopilar datos que conforman una base documental para su uso en plena actividad periodística.

Ha adoptado, por otra parte, la decisión de confeccionar un fichero para los usuarios de su web, para una adecuada gestión de quienes se registran en su website o página web para participar en concursos o promociones y suscribirse a boletines.

Ha elaborado además un fichero sobre su tienda on line, para la gestión de sus relaciones comerciales a través de la web. Tiene otro dedicado a todos sus colaboradores, así como los habituales sobre suscriptores, para gestión de personal, y de control de acceso a sus instalaciones.

Todos ellos están enumerados en el Anexo que dedicamos a los ficheros inscritos ante la Agencia Española de Protección de Datos por el diario sevillano El Correo de Andalucía.

5.2.3. Ficheros declarados por "Diario de Sevilla".

Perteneciente al Grupo Joly, empresa periodística que abarca varias cabeceras en Andalucía, este periódico ha atendido la tendencia que no parece tener retorno de promover promociones y concursos a través del diario que se distribuye cada día en los numerosos puntos de venta, y ha elaborado ficheros relativos a todas las promociones, sorteos y análogos.

Dispone también de un fichero con datos de anunciantes, y otros para la gestión de personal. En total, cinco con la dirección de la calle Rioja, de Sevilla, aunque el Grupo empresarial tiene registrados en la Agencia Española de Protección de Datos otros ficheros con diferente razón social (Federico Joly y Cia SA) y con dirección en Cádiz, sede matriz de esta empresa titular de periódicos en varias provincias.

En el Anexo correspondiente quedan relacionados los ficheros declarados por "Diario de Sevilla".

6. LAS CADENAS DE EMISORAS DE RADIO Y LA LEGALIDAD DE LOS DATOS.

6.1. La voz como bien jurídico a proteger.

La voz es un dato personal, como ya hemos dejado escrito en el Capítulo 3 del presente estudio, y es un bien jurídico a proteger que, en el caso de las cadenas de emisoras de Radio, adquiere especial consideración. Pero, además, hay que tener en cuenta la opinión y/o información expresada y difundida a través de la voz la que puede colisionar con el derecho a la protección de datos.

La Agencia Española de Protección de Datos ha llegado a tener que emitir una Resolución, la Nº E/00949/2007, de mayo de 2008[466], por la denuncia presentada por una ciudadana contra la cadena de emisoras de "Radio Popular, Cope", en la que planteaba la denunciante sentirse dañada al apuntar que el programa radiofónico 'El Tirachinas' difundió la lectura de un documento comprensivo de datos de carácter personal relativos a su persona y a su ámbito familiar, al referirse el locutor en la emisión a una serie de datos relativos a propiedades de la denunciante y de familiares, ofreciendo detalle de fincas y de otras cuestiones de carácter personal. En concreto, el periodista dio cuenta del contenido de una escritura pública a la que había tenido acceso. Planteaba la denunciante la existencia de una vulneración de medidas de seguridad, de captación de datos de forma fraudulenta sin haber mediado su consentimiento.

Por su parte, la "Cope" argumenta en su defensa ante la Inspección de Datos que "*presta servicios de radiodifusión sonora, cuyo objeto es difundir noticias, ideas y opiniones en el ejercicio del derecho a la información y a la libertad de expresión recogidos en el art. 20 de la Constitución Española*"[467]. Alega la cadena de emisoras de Radio que el periodista está amparado en el derecho al secreto profesional en el ejercicio de comunicar información veraz y manifiesta que se le indicó a la denunciante, en contestación al derecho de acceso, oposición y cancelación

[466] Resolución de la denuncia interpuesta contra la Cadena de Emisoras, disponible en: <http://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/archivo_actuaciones_2008/common/pdfs/E-00949-2007_Resolucion-de-fecha-09-05-2008_Art-ii-culo-10-LOPD-y-20-CE.pdf>.

[467] Ibídem, pág. 2.

de la LOPD, que no mantiene los datos que hayan podido emitirse en el citado programa más allá de su emisión.

En su Resolución Nº E/00949/2007, de mayo de 2008, la Agencia Española de Protección de Datos recuerda el art. 20 de la CE para decir que "*aunque el secreto profesional establecido en este artículo 20.1.d) de la Constitución no ha sido regulado hasta la fecha, ello no obsta para que no tenga aplicación directa en virtud de ese mismo mandato constitucional*". Y argumenta que "*la Jurisprudencia del Tribunal Constitucional tiende a otorgar una posición preferente a la libertad de expresión frente a otros derechos constitucionales, siempre y cuando los hechos comunicados se consideren de relevancia pública y atendiendo a la veracidad de la información facilitada*"[468].

Remarca lo que el Tribunal Constitucional afirma cuando se produce una colisión entre la libertad de información y el derecho a la intimidad y al honor, en la que, en general, la primera goza "*de una posición preferente y las restricciones que de dicho conflicto puedan derivarse a la libertad de información deben interpretarse de tal modo que el contenido fundamental del derecho a la información no resulte, dada su jerarquía institucional desnaturalizado ni incorrectamente relativizado. Resulta obligado concluir que en esa confrontación de derechos, el de la libertad de información transmitida sea veraz, y esté referida a asuntos públicos que son de interés general por las materias a que se refieren y por las personas que en ellos intervienen, contribuyendo, en consecuencia, a la formación de la opinión pública* (STC 171/1990)"[469].

Enlaza las argumentaciones basadas en nuestro ordenamiento con el comunitario, al afirmar la Resolución que lo anterior viene a coincidir, en términos generales, con la propia Directiva 95/46/CE, cuyo *Considerando 37* literalmente señala que, "*para el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio*

[468] Ib., pág. 4.

[469] Ib., pág. 4.

Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales"[470].

Asimismo, continúa reseñando la Agencia Española de Protección de Datos en esta importante Resolución, que la Audiencia Nacional en Sentencia de 12 de enero de 2001[471], considera "*que en la legislación española no existe un tratamiento específico de la concurrencia del tratamiento de datos automatizados de datos personales, con la libertad de información, en contra de lo que ocurre en la normativa europea. En esta línea, la Sala recuerda el Convenio para la protección de las personas con respecto al tratamiento de datos automatizados de datos de carácter personal (BOE de 15 de noviembre de 1985)*".

Continúa sus argumentaciones para afirmar que, en este caso de divulgación de datos a través de la cadena de emisoras de Radio, teniendo en cuenta la doctrina constitucional, "*el derecho fundamental que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, cede ante las libertades del artículo 20 de la Carta Magna*"[472]. Recuerda las obligaciones que tiene el responsable del fichero de datos citando el art. 10 de la LOPD, para asentar que, en todo caso, si se considera lesionado el derecho al honor o a la intimidad personal, la persona afectada podrá acudir a los tribunales de la jurisdicción ordinaria de orden civil, al amparo de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen[473], "*dado que la Agencia Española de Protección de Datos no es el órgano competente para dirimir estas cuestiones, que deben ser resueltas en sede jurisdiccional"*, concluye la citada Resolución NºE/00949/2007.

---

[470] Diario Oficial n° L 281 de 23/11/1995, op. cit., pág. 0031.

[471] Recogida en el Informe 0624/2009 de la Agencia Española de Protección de Datos, sobre publicación de datos personales en una revista. Véase: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdfs/2009-0624_Publicaci-oo-n-en-revista-de-foto-ganadora-de-concurso-con-im-aa-genes-de-personas.-No-necesidad-de-consentimiento.pdf>.

[472] Ibídem.

[473] B.O.E., núm. 115, de 14/5/1982, pág. 12546.

El caso es referente en nuestra materia de estudio, pues rechaza las pretensiones del reclamante y respalda la emisión de la "Cadena Cope" al sobreponer el derecho a la libertad de información.

6.2. Los llamantes a concursos y las grabaciones de voz.

Concierne a las emisoras de Radio las consideraciones que la Agencia Española de Protección de Datos ha compendiado al referirse a las grabaciones de voz de personas que, en una práctica cada vez más habitual, componen bases de datos, remarcando el derecho que tienen los ciudadanos a poder acceder a esas grabaciones y ejercer sus derechos.

Han sido varias las Resoluciones dictadas sobre grabaciones de voz y derecho de acceso a esas bases, como la R/01127/2009, formulada tras la reclamación de un particular contra Telefónica España, y basada en el Informe Jurídico 497/2007[474], sobre grabaciones de voz, en el que la Agencia indica que los artículos 1 y 2 de la LOPD, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, y acude a la definición del artículo 3.a) de la Ley Orgánica como "*cualquier información concerniente a personas físicas identificadas o identificables*", para señalar que la voz recogida en grabaciones, sólo podrán ser consideradas como datos de carácter personal cuando las mismas permitan la identificación de las personas que aparecen en dichas voces, no encontrándose amparadas en la Ley Orgánica de Protección de Datos en el caso contrario.

Argumenta la Agencia Española de Protección de Datos, además, que será necesario que esos datos se encuentren incorporados a un fichero, definido como "*todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*"[475], por el artículo 3.b) de la Ley. En consecuencia, en caso de haberse hecho efectiva la recogida de las voces en un fichero y haberse procedido a la identificación de las voces por asociación con otros datos personales, tal circunstancia debería comunicarse a quienes pudieran aparecer en dichas voces, debiendo

[474] En el canal de documentación dedicado a los Informes Jurídicos de la Agencia Española de Protección de Datos. Véase: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdfs/2007-0497_Grabaciones-de-voz-por-los-agentes-de-tr-aa-fico.pdf>.

[475] B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43088.

además el fichero resultante ser inscrito en el Registro General de Protección de Datos.

Para el acceso a grabaciones de voz, recuerda la Agencia en su Resolución R/01688/2009, al abordar una reclamación de particular contra Vodafone España para acceder a grabaciones de voz, que el artículo 29.3 del Real Decreto 1720/2007, determina que "*la información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos*"[476].

Insiste en que a la hora de facilitar las grabaciones, si se hace en un CD, debe añadirse las claves y/o códigos de acceso sin problemas de cifrado de datos.

Es claro, por tanto, el hecho de que el responsable de toda base de datos con grabaciones de voz que permitan identificar a personas debe ofrecer las garantías y derechos que establece la Ley Orgánica de Protección de Datos, y que queda sujeta a las obligaciones que marca, en este sentido, la normativa española.

6.3. La creación de ficheros por las cadenas de emisoras de Radio.

Las cadenas de emisoras de Radio que operan en Sevilla tienen centralizada a nivel nacional la gestión y declaración de ficheros con bases de datos de carácter personal, y los incluyen en el conjunto de las inscripciones que las empresas han efectuado ante el Registro de la Agencia. De esta manera, las emisoras de Radio que difunden sus programaciones desde Sevilla tienen sus ficheros inscritos con sede en Madrid, a excepción de "Canal Sur Radio", cuyas bases de datos están vinculadas a los ficheros declarados por "Radio y Televisión de Andalucía, Rtva".

[476] B.O.E., núm. 17, de 19 /01/2008, op. cit., pág. 4116.

6.3.1. "Radio Nacional de España".

La cadena de emisoras de "Radio Nacional de España" tiene inscritos una treintena de ficheros en el Registro General de la Agencia Española de Protección de Datos dedicados tanto a gestión económico-administrativa como a actividad ligada al ejercicio de la labor periodística[477].

En concreto, tiene inscrito un fichero, de nombre 'Agendari', con datos de carácter personal para la localización de invitados para las intervenciones en programas radiofónicos, tal como lo señala en la finalidad del mismo. Significativo es también el fichero que dedica a los oyentes, bajo esas siglas, y que tiene como fin la gestión de las reclamaciones y preguntas de los oyentes de los distintos programas de radio[478].

Tiene inscritos, además, ficheros dedicados a la gestión del personal de la empresa, así como otro dedicado a personal colaborador, denominados 'Data Personal RNE' y 'Personal Colaborador', y uno titulado 'Banco de Datos'[479], para la gestión de puestos de trabajo vacantes con personas que han realizado prácticas o pruebas específicas en la empresa.

El resto de los treinta ficheros que tiene declarados "Radio Nacional de España" ante el Registro General de la Agencia Española de Protección de Datos están centrados a tareas administrativas y de gestión económica, como los configurados con datos para nóminas, promociones, candidatos, clientes, proveedores, etc., e incluso tiene elaborado un fichero con datos para el seguimiento de las reclamaciones que tiene en vía judicial.

No tiene ninguno de esos ficheros inscritos con dirección en su sede de Sevilla, desde donde emite para su cobertura regional en Andalucía. Los tiene todos ellos vinculados a la dirección madrileña de Pozuelo de Alarcón, donde se encuentran sus estudios centrales nacionales.

---

477 Anexo número 6 de esta Tesis.

478 Ibídem.

479 Ib.

6.3.2. "Cadena SER".

La "Cadena SER", en lo referido a su cabecera de la capital andaluza, "Radio Sevilla", también tiene centralizados sus ficheros con bases de datos personales en su empresa de ámbito nacional, con sede en la capital de España. Lo que caracteriza a sus ficheros es la correspondencia de ellos a diferentes firmas del Grupo empresarial. Los inscribe a nombre de "Prisa Radio", "Sociedad Española de Radiodifusión", "Antena 3 Radio", "Comunicación Radiofónica" y "Sociedad de Servicios Radiofónicos Unión Radio".

Tiene, en total, once ficheros declarados ante el Registro General de la Agencia Española de Protección de Datos. Casi todos ellos están dedicados a datos relacionados con la gestión económica y administrativa de su amplia red de emisoras, la mayor de España, y ninguno con datos de carácter personal que tengan que ver con la actividad meramente periodística.

Inscribe un fichero con el nombre de 'Concursos', que dice tener como finalidad la gestión de sorteos, promociones y concursos, con razón social correspondiente a "Antena 3 de Radio, S.A.", como filial perteneciente al grupo empresarial, y adscrito a la dirección de la calle Gran Vía, 32. A esa dirección postal de Madrid tiene vinculados todos los ficheros declarados por el Grupo "Prisa" relacionados con sus emisoras de Radio[480].

Los otros ficheros inscritos por las emisoras de la Cadena SER están destinados a gestión administrativa, aunque uno de ellos, titulado 'CMD', tiene como finalidad centralizar las bases de datos del Grupo Prisa y el envío de información comercial[481].

6.3.3. "Cadena COPE".

La cadena de la "Confederación de Ondas Populares Españolas, Cope", que emite su programación desde la capital andaluza, también tiene inscritos sus ficheros con datos de carácter personal bajo dirección de la capital de España, en la calle Alfonso XI, nº 4, de Madrid.

---

480 Véase Anexo número 7 de esta Tesis.

481 Ibídem.

En total ha declarado doce ficheros de datos ante el Registro General de la Agencia Española de Protección de Datos. Al contrario que las otras, esta cadena de emisoras sí ha dedicado algunos ficheros a compendio de datos de obtenidos por la participación de ciudadanos, a través de Internet, en la página web de la empresa.

Concretamente, bajo el nombre de 'Usuarios de Internet', tiene inscrito un fichero para la gestión de los datos relativos a los usuarios de la página web de la entidad, ya sea porque introducen comentarios a noticias o porque soliciten recibir un newsletter de diario de noticias, tal y como indica exactamente en la finalidad del mismo, lo que le convierte en uno de los ficheros de Medios de Comunicación mejor adaptados a lo que requiere la normativa objeto de nuestro estudio[482].

Ha inscrito la "Cadena Cope", además, ante el Registro General de la Agencia Española de Protección de Datos un fichero con la denominación de 'Programas', para la gestión de concursos y sorteos, y participantes en los programas, grabación de emisiones y programación , así como para la fidelización de oyentes. Y otro fichero, llamado 'Contactos', para la gestión y el mantenimiento de relaciones externas de personas de contacto de la sociedad, lo que supone una gran base de datos que puede tener un uso diverso[483].

Dispone, asimismo, de un fichero dedicado a la actividad de 'Markentig Directo', cuya finalidad es el uso de los datos de los participantes en determinadas iniciativas promovidas por la empresa "Radio Popular S.A., Cadena Cope", para su utilización en envíos de comunicaciones de productos y servicios, según señala en la propia ficha[484].

Como hecho curioso, tiene declarado un fichero dedicado a la participación ciudadana, para gestionar datos de los interesados que apoyan las iniciativas de la entidad, según indica. El resto son ficheros para la gestión económica y administrativa de clientes, personal, candidatos, accionistas y consejeros de la empresa.

---

[482] Accédase al Anexo número 8 de esta Tesis.

[483] Ibídem.

[484] Ib.

6.3.4. "Cadena Onda Cero Radio".

La cadena de emisoras "Onda Cero Radio", que emite su programación desde la capital andaluza, tiene inscritos sus ficheros con datos de carácter personal vinculados a Uniprex S.A., la empresa que titulariza a esta cadena de Radio. Presentan especial interés los ficheros que declara en referencia a la empresa y a la radio, a su actividad comercial y a sus contenidos.

Tiene desarrollado esta cadena de emisoras de Radio un fichero con un registro de las direcciones IP (Internet Protocol) de quienes acceden al portal web de información en Internet, con la dirección de su sede central de la Avenida Isla Graciosa de la localidad madrileña de San Sebastián de los Reyes, como todos sus ficheros declarados[485].

Igualmente, tiene inscrito un fichero denominado 'Registro de Usuarios', con datos personales de quienes que han participado en las diferentes secciones y concursos de las webs de Uniprex, con fines estrictamente comerciales, que emplea para el envío de promociones "*que puedan resultar de su interés*", según reseña[486].

Aparece otro fichero de "Onda Cero" con el nombre 'Fondos Documentales', para gestionar los fondos documentales informativos de la emisora para los programas de Radio con contenidos informativos.

Declara, de igual modo, un fichero 'Acciones', para gestionar la participación en servicios, concursos, promociones, votaciones y juegos; así como la gestión de premios, publicidad y prospección comercial. Denomina 'Programas' a otro fichero que tiene como fin la participación en promociones y la gestión del envío de regalos y premios, según indica[487].

Los otros ficheros guardan relación más directa con la gestión administrativa y económica del personal, clientes, proveedores y servicio médico.

---

485 Remitimos al Anexo que recoge los correspondientes ficheros.

486 Ibídem.

487 Ib.

7. IMAGEN Y OTRAS COBERTURAS EN LAS TELEVISIONES.

7.1. La imagen como bien jurídico a proteger.

Como ya queda recogido en el Capítulo 3 del presente estudio, la imagen de la persona es un dato de carácter personal. Lo deja claro la propia Ley Orgánica de Protección de Datos y el Reglamento 1720/2007, pero además son numerosas las sentencias de nuestros más altos tribunales que lo argumentan y que han sido citadas en este estudio. Destaca, por significativa para esta materia, la Sentencia del Tribunal Constitucional 14/2003, de 30 de enero, que resuelve el recurso de amparo 4184/2000[488], por vulneración de derechos contra la propia imagen personal y el honor.
O la Sentencia del Tribunal Constitucional 81/2001, de 26 de marzo de 2001[489].

En su Informe Jurídico 0132/2010, la Agencia Española de Protección de Datos hace converger la libertad de información en el ámbito de la protección de datos, aludiendo a la sentencia de la Audiencia Nacional de 9 de julio de 2009, que estima un recurso interpuesto contra resolución de archivo de la Agencia, referente a la publicación por un Medio de Comunicación de imágenes relativas a una víctima de los atentados producidos en Madrid el 11 de marzo de 2004, y después de que se había considerado prevalente el derecho a la libertad de información, al concluir lo siguiente: "*La imagen, pues, es un dato que encuentra amparo en la Ley Orgánica 15/99 pero resulta que un examen detallado del expediente permite entender que, aunque las imágenes no sean de buena calidad, puede entenderse que el tratamiento del dato de la imagen ha sido excesivo tomando en consideración que no se encuentra amparado por el consentimiento de los afectados (no consta que conocieran la publicación de las imágenes) y tampoco se encuentra amparado por la libertad de información y, en todo caso, parece que se ha producido un empleo desmedido de la imagen como dato personal puesto que el carácter noticiable de la información se cumplía suficientemente sin necesidad de incluir imágenes directas de los enfermos*"[490].

---

488 B.O.E., núm. 43. Suplemento de 19/02/2003, pág. 109.

489 B.O.E., núm.104. Suplemento de 01/05/2001, pág. 50.

490 Informe Jurídico sobre libertad de información y publicación de datos, disponible en el Canal de Documentación de la Agencia Española de Protección de Datos: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdfs/2010-0132_Protecci-oo-n-de-datos-y-libertad-de-informaci-oo-n.-Publicaci-oo-n-en-un-diario-del-texto--ii-ntegro-de-sentencias.pdf>.

Desde ese razonamiento, concluye que cabe publicar en un diario el texto íntegro de las sentencias que le sean comunicadas siempre y cuando dicha publicación respete los límites y requisitos a los que se ha hecho referencia, una circunstancia que exigirá ponderar en cada caso concreto la relevancia pública e interés general de la información que se divulgue con la sentencia y el modo en que aquéllas resulten afectadas por la inclusión o no en el texto difundido de los datos de carácter personal que aquélla contenga.

De este modo, si analizada esa afectación, la publicación de los datos personales resulta necesaria para que la información mantenga el carácter noticiable y la relevancia pública a la que se refiere la doctrina emanada del Tribunal Constitucional, "*dicha publicación no resultará contraria al derecho fundamental a la protección de datos de carácter personal. En caso contrario, continúa explicando, es decir, cuando la inclusión de los datos identificativos de las personas a las que la sentencia publicada se refiere no aporten ningún valor noticiable a la información difundida, debería procederse a la previa disociación de la sentencia*", señala el citado Informe Jurídico 0132/2010[491].

Para la Agencia Española de Protección de Datos, y tal y como sostiene en el citado Informe Jurídico, "*deberá considerarse lícita la divulgación de información que contenga datos de carácter personal en los supuestos en que dicha revelación resulte adecuada pertinente y no excesiva en relación con el libre ejercicio de la libertad de información, en los términos en que la doctrina constitucional ha entendido que dicho derecho prevalece sobre el de la protección de datos. De este modo, la información a divulgar debería ser la que resulte necesaria para que informaciones que revistan la relevancia pública a la que se ha venido haciendo referencia puedan ser conocidas por los ciudadanos. Del mismo modo, cualquier información adicional que, conteniendo datos de carácter personal, resulte irrelevante para que la información facilitada tenga el carácter noticiable constitucionalmente requerido debería ser objeto de un previo procedimiento de disociación*"[492].

7.1.2. La grabación de imágenes con cámara oculta.

[491] Ibídem., pág.5.

[492] Ib., pág. 3.

La grabación de imágenes con cámara oculta trasciende la normativa sobre protección de datos, al emerger la protección de la intimidad. En sus pronunciamientos, el Tribunal Supremo ha establecido que la difusión en televisión de imágenes captadas con aparatos ocultos de captación de imagen y voz, sin consentimiento del interesado, supone una intromisión ilegítima en la esfera de la intimidad que no está justificada por el ejercicio del derecho a comunicar libremente información. Así lo ha acordado a comienzos de 2009 el pleno de la Sala de lo Civil del Supremo, al estimar un recurso de una mujer que ejercía la naturopatía y que fue grabada sin ella saberlo por una periodista que se hizo pasar por un posible paciente y las imágenes fueron emitidas en 2000 en un programa de televisión de una cadena valenciana[493].

En la sentencia dictada a comienzos de 2009, (STS 1233/2008 de 16 de enero de 2009)[494], el Supremo estima el recurso de esta ciudadana, quien fue condenada por intrusismo por la Audiencia Provincial de Valencia, contra la sentencia que absolvió por estos hechos a la periodista, a una productora y a Canal 9. La Audiencia de Valencia concluyó que el citado proceder se enmarcaba en el denominado periodismo de investigación, lo que no era reprochable, salvo que se intercepten o graben conversaciones privadas de terceras personas que no son parte en la conversación que directamente se mantiene. También señaló que no se había vulnerado el derecho a la intimidad de la mujer, ni tampoco el derecho a la imagen. Además, el tribunal valenciano consideró que no cabía responsabilidad alguna, toda vez que era indudable el ánimo puramente informativo, al haberse vertido datos ciertos y objetivos.

Sin embargo el Supremo sienta doctrina y condena a los demandados al pago de una indemnización, al señalar que, con tales comportamientos, "*se produjo una intromisión ilegítima en la esfera de la intimidad de la demandante, que afecta también a los demás derechos fundamentales mencionados en la demanda, y que, en aplicación del principio de proporcionalidad de acuerdo con las circunstancias concurrentes, no está*

493 "*El País*", 19/12/2008. Disponible en su página web: <http://elpais.com/diario/2008/12/19/sociedad/1229641203_850215.html>.

494 Sentencia 1233/2008 del Tribunal Supremo. Disponible en: <http://www.poderjudicial.es/eversuite/GetDoc?DBName=dPortal&UniqueKeyValue=71484&Download=false&ShowPath=false>.

justificada por el ejercicio del derecho a comunicar libremente información"[495].

La jurisprudencia del Tribunal Supremo, como la del Tribunal Constitucional, venía amparando el uso de la cámara oculta sólo en casos del llamado 'periodismo de investigación', siempre que la información así obtenida fuese de enorme importancia e interés público[496].

7.2. Los concursos, el envío de SMS y las llamadas.

La Agencia Española de Protección de Datos ha tenido constancia, por actuaciones previas, de que en el 'casting' de determinados concursos televisivos se recaba una serie de datos de carácter personal, lo más vinculado a la esfera de la intimidad, con información, entre otras cosas, acerca de la vida sexual de los aspirantes, al ser éste un condicionante de la forma en que se plantearán sus relaciones de convivencia durante el desarrollo de un determinado programa. Estamos refiriéndonos, obviamente, a ese formato lanzado y extendido en España a partir de finales de los años noventa, bajo el paraguas de lo denominado 'reality show', cuya producción audiovisual consiste en emitir en directo (o en diferido) todas las horas de la vida y relaciones sociales que emprenden una serie de protagonistas seleccionados mediante 'casting' elaborado 'ad hoc' por la propia productora televisiva, titularidad de Zeppelin, y que se promociona bajo el nombre de 'Gran Hermano'[497].

La información de los aspirantes a concursar es recabada de entre las propias declaraciones de los aspirantes y las impresiones o percepciones de los entrevistadores durante el proceso de selección que pueden, por ejemplo, referirse a la orientación sexual de los candidatos. En todo caso, se requiere que el titular del dato lo consienta expresamente, de acuerdo con lo previsto en el artículo 7.3 de la Ley Orgánica de Protección de

[495] Ibídem.

[496] Sentencia de la Audiencia Provincial de Madrid. Sección 21ª, de 05/06/2007.

[497] El formato fue creado por el neerlandés John de Mol y desarrollado por su productora, Endemol. Ha sido emitido en más de 70 países, reportando a Endemol importantes beneficios. El nombre del programa hace referencia a la novela que George Orwell publicó en 1949, Mil novecientos ochenta y cuatro, en la que el Gran Hermano es el líder que todo lo ve. En el programa televisivo, los participantes son grabados por cámaras las 24 horas del día.

Datos[498], sobre el consentimiento. De esta forma, debe tenerse en cuenta que tales datos no podrán ser recabados ni tratados durante el proceso de selección cuando no medie este consentimiento expreso del aspirante.

En este tipo de concursos, por otra parte, participan en ocasiones profesionales especializados que obtienen perfiles de personalidad y valoraciones psicopatológicas de los aspirantes, a través de tests específicos, los cuales, en ciertos casos, podrían constituir evaluaciones acerca de la salud mental, por lo que deberían también atenderse las garantías legalmente previstas en el citado artículo 7.3, es decir, que se obtenga previamente el consentimiento expreso de los afectados.

Es un caso referente, para nuestro estudio, el de la sanción impuesta por la Agencia Española de Protección de Datos a la empresa productora Zeppelin, realizadora del citado programa 'Gran Hermano', por incumplimiento de varios preceptos que contempla la Ley Orgánica de Protección de Datos.

La sanción, que supera el millón de euros (1.080.000 euros), fue ratificada además por el Tribunal Supremo en su sentencia de abril de 2007[499], con lo que a la empresa productora televisiva no le ha quedado más opción que tener que afrontar el pago de la sanción por no atender los derechos y obligaciones que contempla la normativa española, y que hemos visto aquí.

Al recurso de la empresa Zeppelin, que incumple, entre otros, el principio de pedir consentimiento e informar en la recogida de datos a los titulares de los mismos, aspirantes a concursantes y participantes en una serie de 'castings', el alto tribunal español se emplea con firmeza al dejar bien sentado después de que la parte recurrente cuestione que las sanciones son demasiado elevadas en función del daño producido, que "*no se aprecia una conducta que disminuya la culpabilidad y antijuridicidad de las sanciones, sino que la conducta del recurrente resulta claramente*

498 B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43090.

499 Sentencia de Tribunal Supremo, Sala 3ª, de lo Contencioso-Administrativo, de 17/04/2007. Responde al recurso de casación interpuesto por la entidad Zeppelin Televisión, S.A., contra la sentencia de 31 de enero de 2003, dictada por la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, en el recurso 534/01, en el que se impugna la resolución del Director de la Agencia de Protección de Datos de 21 de febrero de 2001, que desestima el recurso de reposición interpuesto contra la resolución de 29 de diciembre de 2000, por la que se imponen sanciones a la productora televisiva.

contraria a las exigencias legales en el tratamiento de los datos personales, con inobservancia de los requisitos elementales"[500], como explica la sentencia en su Fundamento de Derecho duodécimo.

El Tribunal Supremo zanja en su Fundamento décimo cualquier duda acerca de la cuantía de la sanción que impone a la productora dejando escrito que "*la proporcionalidad no puede cuestionarse alegando que no se ha probado que la no adopción de medidas supusiera peligro real para el bien jurídico protegido, siendo que se trata de unas medidas básicas o mínimas, y por tanto, elementales para evitar dicho peligro, señalando la Sala de instancia cómo pudo comprobar la Inspección de la Agencia Española de Protección de Datos desde un ordenador personal la publicación a través de Internet de un fichero que contenía una tabla con 1722 registros con datos de carácter personal de aspirantes al concurso de Gran Hermano*"[501].

Contraria a las alegaciones de la productora Zeppelin, la sentencia es indubitada, afirmando que "*no puede decirse que se ha vulnerado el principio de proporcionalidad, cuando la conducta observada por la entidad recurrente en la recogida de datos para la confección de un fichero sobre posibles concursantes del programa que conocemos, se ha basado en el más completo desprecio hacia la exigencia del consentimiento consciente e informado de los afectados. Exigencia de mayor intensidad cuando se refiere a los denominados 'datos sensibles', como pueden ser, de una parte, la ideología o creencias religiosas - cuya privacidad está expresamente garantizada en el art. 16.2 de la Constitución - y, por otra parte, la raza, la salud y la vida sexual*"[502].

Es lo más relevante que ha quedado establecido al final de la tensión que ha mantenido a Zeppelin con el caso Gran Hermano y a los diferentes órganos jurisdiccionales pugnando durante siete años de litigios.

Como la realidad deja entrever, Zeppelin lleva desde entonces un cuidado mucho más esmerado a la hora de tratar los datos personales, claro

---

500 Disponible en el banco de sentencias de la página web del Poder Judicial español: <http://www.poderjudicial.es/search/documento/TS/503664/proteccion%20de%20datos%20de%20caracter%20personal/20070531>.

501 Ibídem., pág. 33.

502 Ib., pág. 36.

que después de que le haya costado algo más de un millón de euros interpretar lo que establece la Ley Orgánica de Protección de Datos.

7.2.1. Los 906 ó similares.

Los problemas que se dan con los datos personales y los concursos de las cadenas de televisión que emplean servicios de llamadas a través de teléfonos 906, 902, 807 y similares, así como envíos y recepción de SMS pasan por la presencia de compañías intermediarias, especializadas en desarrollar ese tipo de concursos, y que se valen de las emisiones para recopilar datos de personas llamantes.

Una de las prácticas más recientes y que peor conjugan con la protección de datos personales es la protagonizada por la cadena televisiva Antena 3, con un juego que promovió bajo la frase *"Tu número de teléfono puede estar premiado! Solo responde SI al 25354 y puedes ser finalista de 200.000 euros hoy en Antena3!"*. Con este mensaje SMS enviado a miles de números, "Antena 3" ha estado tratando, y logrando, captar datos personales de manera indiscriminada. Pero lo hace vulnerando varios preceptos legales.

Al descomprimir la parte final del mensaje, nos viene a decir que por cada SMS se nos cobrará 1,42 euros y que el número de atención al cliente es el 902103347. Este simple mensaje que ha estado enviando "Antena 3" vulnera prácticamente todas las normativas aplicables que regulan el envío de los mensajes SMS de esta naturaleza, como sostiene en su blog Samuel Parra[503]:

- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE)[504]. Que contiene las previsiones para el envío de comunicaciones comerciales por vía electrónica, y que califica de infracción el envío de un SMS de contenido comercial sin el consentimiento del destinatario (artículo 21). Pero además, en su párrafo tercero, establece el art. 22 que "*los prestadores de servicios deberán habilitar procedimientos sencillos*

[503] Análisis realizado por S. Parra en su blog sobre casuística de Protección de Datos: < http://www.samuelparra.com/2011/01/03/25354-rico-al-instante-antena-3-normativa-contra-spam/>.

[504] B.O.E., núm. 166, de 12 /07/2002, pág. 25388.

y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado"[505]. Es decir, en el mismo SMS o en uno posterior, debería indicarse la forma en la que podemos oponernos directamente a que sigan tratando nuestro número de teléfono para estos fines comerciales, cuestión que tampoco hace Antena 3 en ese concurso. Por otra parte, el artículo 20 de la LSSI obliga a que las comunicaciones comerciales realizadas por vía electrónica tienen que ser claramente identificables como tales y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable, tal y como establece el texto legal. Establece para el caso en el que tengan lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente la obligación de incluir al comienzo del mensaje la palabra publicidad o la abreviatura '*publicidad*'[506].

- Además de la normativa general sobre el envío de comunicaciones comerciales, desde 2009 tenemos contamos con varias normas concretas que pretenden regular, para evitar los abusos existentes, el envío de los mensajes SMS de tarificación adicional (suelen tener un coste entre 1,49 euros y 7 euros). El caso de la Resolución de 8 de julio de 2009, de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, por la que se publica el código de conducta para la prestación de los servicios de tarificación adicional basados en el envío de mensajes, modificada en julio de 2010[507],que entre otras obligaciones, impone las siguientes: En el punto 5.1.2 indica que "*el operador titular del número deberá ser siempre fácilmente identificable por los usuarios, de tal forma que éste pueda ponerse en contacto con él sin dificultades. Dicho operador se identificará informando expresamente en la publicidad de, al menos, los siguientes datos: titular (nombre y apellidos completos o denominación social), número de teléfono del servicio de atención al cliente y una dirección postal y electrónica*"[508]. Obliga a que se indique, por tanto, la denominación social completa

[505] Ibídem, pág., 25394.

[506] Ib., pág. 25394.

[507] Resolución de 2 de julio de 2010, de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, por la que se publica la modificación del código de conducta para la prestación de los servicios de tarificación adicional basados en el envío de mensajes. B.O.E., núm.178, de 23/07/2010, sec. III, pág. 64647.

[508] Ibídem.

> del titular, un número de teléfono de contacto, una dirección postal y otra electrónica. En el mensaje enviado por "Antena 3" sólo se ha estado respetando lo referente al número de teléfono de contacto. En el punto 5.3.5 de la Resolución de 2009, se establece que "*en orden a ofrecer una información adecuada al usuario, la utilización de abreviaturas en la publicidad de los servicios se podrá realizar siempre que sean las comúnmente aceptadas, y se exprese de forma clara y precisa el contenido de la información mínima requerida por el presente Código para cada tipo de servicio. Cada palabra o vocablo abreviado contará al menos con tres signos alfanuméricos excluido el punto ortográfico indicativo de la abreviatura. La omisión de estas especificaciones representará un incumplimiento del Código de Conducta. Caso de utilizarse los términos o abreviaturas que a continuación se detallan, las mismas habrán de expresarse, preceptivamente, en los siguientes términos:*
> *Indicación del precio euros: € o Eur.*
> *Identificación del número de Atención al Cliente: n.º atn clte.*"[509].

Como ya hemos dejado indicado en el Capítulo 3 de este estudio, en el caso de los mensajes SMS, la Agencia Española de Protección de Datos ya constató en su inspección en las televisiones y productoras que no habían sido implantados aún procedimientos efectivos para el borrado periódico de los datos reflejados en cada envío una vez concluidas las actividades que los originan. Ha comprobado que alguna compañía especializada en estos servicios conserva en sus servidores la práctica totalidad de los mensajes recibidos desde el inicio de su actividad, lo que le reporta gran cantidad de información sobre el comportamiento de cada uno de los usuarios del servicio, identificados normalmente por su teléfono móvil.

Otra conclusión extraída por la Agencia Española de Protección de Datos sobre la actividad de estas empresas especializadas en concursos de televisión que intermedian entre las cadenas y los televidentes que participan es la ausencia de contratos entre ambas partes estipulando alguna condición sobre la protección de los datos de carácter personal. Y, si hay contrato que lo refiera, lo menos frecuente, no suele estipularse el destino de los datos personales que se recaban.

El problema principal es que la mayoría de los participantes pueden creer que están facilitando sus datos a una compañía de televisión cuando,

[509] B.O.E., núm. 180, de 27/07/2009, sec. III, pág. 63642.

en realidad, lo están recabando a través de otros servidores una serie de compañías que, a la postre, no ofrecen garantías respecto del tratamiento que se dará a los datos facilitados telefónicamente.

En su Inspección Sectorial de oficio "Concursos, juegos y sorteos de TV" , de octubre de 2002, la Agencia dicta unas recomendaciones que deberán ser observadas por todas las compañías implicadas en la producción y realización de programas de televisión, al objeto de adecuar éstas a los principios de la Ley Protección de Datos de carácter personal, y a la normativa que la desarrolla[510].

Incide, en primer término, en la información que ha de ofrecerse siempre a la hora de recoger datos personales, y conmina a que esa información debe ser facilitada con carácter previo independientemente de la vía a través de las cual se recaben datos personales, ya sea a través de líneas telefónicas, mensajes SMS, correo postal, Internet o cualquier otra, cualquiera que sea la tecnología utilizada para el almacenamiento de los datos, según destaca la Agencia Española de Protección de Datos en la citada Inspección, que recalca la necesidad de que suministrar esa información, sin importar la tipología de datos personales que se recaban, y haciéndolo de forma claramente legible.

El consentimiento voluntario del afectado es requisito lógico indispensable, como también una adecuación del empleo y uso de los datos que se recogen a las finalidades por las que se recaban, señalando para el caso de las líneas telefónicas la Inspección en su recomendación tercera, que "*no se recabarán datos personales a través de líneas 906 cuando éstos no vayan a ser utilizados para la finalidad comunicada y su recogida sólo esté motivada por cuestiones promocionales*"[511].

Las siguientes recomendaciones hacen referencia a la cancelación de datos, que serán cancelados, señala la Agencia Española de Protección de Datos, "*cuando así lo solicite el interesado*", y los datos relativos a salud y vida sexual, que "*sólo podrán ser recabados, tratados y cedidos por*

[510] Informe de la Agencia de Protección de Datos 'Inspección Sectorial de oficio 'Concursos, juegos y sorteos de TV' de octubre de 2002, op. cit., pág. 16. <https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/recomendaciones_concursos_tv.pdf>.

[511] Ibídem, pág. 17.

razones de interés general, así lo disponga una Ley o el afectado consienta expresamente"[512].

Establece, de igual modo, una recomendación en materia de seguridad que recuerda los establecido en la Ley Orgánica de Protección de Datos, considerando que "*se considera una buena práctica la adopción de medidas que eviten que la información circule por Internet de forma inteligible y, por tanto, susceptible de ser conocida o manipulada por terceros*"[513].

Las nueve recomendaciones que establece la Agencia de Protección de Datos en su 'Inspección Sectorial de oficio 'Concursos, juegos y sorteos de TV', de octubre de 2002, están relacionadas en los Anexos de esta Tesis.

7.3. La creación y declaración de ficheros de las Televisiones.

7.3.1. La "Radio Televisión de Andalucía, RTVA".

De entre los ficheros declarados e inscritos por la "RTVA" ante el Registro General de la Agencia Española de Protección de Datos, destacan los que tiene elaborados para compendiar imágenes y sonidos con los fondos documentales de la cadena regional de emisoras radio y de sus dos canales televisivos, "Canal Sur Televisión" y "Canal Sur 2 Andalucía", denominado 'Fondos documentales de Radio y Televisión', a fin de realizar programas en base a la información recogida de medios tanto propios como externos.

Tiene un fichero, titulado 'Base de Datos de Registro de Programas', con datos de las personas que presentan un proyecto en el registro para contactos posteriores, tal y como reseña en su finalidad.

Asimismo, un fichero con datos de quienes compran productos a través de Canal Sur Televisión, y otro con los datos de los socios de un programa infantil, La Banda, que se abre a la participación e inclusión de niños televidentes que se inscriben a un grupo denominado 'Club de la Banda'.

---

512 Ib., pág. 18.

513 Ib., pág. 19.

Destaca también un fichero que tiene inscrito oficialmente con los datos de los usuarios que contactan con el Defensor de la Audiencia. Los otros están directamente relacionados con la gestión económica y administrativa del personal de la empresa, y de los clientes o proveedores. De la radio sólo aparece uno declarado, el relativo a 'Clientes de publicidad'.

No falta el fichero vinculado al control de acceso a las instalaciones, con las imágenes que recepciona las cámaras de videovigilancia en los halls de entrada en las distintas sedes de la Radio Televisión de Andalucía.

El último en incorporar, con el que la "RTVA" suma catorce ficheros declarados ante el Registro General de la Agencia Española, es una base con datos de espectadores que han enviado audios y/o vídeos para participar, incluso con su imagen, en promociones impulsadas para la promoción y publicidad de la parrilla de programas de la televisión y la radio. Todos los ficheros de datos de la "RTVA" están relacionados en los Anexos de esta Tesis Doctoral.

8. LOS WEBS SITES, LAS EDICIONES DIGITALES Y LA PROTECCIÓN.

8.1. La indexación de datos personales en Internet.

La indexación o publicación de datos personales en Internet, es decir, lo que vienen haciendo desde hace algunos años los Medios de Comunicación, en especial los periódicos en sus versiones digitales, nos conduce, como trazo preliminar, a dejar constancia que la prensa digital adquiere similar objeto de aplicación de la normativa vigente al de la prensa escrita convencional, siempre que se trate de un ejercicio periodístico profesional como el de su versión de papel.

A la prensa digital, como a la prensa escrita, es de aplicación, por tanto, la LOPD y, además, la Ley 14/1966 de Prensa e Imprenta[514] por su art. 65, que estableció responsabilidad civil solidaria de "*autores, directores, editores, impresores e importadores o distribuidores de impresos extranjeros*"[515] por los daños producidos como consecuencia de las actividades de los medios informativos, un precepto cuya vigencia ha planteado dudas pero que sigue siendo de aplicación, como sostienen Grimalt Servera y Cavanillas Múgica, así como la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), "*siempre que no actúe como 'mero intermediario en la sociedad de la información', en lo relativo al régimen de responsabilidad de los intermediarios de información en medios electrónicos*"[516].

Asentada la vigencia de las dos leyes citadas, ha de remarcarse la prevalencia de las libertades y derechos del art 20 de la Constitución sobre otros derechos, como el de la protección de datos, tal y como ha señalado la Agencia Española de Protección de Datos en pronunciamientos aquí referidos, (los casos de reclamaciones contra las versiones digitales de ABC de Sevilla y La Vanguardia, ambas de mayo de 2010[517]) al explicar

514 B.O.E., núm. 67, de 19 /03/1966, pág. 3310.

515 Ibídem., pág. 3314.

516 GRIMALT SERVERA, Pedro; CAVANILLAS MÚGICA, Santiago y otros.: '*Responsabilidades de los proveedores de información en Internet*'. Comares, Granada, 2007, pág. 41.

517 Resolución 00962/2010 de la Agencia Española de Protección de Datos, del procedimiento TD/00030/2010, de mayo de 2010. Publicada en el canal de su web

que, si bien la publicación de una noticia en prensa se encuentra amparada por el citado artículo de la CE, que consagra las libertades de opinión e información, y que el derecho a 'recibir libremente información veraz por cualquier medio de difusión' prevalece frente a otros derechos constitucionales, no cabe duda de que el desarrollo de Internet y la implantación generalizada de los motores de búsqueda "*suponen una divulgación exponencial y permanente de los datos personales incluidos en la información de prensa, y que deberían por ello los Medios de Comunicación reflexionar sobre la trascendencia que tiene mantener de manera permanente una absoluta accesibilidad de los datos contenidos en noticias cuya relevancia informativa probablemente es inexistente en la actualidad. Y tener en cuenta la trascendencia sobre la privacidad de las personas que puede derivar de ello*"[518].

Ello plantea, según la Agencia, la conveniencia de que, en el caso de que concurra un interés legítimo de un particular y manteniendo la información inalterable en su soporte, dado que no se borraría de sus archivos ni de sus históricos, desde la webmaster se evite la indexación de la noticia por los motores de búsqueda en Internet, lo que limitaría su divulgación indiscriminada, permanente y, en su caso, lesiva. Una cuestión, la de que los datos personales figuren y permanezcan en la memoria caché de Google, que no está amparada por la libertad de información, acota la Agencia Española de Protección de Datos en el citado pronunciamiento de mayo de 2010[519].

Ahora bien, una cuestión es lo relativo a la publicación de datos personales por los periódicos en sus versiones digitales, y otra cuestión más problemática es la indexación de esos datos por los buscadores de Internet, que pueden llegar a dejarlos en su memoria 'caché' de manera indefinida en el tiempo y sin limitaciones para el acceso a los mismos. El problema lo causan portales y buscadores como Google, Yahoo, Netscape o Terra, que se asemejan cada vez más a un periódico e insertan noticias e incluso 'últimas horas' proporcionadas por agencias de noticias o periódicos digitales.

---

dedicado a resoluciones sobre defensa y tutela de derechos, en: <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-00030-2010_Resolucion-de-fecha-24-05-2010_Art-ii-culo-16-LOPD_Recurrida.pdf>.

[518] Ibídem, pág., 24.

[519] Ib., pág. 25.

Estamos ante lo que algunos autores asocian a una convergencia de medios de comunicación y servicios de la Sociedad de la Información. Ello tiene un sentido doble, según Cavanillas Múgica: de un lado, "*los tradicionales Medios de Comunicación se transforman y son objeto de un 'mestizaje', alejándose (en el caso de los periódicos) de los parámetros con los que actúan en las ediciones de papel y, de otro lado, dejan de ostentar el monopolio de la provisión de información, que ahora deben compartir con empresas tecnológicas cada vez menos dispuestas a limitarse a su papel mediador o facilitador de información y datos*"[520].

Siguiendo a Cavanillas Múgica, convergen no sólo los aparatos, sino también los servicios, como se comprueba llevando a cabo una mirada a las noticias económicas de los últimos tiempos. Puede detectarse una incesante emergencia de fusiones o acuerdos entre empresas del sector de las telecomunicaciones, de la producción audiovisual y de los Medios de Comunicación. En segundo término, la navegación habitual por Internet ofrece un panorama claro sobre la manera en que los tradicionales Medios de Comunicación, sobre todo los periódicos, "*adoptan en Internet diseños y contenidos más 'convergentes'. Pasados los primeros tiempos en los que los periódicos electrónicos constituían un calco o un resumen de las versiones en papel, se observa luego una tendencia a un distanciamiento creciente; las versiones digitales tienden a convertirse en portales que combinan los contenidos propios del periódicos con utilidades interactivas, como buscadores, directorios, foros, tienda electrónica, etc*"[521].

Los periódicos han llegado a incorporar en sus versiones digitales variados recursos propios de las nuevas comunicaciones electrónicas, que le permiten ampliar el espectro de su oferta informativa: bitácoras o blogs, enmarcado (framing) y enlaces directos (inline links), franjas de noticias o tickers, banners publicitarios, etc.

8.1.1. Bitácoras o blogs.

Los blogs se traducen, normalmente, al castellano como 'cuaderno de bitácora', 'bitácoras' o 'ciberbitácoras', suponen una combinación de una página web personal y un foro. Como página web, es mantenida por un editor o autor principal, llamado habitualmente blogger, que introduce

[520] CAVANILLAS MÚGICA, S. en AA.VV.: op. cit., pág. 3.

[521] Ibídem., pág. 2.

entradas con texto, fotografías, enlaces, etc., de acuerdo con un orden cronológico inverso, por lo que las entradas más recientes aparecen en la parte superior de la página. Al ofrecerse como foro, deja la posibilidad a terceros de introducir mensajes referidos a algunas de las mencionadas entradas y, a su vez, esos mensajes, pueden dar lugar a nuevos mensajes. Lo habitual es que el editor y/o autor (blogger) tenga capacidad técnica para borrar uno o todos los mensajes recibidos.

Los blogs pueden incorporar otros servicios, como la indexación automática de las entradas o mensajes visualizados, el archivo histórico de las entradas ya retiradas, etc. Los blogs pueden formar parte de un Medio de Comunicación y pueden ser mantenidos por periodistas (por ejemplo, el blog 'EP3' del periódico "El País", en http://blogs.ep3.es/), o pueden ser realizados por particulares, sin que ello obste a que se produzca 'actividad económica', matiz significativo para que le sea de aplicación la LSSI, sea mediante recuadros publicitarios (banners), ventas o donaciones.

Estamos, pues, según S. Cavanillas, ante "*un servicio mixto o híbrido, en el que la provisión de información (entradas principales introducidas por el autor/editor del blog) se combina con una prestación de alojamiento*" (recepción y publicación de mensajes y comentarios de terceros)[522].

Para P. Grimalt, los blogs vinculados a periódicos digitales son aquellos cuyo autor/editor es colaborador, habitual o no, de ese periódico, dándose entonces varias situaciones[523]: en la primera, el blog se integra en ese periódico digital, no se trata de una página web del colaborador, sino que es una parte más del periódico digital, en cuyo caso, no caben dudas sobre la aplicación del art 65 de la Ley de Prensa y los preceptos de la Ley Orgánica de Protección de Datos (LOPD) al editor del periódico y, a tenor de la jurisprudencia, también al director. En la segunda, el blog es una web creada por el propio autor al margen del periódico digital del que es colaborador. Al no existir, en este caso, relación entre blog y periódico digital no será de aplicación al Medio el art 65 de la Ley de Prensa, ni la LOPD, pues no hay ni control ni beneficio por parte de la editora del periódico digital, ni tampoco del director. Hay una tercera situación, según P. Grimalt[524], cuando el periódico digital dispone de un enlace hacia el blog

522 Ib., pág. 4.

523 GRIMALT SERVERA, P.: op.cit., pág. 78.

524 Ib., pág. 79.

del colaborador pero con la peculiaridad de que la bitácora no está en la estructura digital del periódico, sino que es una página web independiente. Con lo que habría que ver si el blog aparece con un enlace individualizado o no, siendo el primer caso el que lleva al periódico digital a verse sometido a la aplicación del régimen de responsabilidad civil y administrativa.

Los pronunciamientos de la Agencia Española de Protección de Datos han ido produciéndose siempre, en aras de la tutela de derechos, a favor del ciudadano que reclama contra el propietario del blog para la cancelación en el mismo de sus datos personales. Así, las Resoluciones R/01434/2010, sobre datos en blog propiedad de un buscador[525]; la R/00937/2010, sobre datos en blog cuyo propietario, Google, no los cancela[526]; la R/01509/2010, en el mismo sentido[527]; o la R/00954/2008 sobre cancelación de datos en un blog sindical[528].

A mediados de los años 90 se remonta su tecnología, aunque el uso de blogs fue generalizándose hasta explotar a inicios del siglo XXI. Se ha cifrado la existencia de decenas de millones el número de bitácoras disponibles en Internet.

8.1.2. Los foros de la prensa digital.

[525] Véase:
<http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-00242-2010_Resolucion-de-fecha-02-07-2010_Art-ii-culo-16-LOPD_Recurrida.pdf>.

[526] Véase:
<http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-00021-2010_Resolucion-de-fecha-24-05-2010_Art-ii-culo-16-LOPD.pdf>.

[527] Véase:
<http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-00412-2010_Resolucion-de-fecha-16-07-2010_Art-ii-culo-16-LOPD.pdf>.

[528] Véase:
<http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2008/common/pdfs/TD-00212-2008_Resolucion-de-fecha-22-07-2008_Art-ii-culo-16-LOPD.pdf>.

En los foros de la prensa digital, sus lectores internautas pueden expresar sus opiniones en tiempo real. Se trata de un espacio puesto a disposición de los lectores digitales para que, como actividad legítima, puedan ejercer su libertad de expresión o de información, limitándose el periódico a ser, sostiene P. Grimalt, "*un mero medio de transmisión de la opinión de sus lectores*"[529], por lo que no responde de los posibles daños al honor o a la intimidad de terceros, ni tampoco por la violación de datos personales, causados por la intervención de los lectores digitales en el foro, siempre, eso sí, que el periódico tenga identificados a los lectores digitales que participen, pues en caso contrario, debemos concluir que el Medio de Comunicación hace suyas estas intervenciones y, por tanto, debe responder a la violación del derecho a la protección de datos y las lesiones al honor o intimidad de terceros que puedan darse. En todo caso, "*el periódico digital actúa como mero intermediario de la sociedad de la información*"[530] y no queda fuera del ámbito de aplicación de la LSSICE (arts. 16 ó 17).

Sobre cancelación de datos en un foro, la Resolución R/00473/2009 de la Agencia Española de Protección de Datos, de marzo de 2009, tras denuncia formulada por un ciudadano contra una web[531].

8.1.3. Enmarcado (framing) y enlaces directos (inline links).

La página web de un periódico, como cualquier otra, puede dividirse en distintos marcos o frames. Cualquier enlace puede definirse, a su vez, para que su contenido se haga presente en una nueva página o en el seno de uno de los marcos de la página de origen. De esta manera, la combinación de las posibilidades de enlazar y enmarcar en páginas web permite sumar o embeber la información ajena que viene enlazada, de forma que esos contenidos ajenos puedan aparecer bajo el diseño de la página de origen y combinados con los restantes contenidos que se incluyan, como explica S. Cavanillas en su preliminar acerca de la responsabilidad de los proveedores de información en Internet[532].

---

529 GRIMALT SERVERA, P.: op.cit., pág. 80.

530 Ibídem, pág. 81.

531 Véase: <https://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2009/common/pdfs/TD-01521-2008_Resolucion-de-fecha-05-03-2009_Art-ii-culo-16-LOPD.pdf>.

532 CAVANILLAS MÚGICA, S. en AA. VV.: op. cit., pág. 4.

Una página web puede programarse también para que, al descargarse, incorpore automáticamente contenidos ajenos mediante la inclusión, en el código fuente de la página, de un enlace directo (inline link) que hace 'una llamada' e incorpora los contenidos ajenos sin que el proceso sea visible para el usuario. Se produce así una imbricación total entre la página principal o básica y los contenidos añadidos, pues el enlace directo hace imperceptible 'la llamada' al servidor ajeno.

Las más frecuentes utilidades de ambas técnicas (enmarcado y enlace directo) suelen resultar ser los tickers o franja de noticias y los 'banners' o recuadros publicitarios.

8.1.4. Franjas de noticias o news tickers.

Los news tickers son pequeñas franjas de información que aparecen en la pantalla de televisión, por ejemplo en algunos informativos televisivos matinales, o en algunas páginas webs, generalmente de periódicos digitales. En estas pequeñas franjas se van dando informaciones muy escuetas, a veces resumidas en una frase, o enlazando con otras direcciones webs, y que se van renovando constantemente[533].

Estas franjas informativas sí están controladas por el propio Medio de Comunicación que las emite, no plantean problema alguno desde la perspectiva de la Ley de Prensa, pues se trataría de una 'sección informativa' más del medio informativo y cuya responsabilidad no diferirá de los aquí señalado.

Sin embargo, y en opinión de P. Grimalt, mayores problemas presentan los news tickers controlados por personas ajenas al Medio de Comunicación, que se da en aquellos casos en que el máximo responsable del periódico (el director) ha dado su permiso para que un tercero informe a través de los news tickers, lo que da lugar a dos posibilidades: de un lado,

---

[533] Un teletipo de noticias (a veces referido como un "rastreador" o "slide") reside en el tercio inferior del espacio de la pantalla de televisión en las cadenas de noticias de televisión dedicados a presentar a los titulares o piezas pequeñas de noticias. Dado que el crecimiento en el uso de la World Wide Web, tickers de noticias han sindicado en gran medida los mensajes de noticias de los sitios web de los servicios de radiodifusión que producen las emisiones, según define news-ticker wikipedia.

equiparar esta actividad con las 'cartas al director' (recordar el pronunciamiento de la Agencia Española de Protección de Datos emitido mediante la Resolución TD/01161/2008[534], que ve la reclamación formulada por un ciudadano contra un periódico asturiano), pues son secciones en las que personas ajenas al Medio ejercen su libertad de expresión, con lo que el deber del periódico está en tener bien identificado al responsable del new ticker e impedir si la información u opinión que transmite viola los derechos a la protección de datos personales o invade u ofende la intimidad de personas sin visos de que pueda estar amparada por la libertad de información[535].

De otro lado, analizar "*el binomio negocio-riesgo*", según P. Grimalt, ante la posibilidad cierta de que el periódico, a fin de obtener un beneficio económico, cede una franja para que un tercero pueda emitir sus noticias, por lo que debe asumir el riesgo de eventuales lesiones a los derechos del art.18 de la Constitución que ostenta todo tercero. Tanto la cadena de televisión como el periódico digital, deberán asumir en todo momento una actitud de '*in vigilando*' para que, en cualquier caso, no se ataquen en sus espacios de información en línea los derechos de las personas[536].

Los newsletters o boletines informativos conforman otra de las nuevas formas de lanzamiento de noticias que emplean desde hace pocos años los Medios de Comunicación. Queden aquí reflejados ese conjunto de noticias, a modo de selección, que se envían por correo electrónico a los suscriptores de periódicos digitales. En esos newsletters pueden aparecer resúmenes de prensa, artículos, enlaces a páginas webs que conducen a más amplia información, etc. Las responsabilidades civiles (las contempladas por nuestro Código Civil) y administrativas (las de la Ley Orgánica de Protección de Datos) por el contenido de los mismos, son perfectamente equiparables a lo reflejado anteriormente y extensibles, por tanto, al autor, editor y, en su caso, al director del Medio de Comunicación.

---

534 Véase:
<http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2009/common/pdfs/TD-01161-2008_Resolucion-de-fecha-13-01-2009_Art-ii-culo-16-LOPD.pdf>.

535 GRIMALT SERVERA, P.: op.cit., pág. 76.

536 Ibídem, pág., 77.

8.1.5. Banners publicitarios.

Describe S. Cavanillas que los banners o recuadros publicitarios funcionan de manera muy parecida a los tickers, la diferencia más significativa es que en la selección de la información a introducir en el correspondiente recuadro es realizada por el servidor de la empresa publicitaria o anunciante de acuerdo con algunos algoritmos estadísticos o aleatorios, aunque se caracterizan por la finalidad. El objetivo de los banners "*consiste en introducir en ciertas páginas webs información publicitaria que no se encuentra en el servidor que aloja dichas páginas*"[537].

Esa misma tecnología de los enlaces directos sirve para otras dos formas de inserción publicitaria en Internet: las páginas emergentes, o pops-ups, y las páginas intersticiales. Sostiene Cavanillas que "*en ambos casos, la orden de descarga procede de la propia página visitada, y el contenido publicitario es proveído por la propia empresa anunciante o publicitaria*"[538].

Relacionadas, por tanto, las citadas definiciones, y dejada sentada la aplicación de la normativa civil (Código Civil) y administrativa (LOPD) a los autores y editores, constituye todo ello campo de acción para que se aplique la LSSI, al estar ante 'servicio de la sociedad de la información', a la puesta a disposición de bases de datos mediante tecnología web, las páginas emergentes (pop-ups), los recuadros publicitarios (banners), las franjas de noticias (tickers), los newsletters, los foros, los blogs, los archivos multimedia de audio, de videos o de texto que sean descargables, los mensajes cortos de texto (sms) o mensajes multimedia (mms), etc.

8.2. Hemeroteca de periódicos digitales y buscadores.

El problema surge no ya sólo por la publicación e indexación da datos en Internet por parte de los Medios de Comunicación en sus versiones digitales, sino en la conservación de los mismos en la Red. Un problema que se ve acrecentado por la actividad de los buscadores que, en su acción de '*rastreo*' y búsqueda de datos, dejan indexada gran cantidad

[537] CAVANILLAS MÚGICA, S. en AA.VV.: op. cit., pág. 6.

[538] Ibídem, pág., 6.

de información, permitiendo seguir la huella de miles, millones, de datos personales.

La Agencia Española de Protección de Datos compila sus criterios al respecto en la Resolución Nº R/00898/2010[539], emitida en mayo de ese año tras la reclamación formulada por un ciudadano contra Google Spain, S.L. y contra el periódico "La Vanguardia, S. L.", con sede en Barcelona, por no haber sido debidamente atendido su derecho de oposición al tratamiento de sus datos personales, referidos en la publicación de un artículo en el sitio web <hemeroteca.lavanguardia.es>, de fecha 14 de julio de 1989, y que permanecían accesibles a cualquiera en Internet.

En esta Resolución, al igual que en el caso protagonizado por "Abc" de Sevilla visto en el Capítulo dedicado a los datos en la Prensa escrita, la Agencia Española también estima el derecho del reclamante frente a Google Spain, y concede la razón al periódico "La Vanguardia", pero matizando que, si bien la publicación de una noticia en prensa se encuentra amparada por el artículo 20 de la Constitución Española, que consagra las libertades de opinión e información, y que el derecho a "*recibir libremente información veraz por cualquier medio de difusión*" prevalece frente otros derechos constitucionales, no cabe duda de que el desarrollo de Internet y la implantación generalizada de los motores de búsqueda suponen una divulgación exponencial y permanente de los datos personales incluidos en la información de prensa. Ello plantea, señala la Agencia Española de Protección de Datos, "*la conveniencia de que en el caso de que concurra un interés legítimo de un particular y manteniendo la información inalterable en su soporte, dado que no se borraría de sus archivos ni de sus históricos, desde la webmaster se evite la indexación de la noticia por los motores de búsqueda en Internet, lo que limitaría su divulgación indiscriminada, permanente y, en su caso, lesiva*"[540]. Argumentación similar a la del caso de "Abc" de Sevilla, aunque se extiende en su Resolución sobre la hemeroteca digital de "La Vanguardia" al explicar por qué el buscador Google no cumple con la normativa de protección de datos personales.

---

539 Procedimiento Nº: TD/01887/2009.
<http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-01887-2009_Resolucion-de-fecha-24-05-2010_Art-ii-culo-6.4-LOPD_Recurrida.pdf>.

540 Ibídem, pág. 24.

Alega en su defensa la compañía Google Spain[541] "*que su empresa no es ni responsable, ni encargada de la prestación del servicio de búsquedas en Internet*". Se basa en que Google Spain dice limitarse a representar a 'GOOGLE INC' en el negocio que ésta desarrolla de vender el espacio publicitario disponible en su página web. Agrega en sus alegaciones que 'GOOGLE INC' es la única compañía de quien, en su caso, se podría exigir la eventual atención de cualesquiera derechos, quejas o sugerencias de las personas en relación con los servicios que presta esta compañía. En cuanto a la normativa aplicable, alega que a los servicios de buscador que presta 'GOOGLE INC' desde los Estados Unidos, no resulta de aplicación ni la directiva europea de protección de datos ni la ley española que la aplica.

Pero la Agencia Española de Protección de Datos rechaza el intento de Google de hacer una huída de nuestra normativa, y refuta todas las alegaciones del conocido buscador. En esta importante Resolución Nº R/00898/2010, invoca el artículo 3 del Reglamento aprobado por Real Decreto 1720/2008, que traspone el artículo 4 de la Directiva 95/46/CE, relativo al 'Derecho nacional aplicable', y remarca, en especial, el art 1, c) de la norma comunitaria: "*el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio d de la Comunidad Europea*". Recuerda también los Considerandos 18, 19 y 20 de la Directiva 95/46 CE[542] para evidenciar que Google Spain no escapa del ámbito de

---

[541] Ib., pág. 2.

[542] Diario Oficial de la Unión Europea. N° L 281, de 23/11/1995, pág. 33.

El Considerando 18 expresa que "*para evitar que una persona sea excluida de la protección garantizada por la presente Directiva, es necesario que todo tratamiento de datos personales efectuado en la Comunidad respete la legislación de uno de sus Estados miembros; que, a este respecto, resulta conveniente someter el tratamiento de datos efectuados por cualquier persona que actúe bajo la autoridad del responsable del tratamiento establecido en un Estado miembro a la aplicación de la legislación de tal Estado*".

El Considerando 19 indica que "*el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos*

aplicación de la normativa europea y española en materia de protección de datos personales.

Respecto a si un buscador como Google es responsable de tratamiento de datos, la Agencia Española de Protección de Datos se basa en lo establecido por el Grupo de Trabajo "G 29", en el documento WP 148, de 4 abril de 2008[543], relativo a motores de búsqueda, para hacer constar que un proveedor de buscadores que trata datos de los usuarios incluyendo direcciones IP y/o cookies permanentes que contengan un identificador único se encuentra dentro de la definición de responsable de tratamiento, puesto que determina de forma efectiva las finalidades y los medios del tratamiento. Ello, a pesar de las dificultades que ocasiona la naturaleza multinacional de los grandes proveedores de servicios de búsqueda, que con frecuencia disponen de oficinas principales ubicadas fuera del territorio comunitario, con servicios prestados en todo el mundo, y con la implicación de distintas sucursales y posiblemente de terceros en el tratamiento de los datos personales.

Describe la Agencia Española de Protección de Datos el servicio de búsqueda de Google (Google Search)[544], para reflejar que se presta a nivel mundial a través del sitio web <www.google.com>, aunque en muchos países existen versiones locales adaptadas al idioma nacional, a las cuales se accede por defecto, en función de la ubicación geográfica del usuario. La versión española del servicio se presta a través del sitio www.google.es.

---

cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades"

El Considerando 20 dice que "*el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adaptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva"*.

[543] En: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_es.pdf>.

[544] Google Search Appliance es un sistema de búsqueda universal que permite a las organizaciones incorporar información procedente de una variedad de fuentes externas e internas (incluyendo sistemas de archivos, intranets, bases de datos, aplicaciones, servicios alojados y sistemas de gestión de contenidos). El software es producido por Google y el hardware, fabricado por Dell Computers y se basa en la Dell PowerEdge R710, según la definición que ofrece la enciclopedia electrónica wikipedia. Véase: <http://es.wikipedia.org/wiki/Google_Search_Appliance>.

El motor de búsqueda de Google es un complejo sistema informático que indexa documentos almacenados en millones de servidores de páginas web (más comúnmente conocidos como servidores web), facilitando al usuario del servicio de búsqueda su inmediata localización, a través de determinadas palabras contenidas en los documentos buscados. El índice del motor de búsqueda de Google se actualiza de forma dinámica a partir de la información obtenida por robots, que continuamente rastrean los servidores web públicamente disponibles en Internet, utilizando para ello la capacidad tecnológica de los propios servidores de la compañía, usualmente conocidos como "arañas web" o "web crawlers"[545].

Las "arañas web" analizan de forma metódica páginas web HTML disponibles públicamente, recopilando los hiperenlaces que figuran en éstas (referencias a otras direcciones URL), para extender así su labor de rastreo, de forma encadenada, a todas las páginas y documentos referenciados. El rastreo consiste en extraer, de todos los documentos visitados (no sólo de las páginas con formato HTML, sino también de los documentos que presentan otros formatos), las palabras clave que serán indexadas. Para que la información que ofrece el buscador Google sea lo más universal y completa posible, la labor de rastreo de sus "arañas web" se extiende a las páginas web que se almacenan en servidores informáticos ubicados en todo el mundo.

En su Resolución[546], la Agencia hace hincapié, en particular, en que los servidores web ubicados en territorio español son expresamente visitados para extraer la información que, en una alta proporción, dará respuesta a las búsquedas de usuarios españoles, para acotar que "*la información rastreada expresamente por Google en los servidores*

[545] Una araña web (o araña de la web) es un programa que inspecciona las páginas del World Wide Web de forma metódica y automatizada. Uno de los usos más frecuentes que se les da consiste en crear una copia de todas las páginas web visitadas para su procesado posterior por un motor de búsqueda que indexa las páginas proporcionando un sistema de búsquedas rápido. Las arañas web suelen ser bots (el tipo más usado de éstos). Entre las tareas más comunes de las arañas de la web: Crear el índice de una máquina de búsqueda; analizar los enlaces de un sitio para buscar links rotos, y recolectar información de un cierto tipo, como precios de productos para recopilar un catálogo, según wikipedia. Véase: <http://es.wikipedia.org/wiki/Ara%C3%B1a_web>.

[546] Procedimiento Nº: TD/01887/2009, op., cit., pág. 12. <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-01887-2009_Resolucion-de-fecha-24-05-2010_Art-ii-culo-6.4-LOPD_Recurrida.pdf>.

ubicados en territorio español incluye datos de carácter personal relativos a personas que no necesariamente son usuarios del buscador y que, al margen de los derechos que debe reconocerse a éstos, también se hallan en disposición de ejercitar sus propios derechos, en relación con los distintos tratamientos que de sus datos realiza Google. Así, conviene centrarse no sólo en el tratamiento realizado por Google consistente en presentar datos al usuario que realiza la búsqueda, sino también en el que previamente efectúa, al rastrear tales datos de carácter personal en los citados servidores españoles, con objeto de facilitar su posterior localización".

Por otra parte, una de las facilidades que la versión española del servicio de1 buscador ofrece al usuario es, precisamente, discriminar el resultado de su búsqueda en función del idioma de redacción de los documentos o de la localización geográfica de los servidores web que los alojan. Así, el usuario puede decidir que los resultados de su búsqueda se refieran a "*páginas de España*", sin más que indicarlo en la página principal del buscador, o bien, haciendo uso de la funcionalidad "*búsqueda avanzada*", directamente accesible desde la página principal, el usuario puede seleccionar sólo aquellas páginas que estén "*ubicadas en España*". En ambos casos, explica la Resolución de la Agencia Española de Protección de Datos, "*resulta imprescindible que Google haya visitado con anterioridad las páginas ubicadas en servidores web españoles y registrado esta circunstancia durante la labor de rastreo realizada por sus "arañas web", de forma tal que si estos servidores no hubieran sido rastreados previamente, el resultado de la búsqueda se vería seriamente limitado para los usuarios españoles*"[547].

Todo ello, según la Agencia, viene a demostrar que, para la prestación del servicio de búsqueda a los usuarios españoles, es requisito ineludible que se utilicen medios técnicos ubicados en territorio español, siendo plenamente consciente de ello la compañía prestataria del servicio. El servicio de búsqueda prestado a través del sitio web www.google.es, es un servicio dirigido específicamente al territorio español. La afirmación de que el servicio de búsqueda está dirigido específicamente al territorio español se basa en los siguientes hechos: El lenguaje de la página www.google.es está redactada en castellano, (también da la posibilidad de catalán, euskera y gallego); el dominio bajo el que se aloja el servicio de buscador Google en España es del tipo .es, que es un dominio territorial registrado en Red.es "*bajo el código de país correspondiente a España*" (Disposición adicional 6ª de la Ley 34/2002 de 11 de julio, de Servicios de

[547] Ibídem, pág. 13.

la Sociedad de la Información y de Comercio Electrónico)[548]; cuando se realizan búsquedas en www.google.es, los resultados que aparecen están dirigidos a usuarios ubicados en el territorio español.

Agrega entre sus argumentaciones del pronunciamiento de la Agencia Española de Protección de Datos que la publicidad es la forma de financiación del buscador gratuito de Google, hasta tal punto, que el usuario no puede evitarla si quiere utilizar este servicio. Tal y como establecen sus condiciones de uso "Google llevará a cabo el tratamiento de los datos personales únicamente de conformidad con lo dispuesto en la presente Política de Privacidad o en las notificaciones adicionales que se incluyan en determinados servicios.

No sólo es la normativa específica de protección de datos la que, con arreglo a los argumentos anteriores, determina la Ley aplicable al caso protagonizado por el buscador Google, sino que dicha normativa resultaría en todo caso aplicable por determinación del tenor literal del art. 4 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. Y, en atención a la actividad de los buscadores de Internet, su art.17, sobre 'responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda', que dispone lo siguiente: "*1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que: a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o, b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente*"[549].

La Resolución de la Agencia concluye así que "*los datos personales que obtiene Google afectan a la dignidad de la persona y pueden lesionar derechos de un tercero, por lo que el Director de la Agencia Española de Protección de Datos como órgano competente para velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, atendiendo a la reclamación formulada por el reclamante*",

[548] B.O.E., núm. 166, de 12/07/2002, op. cit., pág. 25399.

[549] Ibídem, pág. 25393.

requiere al responsable del tratamiento (Google Spain SL) la adopción de medidas[550].

Establece, en esta trascendente Resolución que resuelve el caso de datos de la hemeroteca del periódico La Vanguardia que es necesario insistir en los efectos divulgativos multiplicadores que se producen a través de Internet y, en mayor medida de los buscadores y su repercusión en la protección de datos de las personas, especialmente sin trascendencia pública. Por todo ello, "*cabe proclamar que ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la RED sin poder reaccionar ni corregir la inclusión ilegítima de los mismos en un sistema de comunicación universal como Internet. Si requerir el consentimiento individualizado de los ciudadanos para incluir sus datos personales en Internet o exigir mecanismos técnicos que impidieran o filtraran la incorporación no consentida de datos personales podría suponer una insoportable barrera al libre ejercicio de las libertades de expresión e información a modo de censura previa (lo que resulta constitucionalmente proscrito), no es menos cierto que resulta palmariamente legítimo que el ciudadano que no esté obligado a someterse a la disciplina del ejercicio de las referidas libertades (por no resultar sus datos personales de interés público ni contribuir, en consecuencia, su conocimiento a forjar una opinión pública libre como pilar básico del Estado democrático) debe gozar de mecanismos reactivos amparados en Derecho (como el derecho de cancelación de datos de carácter personal) que impidan el mantenimiento secular y universal en la Red de su información de carácter personal*"[551].

8.3. Movimiento internacional de datos.

Los intentos de compañías como Google, entre otras, de intentar eludir las normas españoles y comunitarias nos llevan a mirar las reglas esenciales que rigen para el movimiento internacional de datos, ya sea cesión, o constituya transferencia de datos, y que se encuentran en los artículos 33 y 34 de la Ley Orgánica de Protección de Datos, respaldados por la Instrucción 1/2000[552] dictada por la Agencia Española de Protección

[550] Procedimiento Nº: TD/01887/2009, op., cit., pág. 19.

[551] Ib., pág. 20.

[552] B.O.E., núm. 301, de 16/12/2000, pág. 44253.

de Datos para regular este tipo de situaciones. El principio general contemplado en la Ley es la prohibición de efectuar transferencias de datos de carácter personal, sean temporales o definitivos, a países que no presenten un nivel equiparable de protección al que otorga nuestra norma.

Sólo cabrá excepción a esta regla general prohibitiva cuando se obtenga autorización administrativa previa del Director de la Agencia Española de Protección de Datos. Éste ostenta la facultad de suspender la transferencia internacional si las autoridades de la protección de datos del Estado destinatario resuelven que quien recibe los datos ha vulnerado las normas de su derecho interno, o si hay indicios de que se están vulnerando las normas o principios de la protección de datos personales por parte del destinatario de la transferencia y las autoridades competentes del Estado no asumen la evitación del riesgo. Cabe también la posibilidad de que el responsable del tratamiento se acoja a algunos de los once supuestos de excepción del art. 34 de la Ley Orgánica de Protección de Datos (LOPD)[553].

Hay que delimitar si estamos ante una cesión de datos o ante una transferencia internacional de datos.

En cuanto a las cesiones de datos a países que ofrecen un equiparable nivel de protección, lo que contempla el sentido de los artículos 33 y 34 de la LOPD, desarrollado por la Instrucción 1/2000 de la Agencia, sólo es aplicable a transferencias internacionales de datos en su justa acción, es decir, no abarca lo que antes ha ocurrido con el responsable del fichero que trasmite y el responsable del fichero que recibe.

Del citado art. 33 de la LOPD[554] se desprende que las transferencias internacionales de datos con destino a países que proporcionan un nivel de protección equiparable al que concibe nuestra normativa son aceptadas. No requerirán esa autorización del Director de la Agencia al ofrecer el país de destino las garantías adecuadas a la protección no sólo de los datos de carácter personal sino de los derechos y libertades de los individuos en general.

---

553 B.O.E., núm. 298, de 14/12/1999, pág. 43095.

554 Ibídem, pág., 43094.

La decisión sobre qué país tiene nivel de protección adecuado corresponde a la Comisión Europea, como dice la Instrucción 1/2000 en su artículo II[555]. La LOPD atribuye esa capacidad a la Agencia Española de Protección de Datos aunque la primacía la ostenta la Comisión Europea cuyas decisiones imperarán en nuestro ordenamiento.

Para estar al tanto de las actualizaciones de la lista de países con nivel adecuado de protección de los datos personales, la Comisión Europea ofrece información puntual al respecto en su página web[556].

El hecho de que se reconozca un nivel de protección adecuado para los datos personales no quiere decir que se extienda a todos los sectores. Esa protección puede hacer referencia sólo a determinados sectores. Es el caso de EE.UU. cuyo nivel de protección n o es tan alto como el de Europa pero que sin embargo ha alcanzado unos acuerdos, denominados '*Acuerdos de Puerto Seguro*'[557] por los que se permite una libre circulación de los datos de carácter personal entre empresas europeas y las empresas estadounidenses que se hayan adherido a los mismos[558].

8.4. Dictamen europeo sobre buscadores en Internet y protección de datos.

Los especialistas comunitarios han querido aclarar el problema de los buscadores de Internet, las páginas web y la protección de datos, y el Grupo de Trabajo del art.29 emitió el Dictamen WP 148 sobre cuestiones de protección de datos en relación con buscadores, antes citado.

El Dictamen 1/2008[559] define a los buscadores como un tipo de servicio de la sociedad de la información, e indica que tratan datos como ficheros históricos (ficheros log), direcciones IP, cookies, o cookies en flash. Remarca que los buscadores que recurren a medios en el territorio de

555 B.O.E., núm. 301, de 16 /12/2000, págs. 44253 y 44254.

556 Véase:<http://www.europa.eu.int/comm/internal_market/privacy/adecuacy_fr.htm>.

557 La lista de entidades estadounidenses adheridas a los principios de "Puerto Seguro" está disponible en: <www.export.gov/safeharbor>.

558 COUDERT F.: op. cit., pág. 435.

559 En: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_es.pdf>.

un Estado miembro (EEE, es decir, bajo el ámbito de aplicación de las Directivas comunitarias) para el tratamiento de datos personales también se encuentran dentro del ámbito de la legislación en materia de protección de datos de ese Estado miembro.

Matización importante introduce el Dictamen 1/2008 acerca de la no aplicabilidad a los buscadores de las Directivas 2002/58/CE sobre la privacidad y las comunicaciones electrónicas y la 2006/24/CE sobre conservación de datos, al afirmar que los servicios de los buscadores en sentido estricto no se encuentran dentro del ámbito del nuevo marco normativo para las comunicaciones electrónicas[560]. El artículo 2, apartado c) de la Directiva marco (2002/21/CE), que contiene algunas de las definiciones generales del marco normativo, excluye explícitamente los servicios que prestan o ejercen control editorial sobre el contenido: "*Servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos; quedan excluidos asimismo los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas*"[561]. Por lo tanto, los buscadores quedan fuera del ámbito de la definición de servicios de comunicación electrónica.

Un proveedor de buscadores puede ofrecer, sin embargo, un servicio adicional que se encuentre dentro del ámbito de un servicio de comunicaciones electrónicas, como un servicio de correo electrónico públicamente accesible que se encontraría sujeto a la Directiva 2002/58/CE[562] sobre la privacidad y las comunicaciones electrónicas y la Directiva 2006/24/CE[563] de conservación de datos. El artículo 5(2) de la Directiva de conservación de datos dispone específicamente que "*de*

560 Ibídem, pág. 13.

561 Diario Oficial de las Comunidades Europeas L 108, de 24/04/2002, pág. 39.

562 Diario Oficial de las Comunidades Europeas L 201, de 31/07/2002, pág. 37.

563 Diario Oficial de la Unión Europea L 105, de 13/04/2006, pág. 54.

conformidad con la presente Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación". Las propias búsquedas se considerarían contenido en vez de tráfico de datos y, por lo tanto, la Directiva no justificaría su conservación. Por consiguiente, no se justifica ninguna referencia a la Directiva de conservación de datos en relación con el almacenamiento de registros de servidores generados al ofrecer un servicio de buscador.

8.4.1. Buscadores, libertad de expresión, intimidad y protección de datos.

El Grupo de Trabajo dedica en el Dictamen 1/2008 una reflexión a lo que considera papel especial que desempeñan los buscadores en el entorno de la información online, indicando que debe lograrse un equilibrio entre la legislación en materia de protección de datos de la Comunidad Europea y las legislaciones de los diversos Estados miembro, entre la protección del derecho a la intimidad y la protección de los datos personales por una parte, y , de otra, el flujo libre de información y el derecho fundamental a la libertad de expresión.

Señala que lo que se propone la Directiva de protección de datos es lograr este equilibrio en la legislación de los Estados miembros en el contexto de los medios de comunicación. Asimismo, el Tribunal de Justicia Europeo ha indicado claramente que los límites a la libertad de expresión que pudieran derivarse de la aplicación de los principios de protección de datos deben cumplir la ley y respetar el principio de proporcionalidad[564].

Añade el Dictamen 1/2008[565] que la Directiva de protección de datos no contiene ninguna referencia especial al tratamiento de datos personales por parte de los servicios de la sociedad de la información que actúan como intermediarios seleccionados. El criterio decisivo de la Directiva de protección de datos 95/46/CE para su aplicabilidad es la definición del responsable de tratamiento, especialmente si una parte "*sola o conjuntamente con otras determina los fines y los medios del tratamiento de datos personales*". La cuestión de si un intermediario debe considerarse como el propio responsable de tratamiento o un responsable de tratamiento

[564] El Tribunal de Justicia Europeo ha explicado con más detalle la proporcionalidad del impacto de las normas de protección de datos, por ejemplo, sobre la libertad de expresión, en su sentencia en el caso de Lindqvist v. Suecia, apartados 88-90.

[565] <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_es.pdf>, pág.15.

conjuntamente con otros en relación con un tratamiento concreto de datos personales se separa de la cuestión de responsabilidad por dicho tratamiento.

En cualquier caso, el Dictamen 1/2008 establece que el efecto combinado de los artículos 4, apartado 1, letra a), y el artículo 4, apartado 1, letra c), de la Directiva sobre protección de datos es que sus disposiciones se aplican al tratamiento de datos personales por los proveedores de motores de búsqueda en numerosos casos, aunque su sede se encuentre fuera del territorio comunitario.

El Grupo de Trabajo de expertos comunitarios resume, en sus conclusiones, la aplicabilidad de las Directivas comunitarias, los derechos de los usuarios y, en especial, las obligaciones de los proveedores de motores de búsqueda.

8.4.1.1. Aplicabilidad de las Directivas CE.

La Directiva 95/46/CE sobre protección de datos, por tanto, se aplica generalmente al tratamiento de datos personales por los motores de búsqueda, incluso cuando su sede se encuentra fuera del territorio comunitario.

Los proveedores de motores de búsqueda con sede fuera del territorio comunitario deberían informar a sus usuarios de las condiciones en que deben cumplir la Directiva sobre protección de datos, tanto debido a la presencia de un establecimiento como a la utilización de medios que se encuentren en el territorio de un Estado miembro.

La Directiva sobre conservación de datos (2006/24/CE) no se aplica a los motores de búsqueda en Internet, tal y como se ha dejado explicado y reseña el Dictamen 1/2008[566].

8.4.1.2. Obligaciones de los proveedores de motores de búsqueda.

Al hilo de las argumentaciones expuestas, la primera de las obligaciones de los motores de búsqueda es que sólo podrán tratar datos

566 Ibídem, pág., 27.

personales con fines legítimos, y la cantidad de datos debe ser pertinente y no excesiva con relación a los fines previstos.

Los proveedores de motores de búsqueda deben suprimir y hacer anónimos los datos personales (de manera irreversible y eficaz) una vez que no sean ya necesarios para el fin para el que se habían recogido. Para lograr el cumplimiento de todo ello, lo idóneo, para los especialistas comunitarios, es que "*desarrollen programas adecuados para lograr el anonimato*"[567].

Una de las obligaciones más significativas es la relativa a los periodos de conservación, que deberían reducirse al mínimo y ser proporcionales al fin previsto por los proveedores de motores de búsqueda. A la luz de las explicaciones iniciales dadas por los proveedores de motores de búsqueda con respecto a los posibles fines de la recogida de datos personales, el Grupo de Trabajo no ve razón para conservar estos datos más allá de seis meses. Ahora bien, se otorga la posibilidad a los Estados comunitarios de que, a través de sus legislaciones nacionales, puedan exigir que los datos personales se supriman antes. Para que los proveedores de motores de búsqueda puedan conservar los datos personales más de seis meses, deberán demostrar, con todo tipo de detalle, que esa conservación de datos es estrictamente necesaria para el servicio que ofrece.

A tener en cuenta que si los proveedores de motores de búsqueda utilizan cookies, la permanencia de los mismos no debería ser más extensa en el tiempo de lo necesario. Al igual que las cookies de Internet, sólo deberían instalarse cookies flash[568] si se proporciona información

[567] Ib., pág. 28.

[568] Una cookie flash, o Local Shared Object (LSO) (en español, Objeto Local Compartido), es una colección de archivos tipo cookie almacenados como archivo en computador del usuario. Los LSO son usadas por todas las versiones de Adobe Flash Player desde la versión 6 y posteriores de Macromedia hasta el ahora obsoleto Flash MX Player.Con la configuración por defecto, Adobe Flash Player no solicita el permiso del usuario para alojar los LSO en el disco duro. Los LSO contienen datos tipo cookie alojados en determinadas páginas webs o dominios. Cualquier tipo de datos pueden ser alojados, algunos de ellos que tienen que ver con la privacidad. Es más, con estas cookies, los bancos en línea, comerciantes o anunciantes pueden usar los LSO con fines comerciales. Según la definición que ofrece sobre cookie flash wikipedia. Véase en: <http://es.wikipedia.org/wiki/Local_Shared_Object>.

transparente sobre las razones de su instalación y sobre cómo acceder a esta información, modificarla y suprimirla.

Importante obligación establecida, como contempla el Dictamen 1/2008[569], es que los proveedores de motores de búsqueda "*deben proporcionar a los usuarios información clara e inteligible sobre su identidad y su situación, así como sobre los datos que prevén recoger, almacenar o transmitir, y sobre la finalidad de la recogida de estos datos*".

Recuerda esta norma comunitaria que todo lo que sea engrosar o ampliar los perfiles de usuarios con datos no proporcionados por los propios usuarios debe hacerse con el consentimiento de los titulares de esos datos, y que si los proveedores de motores de búsqueda ofrecen medios para conservar los historiales de búsqueda, deben obtener el consentimiento del usuario para estar al cumplimiento normativo.

Otras de las obligaciones importantes para los motores de búsqueda es que deben permitir la elección de los editores de los sitios Internet de no participar en sus servicios, y para ello han de dejarlo indicado, señalando que el sitio de Internet en cuestión no debe explorarse ni indexarse.

Establece el Dictamen 1/2008 que en aquellos casos en que los proveedores de motores de búsqueda cuentan con una memoria oculta en la que los datos personales están disponibles durante mucho más tiempo que en la publicación original, "*deben respetar el derecho de los interesados a que se retiren los datos excesivos o incorrectos de su memoria oculta*"[570].

Para aquellos proveedores de motores de búsqueda especializados en la creación de 'operaciones de valor añadido', es decir, la elaboración de los perfiles de personas físicas (llamados "motores de búsqueda de personas") y los programas de reconocimiento facial de imágenes, se establece que "*deben tener una razón legítima*" para tratar los datos personales, con el consentimiento del interesado, y deben cumplir todos los demás requisitos de la Directiva sobre protección de datos, como la obligación de garantizar la calidad de los datos y la equidad del tratamiento, entre otros.

---

[569] <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_es.pdf>, pág. 28.

[570] Ibídem, pág., 29.

8.4.1.3. Derechos de los usuarios.

Resume el Dictamen 1/2008, aprobado en abril de ese año, que los usuarios de los servicios de motores de búsqueda tienen derecho a acceder, examinar y, en su caso, corregir, con arreglo al artículo 12 de la Directiva 95/46/CE sobre protección de datos[571], todos sus datos personales, incluidos su perfil y sus historiales de búsqueda.

Exige, además, la recogida del consentimiento, al señalar que sólo puede efectuarse la correlación cruzada de datos procedentes de distintos servicios pertenecientes al proveedor del motor de búsqueda si el usuario ha dado su concreta aceptación.

8.4.2. Norma anti '*cookies*'.

Ha sido en marzo de 2012, a través del Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas[572], cuando España ha adaptado la Directiva europea sobre el uso de datos obtenidos en Internet a través de estos programas que se infiltran en la navegación del internauta En concreto, por medio de esa norma, se modifican varios artículos de la Ley 34/2002, de 11 de julio[573], de Servicios de la Sociedad de la Información y del Comercio Electrónico, a fin de adecuar su régimen a la nueva redacción dada, por la Directiva 2009/136/CE[574], a la Directiva 2002/58/CE[575], del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, debiéndose destacar la nueva redacción que se da a su artículo 22.2, para exigir el consentimiento del usuario sobre los archivos o programas informáticos («cookies») y ofrecer a los ciudadanos

571 El artículo 12 es el relativo al derecho de acceso a los datos. Diario Oficial n° L 281, de 23/11/1995, pág. 42.

572 B. O. E., núm. 78, de 31/03/2012, sec. I, pág. 26876.

573 B.O.E., núm. 166, de 12 /07/2002, pág. 25388.

574 Diario Oficial de las Comunidades Europeas L 337 de 18.12.2009.

575 Diario Oficial de las Comunidades Europeas L 201/37, de 31/07/2002.

mecanismos que les permitan preservar su privacidad. La nueva norma obliga a que el usuario acepte la recogida de datos.

8.5. El criterio de INTECO sobre los buscadores.

El Instituto Nacional de Tecnologías de la Comunicación (Inteco) ha elaborado un análisis exhaustivo sobre cómo actuar ante la publicación de una información o documento en Internet cuyo contenido atente contra el derecho a la intimidad y a la protección de datos de carácter personal de un usuario, y en la que analiza la responsabilidad de los proveedores de contenido.

Inteco sienta sus criterios sobre la protección y defensa de los derechos de las personas en Internet para afirmar que, desde el punto de vista de los buscadores, se debe tener en cuenta su posición como simples mediadores, por lo que su responsabilidad queda delimitada por lo dispuesto en el art. 17 de la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico, relativo a la "*responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda*"[576].

Cita Inteco a la propia Agencia Española de Protección de Datos en la argumentación que hace en su Guía legal sobre la protección del derecho al honor, a la intimidad y a la propia imagen en Internet[577] acerca de que la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet se califica en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico como un servicio de intermediación. La ley reconoce un interés legítimo en orden a la prestación del servicio, excluyendo inicialmente su responsabilidad, "…*si bien les impone un deber de colaboración para impedir que determinados servicios o contenidos ilícitos se sigan divulgando, como puede suceder cuando se lesionen los derechos reconocidos por la normativa de protección de datos*"[578].

---

[576] B.O.E., núm. 166, de 12 /07/2002, pág. 25393.

[577] Guía de Inteco de 25 de septiembre de 2008. Accesible en su página web: <http://www.inteco.es/Seguridad/Observatorio/guias//guiaManual_honor_internet>.

[578] Ibídem, pág., 4.

Para Inteco, de todo ello cabe extraer que la Ley Orgánica de Protección de Datos sería de aplicación, a pesar de existir una exención, al menos inicial, de la responsabilidad de los buscadores en la labor de indexación de contenidos publicados en Internet. Exención que se rompe en el caso de que de la indexación se derive una lesión de los derechos reconocidos por la normativa vigente en materia de protección de datos[579].

La Agencia Española de Protección de datos emitió en diciembre de 2007 una amplia e interesante Declaración sobre buscadores de Internet[580].

8.6. Proliferación de los Medios de Comunicación en Internet.

La Asociación para la Investigación de Medios de Comunicación, (AIMC), gestora de los más importantes estudios de audiencia en España, entre otros el famoso EGM, ha realizado a finales de 2010 el primer estudio español sobre "*Internet, en medio de los medios*"[581].

Se fundamenta en la irrupción de Internet en la sociedad, que ha alterado también nuestra forma de relacionarnos con los Medios de Comunicación. Internet, señala AIMC, ha provocado una dilución de las fronteras que tradicionalmente han separado los distintos tipos de Medios. Sugiere que Internet nos permite acceder a numerosas versiones digitales de los soportes tradicionales, lo que amplía el abanico de posibilidades para informarnos y entretenernos al alcance de una sola pantalla, aunque algunos, como remarca R. Salaverría, ya abundaron en el denominado '*ciberperiodismo*' hace bastantes más años[582].

AIMC realizó el primer estudio "*Internet, en medio de los medios*" con el objetivo de conocer un poco más los hábitos de los usuarios y sus opiniones y preferencia, resaltando, entre sus conclusiones, que sólo un

[579] Ib., págs. 4 y 5.

[580] Véase: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/declaracion_aepd_buscadores.pdf>.

[581] Véase: <http://aimc.es/-Internet-en-medio-de-los-medios-.html>.

[582] SALAVERRIA, Ramón: '*Ciberperiodismo: El impacto de Internet en los medios de comunicación en España*'. Comunicación Social Ediciones, Sevilla, 2005.

10% de los encuestados que acceden al soporte tradicional no acceden a la prensa online. Del estudio se desprende que los hábitos de los usuarios están cambiando a la hora de acceder a la prensa. De los lectores que acceden a ambos tipos de soportes (papel y digital) más de un 50% aseguran dedicar menos tiempo a leer las versiones impresas de los diarios. Casi la mitad de los encuestados continúan dedicando el mismo tiempo a la lectura de diarios impresos (48,4%)[583].

Si se examina el tipo de información que busca el lector, la edición impresa prevalece como fuente principal para informarse de temas en profundidad (50,6%) mientras que la inmediatez vence en el terreno online ya que para las noticias de actualidad la Red es la más valorada (43,8%).
A pesar del crecimiento de los diarios en Internet, aún se da ese 10% de los encuestados que no accede a la prensa en formato electrónico. Sus principales razones para no hacerlo son la facilidad que les ofrece el soporte impreso para poder leerlo en cualquier sitio (64,1%) y el no necesitar un soporte electrónico -ya sea un ordenador o un móvil- para poder acceder a la información (15,1%).

En el extremo opuesto encontramos a los que tan sólo acceden a formatos electrónicos. De hecho, cabe destacar que el 38% de estos consumidores de información reconoce que antes leía diarios en papel y que ahora ha dejado de dedicarles tiempo. Sus principales motivos para no buscar información en los diarios impresos son el no tener que desplazarse a ningún sitio para poder acceder a la información (34,5%); la facilidad para poder personalizar la lectura de noticias (33,8%); y la opción de poder leer varios medios por el mismo precio (28,4%).

En cuanto a las emisoras de Radio, el estudio de AIMC evidencia que Internet no puede aún con la radio convencional, pues los oyentes continúan siendo fieles a la radio a través de soporte convencional. De hecho, un 73% de los que escuchan radio a través de los dos soportes asegura que no ha reducido su consumo y tan sólo un 23’9% le dedica ahora menos tiempo. De los que sólo escuchan la radio a través del sistema tradicional, un 42% no lo escucha a través de internet porque utiliza equipos portátiles[584].

Respecto al consumo de televisión a través de Internet, señala el estudio que la Red se ha convertido en una fuente de información y

[583] <http://aimc.es/-Internet-en-medio-de-los-medios-.html>: op. cit., pág. 10.
[584] Ibídem, pág., 15.

entretenimiento imprescindible y muestra de ello es que el 53,6% de los internautas la ha utilizado en los últimos 30 días para ver la televisión principalmente a través del portátil (70%), siendo el ordenador de sobremesa el segundo soporte preferido (50%) y encontrando al teléfono móvil como tercera opción (14,7%). Son muy pocos, el 1,4%, los que admiten que han dejado de ver televisión convencional para disfrutar sólo de sus programas favoritos a través de la Red[585].

8.7. Política de privacidad de la versión digital del Medio de Comunicación.

La página o sitio web del Medio de Comunicación ha de presentar, claramente a la vista, una leyenda con su política de privacidad, relacionada y haciendo mención a la normativa de protección de datos personales, que reseñe, al menos, dónde pueden ejercitarse los derechos ARCO (acceso, rectificación, cancelación y oposición), es decir, el contenido que impone el art. 5 de la Ley Orgánica de Protección de Datos, que regula el derecho de información en la recogida de datos.

La Agencia Española de Protección de Datos no se ablanda ante este tipo de obligaciones, pues entiende que de lo que se trata es que se impida la posibilidad de recabar o difundir datos personales sin dar cuenta de lo establecido por la normativa de protección de datos, y entiende que es una "*falta de diligencia*" el incumplimiento de esta circunstancia, que acarrea una sanción de 15.000 euros por una infracción de carácter leve[586].

[585] Ib., pág., 16.

[586] Sanciones establecidas en el artículo 45 de la Ley Orgánica de Protección de Datos. B.O.E., núm. 298, de 14/12/1999, op. cit., págs. 43097 y 43098.

9. REDES SOCIALES, EXTENSIBILIDAD Y ESTRUCTURA SUPERVISORA.

9.1. La extensión de las redes sociales.

Facebook[587], MySpace[588], Twitter[589], Tuenti[590], Linkedin[591], Migente[592], Orkut[593], Xanga[594], Youtube[595], y así hasta cerca de un centenar de redes sociales conocidas inundan ya Internet ofreciendo interactividad entre miles y cada vez más miles de ciudadanos (más de 400 millones según los últimos estudios) de todos los rincones del planeta, con los datos de carácter personal campando, muy a menudo, de manera ilimitada y multiplicando riesgos de muy variada naturaleza. Cada red social, con sus matices y singularidades[596].

Los millones de usuarios que tiene registrados ya Facebook hacen tambalear los cimientos de la protección de datos y los derechos a la intimidad y al honor, circunstancia que invita a la reflexión por parte de los más reputados especialistas. Las redes sociales pueden permitir a las empresas y los Gobiernos husmear en nuestras vidas, aunque, como escribe Timothy Garton, Catedrático de Estudios Europeos en la Universidad de Oxford, "*comparado con los periódicos tabloides británicos, que interceptan mensajes de móviles para revelar secretos y vender más diarios, Facebook llegar a ser un virtuoso sacerdote protector del secreto de confesión, y es que las mismas tecnologías que reducen nuestra*

[587] <http://www.facebook.com/>.

[588] <http://www.myspace.com/>.

[589] <https://twitter.com/>.

[590]< http://www.tuenti.com/?m=login>.

[591] <http://www.linkedin.com/>.

[592] <http://www.migente.com/>.

[593] <http://www.orkut.com/>.

[594] <http://www.xanga.com/>.

[595] <http://www.youtube.com/>.

[596] ACED, Cristina: '*Redes sociales en una semana*'. Centro Libros PAPF, Planeta, Barcelona, 2010.

privacidad pueden ayudar a defendernos, pero en los últimos años ha contribuido a la erosión de la intimidad, y todavía deja mucho que desear"[597].

9.2. Redes sociales y Medios de Comunicación.

Las características singulares de las redes sociales hace conferirles un papel esencial para los Medios de Comunicación, que no han querido desperdiciar las cualidades que ofrecen, como el carácter multimedia, pues las redes permiten que los usuarios suban contenidos como audios, fotografías o sonidos[598]. Se crean aplicaciones sencillas en estos espacios, que apenas ralentizan la carga de la web, y que se pueden ver u oír en la misma página, sin remitir a ventanas externas.

El hipertexto es una de los rasgos de la nueva comunicación. La naturaleza de Internet se basa en los enlaces y, en el caso de los Medios de Comunicación, los usuarios suben los enlaces de las noticias en las redes sociales, potenciando la navegación entre hipertextos, aportando una mayor profundidad a los contenidos o comentarios publicados.

La interactividad se hace ya imprescindible y, de hecho, las redes sociales permiten el mayor estadio de interactividad posible en la red. No sólo existe una comunicación bidireccional, sino múltiple, ya que en un mismo instante todas las personas conectadas a la red pueden escribir o comentar los contenidos que suba un determinado usuario. Para las nuevas generaciones, que rechazaban realizar comentarios en los medios de comunicación[599], esta opción es una oportunidad que se adapta más a sus preferencias de interactividad. Con esta nueva solución no interactúan directamente con el medio de comunicación sino que usan una noticia del medio para interactuar con sus amigos o seguidores de una red social.

A diferencia de los comentarios que un usuario puede hacer en una noticia de un medio, donde su reflexión pasa por un filtro, el del redactor,

---

[597] "*El País*", 11 de octubre de 2010, pág. 27.

[598] CARDOSO, Gustavo: *'Los medios en la sociedad en red'*. UOC Ediciones, Barcelona, 2008.

[599] BERNAL A.I. '*Los nuevos medios de comunicación y los jóvenes. Aproximación a un modelo ideal de medio*'. Euroeditions, Madrid, 2009.

para su definitiva publicación; en las redes sociales pueden comentar las noticias que hayan enlazado otros amigos con total libertad y sin restricción alguna. En ocasiones los medios de comunicación usan aplicaciones de las redes sociales específicas para la retransmisión en directo de noticias, alcanzando la "*potencialidad de instantaneidad*", es decir, "*la posibilidad de ofrecer informaciones en el mismo momento en que se producen*"[600].

La actualización resulta más inmediata que nunca. Factor que depende no de la propia red social, sino que al ser el usuario y los amigos asociados los creadores de sus perfiles, son ellos los que determinan el grado de renovación de los contenidos.

Las redes sociales no son Medios de Comunicación, aunque sí son un nuevo canal de distribución que permite enlazar sus contenidos en función de lo que publique la audiencia, dando lugar en ocasiones a un periódico personalizado, en el sentido de que pueden ver contenidos que ellos, los usuarios, han seleccionado. Pero las diferencias son notables: en la red social, aparecen exclusivamente las informaciones que los usuarios deciden publicar y, además, los contenidos informativos que decidan publicar se unen a otros más personales sobre los amigos, familiares o compañeros del usuario, etc[601].

A tenor de todo ello, los Medios de Comunicación han pensado introducir 'formatos participativos' que repartan los contenidos de su versión digital. Para registrarse en estas redes se pide al usuario entre cuatro y diecisiete datos personales, lo que origina una herramienta de marketing para la segmentación y planificación. Además, estas redes a su vez invitan a amigos a afiliarse. La rentabilidad de las redes sociales es mucho mayor tanto por la afiliación voluntaria, la colaboración por aportar contenidos, y la mayor atención que prestan a los contenidos publicitarios. Para paliar la ausencia de portabilidad del ordenador, las redes también tienen presencia en terminales portátiles como los móviles, en respuesta a una de las formas de distribución de contenidos más usada por la audiencia[602].

---

600 CABRERA M. A. '*La prensa online. Los periódicos en la www'*. Cims, Barcelona, 2000.

601 Ibídem.

602 Ibídem.

La gran mayoría de los Medios tradicionales presentes en Internet, y también los propios Medios creados en la Red, han respondido a la demanda multitudinaria de las redes sociales. Consiguen varios beneficios: mejorar su identidad de marca, fidelización e interactividad. Y otro rédito que se logra es la oportunidad de publicar o compartir directamente esos contenidos desde el propio Medio.

En nuestro país, se observa cómo los Medios de Comunicación se decantan por redes especializadas en noticias que funcionen como marcadores, como Menename[603] o Del.ici.ous[604], con una mayor preferencia por la primera al ser una herramienta en español, mientras que Del.ici.ous es en inglés. Estas redes permiten mejorar el posicionamiento del Medio informativo. Después, como espacios de publicación sitúan en primer lugar redes sociales como Facebook, donde los periódicos, radios o televisiones pueden configurar una página en la que completar información en torno al Medio de Comunicación y ofrecer noticias y reportajes de interés. La ventaja principal de esta página, según el estudio sobre la materia realizado por N. García Estévez, es que los usuarios no tienen que enviar solicitud de amistad para poder interactuar, sino que simplemente hacen un 'clic' en la pestaña '*Me gusta*' de la red Facebook para poder acceder al mismo[605].

Ningún Medio de Comunicación incluye la red Tuenti, que en España ha llegado a adelantar en audiencia a Facebook, aunque quizá se deba al perfil más juvenil de esa red. También es interesante comprobar que los Medios de Comunicación que han sido creados en la red, que no tienen referente tradicional, ofrecen e invitan en menor medida a publicar sus contenidos en las redes, con menos opciones. Sin embargo, deciden crear su propia red social, como en el caso de Souti o Eskup (en el caso del diario "El País")[606]. Las redes más nuevas son las que más usan los Medios como plataformas de distribución. Redes más clásicas, y que fueron las primeras en aparecer en este nuevo universo comunicativo, como el caso de My Space, han ido perdiendo poder y uso entre la audiencia.

603 <http://www.meneame.net/>.

604 <http://del.icio.us/post/>.

605 GARCÍA ESTÉVEZ, N.: op. cit., pág.228.

606 <http://eskup.elpais.com/index.html>.

9.3. Guía de los supervisores españoles sobre redes.

Tanto las autoridades españolas como las europeas, conscientes de la magnitud que ha ido tomando la nueva situación han ido tomando cartas en el asunto. En nuestro país, la Agencia Española de Protección de Datos no ha cesado en remitir a las redes sociales exigencias para que cumplan con la normativa vigente.

La Agencia, junto al Observatorio del Instituto Nacional de las Tecnologías de la Comunicación (Inteco), tienen elaborado desde 2008 un estudio '*Sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line*'[607], que las define como servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado.

El modelo de crecimiento de estas plataformas se basa fundamentalmente en un proceso viral, en el que un número inicial de participantes, mediante el envío de invitaciones a través de correos a sus conocidos, ofrece la posibilidad de unirse al sitio web. Estos nuevos servicios se configuran como poderosos canales de comunicación e interacción, que permiten a los usuarios actuar como grupos segmentados: ocio, comunicación, profesionalización, etc.

Para el estudio, muy elaborado por parte de la Agencia Española de Protección de Datos y de Inteco, uno de los principales objetivos de la red social se alcanza en el momento en el que sus miembros utilizan el medio online para convocar actos y acciones que tengan efectos en el mundo offline.

En España, las fuentes estadísticas son diversas, pero todas coinciden en que número de usuarios españoles de Internet que utiliza habitualmente redes sociales se sitúa entre el 40% y el 50%. De esta forma, en España más ocho millones de usuarios habituales de Internet (mayores de 15 años y con conexión) utilizan redes sociales, siendo el porcentaje de usuarios de redes sociales más alto entre los más jóvenes, aunque es muy creciente el número de adultos que se incorpora a alguna de ellas.

---

607 Disponible en la página web de la Agencia Española de Protección de Datos en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf>.

Sobre los aspectos más relevantes en cuanto a la problemática específica de las redes sociales en materia de defensa y protección de los datos personales de los usuarios, el estudio español de la Agencia e Inteco destaca los riesgos[608], al establecer que el consentimiento que presta el usuario es válido en el momento en que decide aceptar la política de privacidad y condiciones de uso de la plataforma que constan en el formulario de registro. Por ello, debe estar muy atento a su contenido y consecuencias. Ello no obsta a que resulte exigible que las políticas de privacidad deban ser transparentes, accesibles y claras, prescribe el estudio. La Agencia Española de Protección de Datos ha insistido sobre el particular en su 'Declaración sobre buscadores', anteriormente aquí citada[609].

Del mismo modo, apunta el estudio, los usuarios deben valorar siempre qué tipo de datos proporcionan a la plataforma y publican en su perfil, ya que no tiene la misma trascendencia el tratamiento por parte de la plataforma de los datos de carácter personal de nivel básico (nombre, dirección, teléfono, etc.), que otras información de contenido más sensible (nivel de renta, solvencia, recibos, afiliación sindical o política, salud, vida sexual, etc.), donde el nivel de protección y concienciación por parte del usuario deberá ser mucho mayor, dado que se trata de derechos pertenecientes a la esfera más íntima de su vida[610].

Por ello, a pesar de que la información contenida en los perfiles de los usuarios es alimentada directamente por éstos, es necesario tener en cuenta cuáles son los principales riesgos para la protección de los datos de carácter personal.

Como criterio general, las redes sociales y plataformas colaborativas disponen de avisos legales, condiciones de uso y políticas de privacidad, aunque en ocasiones, redactadas en un lenguaje de difícil comprensión para el usuario. De esta forma, y a pesar de encontrarse recogidas en el sitio

608 Ibídem, pág., 109.

609 Declaración sobre buscadores, de diciembre de 2007, op. cit., disponible en: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/declaracion_aepd_buscadores.pdf>.

610 Estudio realizado '*Sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line'*, op. cit., pág. 110. <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf>.

web, no alcanzan su finalidad última: que el usuario comprenda el objeto, la finalidad y el plazo para el que son recabados y tratados sus datos personales. De ahí que el primer momento crítico para la protección de datos personales se encuentra en la misma fase inicial de registro del usuario, cuando éste proporciona la información personal necesaria para poder operar en la red social. En ese momento, los datos se pueden ver sometidos a varios riesgos, como el hecho de que el tipo de datos solicitados en el formulario de registro, aunque no obligatorios, sean excesivos. En este sentido, debe tenerse en cuenta que, con frecuencia, las redes sociales solicitan a los nuevos usuarios datos relativos a su ideología política, orientación sexual y preferencia religiosa. Si bien es cierto que estos datos tienen carácter voluntario y todo usuario es libre de publicar el contenido que deseé respecto a sí mismo, debe considerar las implicaciones que ello puede conllevar para su vida y las personas de su entorno, ya que estos datos serán visibles por todos sus contactos y, dependiendo de la configuración del perfil, por todos los usuarios de la red. Es por ello que los usuarios y los responsables de las redes deben llevar a cabo un control sobre la trascendencia de los datos publicados. Es posible, también, que el grado de publicidad del perfil de usuario sea demasiado elevado, un aspecto que puede darse fácilmente, pues casi todas las redes analizadas muestran, activado por defecto, el mayor grado publicidad, lo que supone un grave riesgo para la seguridad de los datos personales de los usuarios.

Puede ocurrir, además, que la finalidad de los datos no esté correctamente determinada, por una política de privacidad poco clara. Igualmente, es otro riesgo la transferencia internacional de datos. Es frecuente que este tipo de plataformas se encuentren ubicadas fuera del territorio europeo, principalmente en EE.UU., lo que supone que en el momento de registro del usuario, los datos son trasladados a los servidores y oficinas ubicados en este país. Por ello, según el estudio, "*resulta fundamental que las políticas de privacidad del proveedor garanticen un estándar adecuado de protección*"[611].

El segundo momento considerado crítico para la protección de datos personales se sitúa, según el estudio '*Sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line*' en la fase en la que se utilizan los servicios y herramientas que la plataforma ofrece. En esa actividad, los usuarios pueden incurrir en una publicación excesiva de información personal, propia o de terceros. Se da la posibilidad de que los usuarios publiquen también datos respecto de

611 Ibídem, pág., 111.

terceros, lo que puede conllevar el tratamiento y la cesión pública de datos de personas que no han prestado el consentimiento para ello. De hecho, la Agencia Española de Protección de Datos ha sancionado la captación y publicación de imágenes de terceros en plataformas colaborativas sin consentimiento de las personas afectadas[612].

De la misma forma, la Agencia Española de Protección de Datos ha reconocido el derecho frente al responsable del sitio web a cancelar los datos publicados que habían sido facilitados por terceros en entornos online[613].

Durante esa actividad de uso de las herramientas de la red social, es un riesgo para los datos personales la instalación y uso de "cookies" sin conocimiento del usuario, algo que emplean las redes sociales con mucha frecuencia buscando almacenar determinada información sobre el usuario y su tipo de navegación a través de un sitio web.

Estos ficheros se instalan en los equipos de los usuarios, adivinando casi todo del usuario, el tipo de contenidos accedidos, los lugares más visitados y las acciones habituales realizadas durante la navegación, incluido hasta el tiempo empleado en cada una de las páginas, entre otras muchas funcionalidades, lo que proporciona una herramienta muy valiosa desde el punto de vista del marketing y la publicidad.

Constituye otro riesgo el uso de web "beacons"[614], que son imágenes electrónicas que permiten al sitio web conocer quién y qué contenido online ha sido visitado. Normalmente estas imágenes son incluidas en correos electrónicos, anuncios, etc. Como captan, sobre todo, datos

612 Resolución de la Agencia Española de Protección de Datos PS/00117/2008, en el que se sanciona a un sujeto que publica en la red imágenes obtenidas de la vía pública en las que aparecen personas. B.O.E. Núm. 93, de 17/04/2008.

613 Como la Resolución R/00671/2011, correspondiente al Procedimiento Nº.PS/00619/2010, que sanciona a un sindicato policial que publicó datos de un ciudadano que había pedido la cancelación de los mismos. Disponible en: <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2011/common/pdfs/PS-00619-2010_Resolucion-de-fecha-26-04-2011_Art-ii-culo-10-LOPD.pdf>.

614 Un beacon, o web bug, es un objeto que está incrustado en una página web o de correo electrónico y por lo general invisible para el usuario, pero permite comprobar que un usuario ha visto la página o correo electrónico. Un uso común es en el seguimiento de correo electrónico. Según definición expuesta en wikipedia. <http://en.wikipedia.org/wiki/Web_bug>.

relacionados con el gestor de correo, se emplean para la confirmación de direcciones electrónicas (para envío masivo de correo electrónico no deseado o para comercialización de bases de direcciones confirmadas), etc.

Otro riesgo para los datos en las redes sociales es que el perfil de usuario sea indexado automáticamente por los buscadores de Internet. La mayor parte de las plataformas analizadas para la elaboración del informe, y salvo algunas concretas que así lo han trasladado en las entrevistas mantenidas, permiten que los motores de búsqueda de los principales buscadores de Internet puedan indexar los perfiles de los usuarios de forma pública en la red.

En algunos casos, según advierte el estudio[615], dicha indexación incluye el nombre del usuario registrado, su fotografía del perfil y el nombre y fotografías del perfil de los amigos o contactos con los que cuenta en la red social, así como una invitación general a entrar a formar parte de la plataforma. Este hecho supone una amenaza para la protección de datos personales de los usuarios, en la medida en que sus datos básicos y principales contactos se exponen públicamente en la red, accesibles por parte de cualquier usuario, pudiendo llegar a ser empleadas esas informaciones de forma descontrolada por terceros, sin que éstos queden en el "circulo cerrado" de la red social.

Otros riesgos a los que se exponen los datos personales en la actividad de un usuario de red social son la recepción de publicidad hipercontextualizada; la recepción de comunicaciones comerciales electrónicas no solicitadas (spam), y, especialmente, la suplantación de identidad de los usuarios de la red social. El concepto de "suplantación de identidad" recogido como delito en nuestra normativa penal, adopta una nueva trascendencia en el mundo online, dado que cualquier usuario puede contar en Internet con varias "identidades digitales". Desde luego que no se trata de un comportamiento negativo, sin embargo la posibilidad de que la identidad de una persona sea registrada por otra persona ajena aumenta considerablemente[616].

---

615 Estudio '*Sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line'*, op. cit., pág. 113. <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf>.

616 Ibídem, pág., 115.

Llegamos, así, al tercer momento crítico para la protección de datos personales se sitúa en la fase en la que el usuario pretende darse de baja del servicio. Puede, entonces, que se dé la imposibilidad de realizar la baja efectiva del servicio. Se ha detectado cómo en algunos casos, a pesar de solicitar la baja del servicio conforme a las políticas de privacidad recogidas en algunas plataformas, la baja del servicio no se ha llevado a cabo de manera efectiva, manteniéndose los datos personales de los usuarios a disposición de los responsables de la red social[617].

La conservación de datos y el cumplimiento del principio de calidad de los datos se convierte, por tanto, en otro problema que sucede cuando formamos parte de una red social. Y es lo que han de tener en cuenta los Medios de Comunicación que emplean estas plataformas.

Aunque el caso particular de las redes sociales no es idéntico al de los buscadores, se puede concluir que las redes sociales, como servicios de la Sociedad de la Información, deben someterse a la aplicación de la normativa de protección de datos, debiendo atender a los principios básicos que rigen la norma, como son el principio de calidad de los datos en la medida en que no deben conservar los datos de forma indefinida en sus servidores, el principio de consentimiento, y el principio de información, en la medida en que deben informar de forma clara y comprensible a todos los usuarios respecto a qué van a hacer con sus datos y del derecho a disponer respecto a los mismos en cualquier momento.

El estudio de la Agencia Española de Protección de Datos y del Instituto Nacional de Tecnologías de la Comunicación sugiere medidas para la correcta protección de los datos personales en las redes sociales, como eliminar los datos obsoletos que pudieran existir en distintos servidores, establecer mecanismos de análisis respecto de la fortaleza de la contraseña de manera que se obligue al usuario a seleccionar una que no sea fácilmente descifrable por terceros, disociar los datos incluidos dentro de un perfil de usuario, crear categorías de perfiles para controlar el volumen de datos personales que el usuario permite que resulten visibles al resto de usuarios, así como la creación de categorías de autorizaciones por ellos mismos sobre quién puede visionar sus perfiles. En este sentido, sugiere limitar el grado de publicidad del perfil del usuario conforme a los criterios anteriormente expuesto; limitar, de igual modo, la indexación de los perfiles por parte de los principales buscadores de Internet, limitar la visualización del perfil de manera geográfica, así como la cantidad de datos

617 Ib., pág., 116.

que los usuarios pueden introducir, ya que, por ejemplo, ciertas plataformas deciden operar con perfiles de nickname o seudónimo para que sean los propios usuarios los que consideren a quien mostrarse[618].

Tanto la Agencia Española de Protección de Datos como Inteco se encargan de dirigir una serie de recomendaciones y propuestas hacia la industria, comenzando por las redes sociales y plataformas colaboradoras[619].

Relaciona, también, una serie de recomendaciones y propuestas dirigidas directamente a los usuarios y asociaciones, para la preserva del derecho a la protección de datos personales, al honor, la intimidad y propia imagen.

Destaca la recomendación que se hace a todos los usuarios de servicios de redes sociales para que sean ellos mismos quiénes tienen el control respecto a la información y datos personales que desean publicar, por lo que el nivel de responsabilidad respecto de la publicación excesiva de información y datos puede implicar riesgos para su intimidad. El especial cuidado a la hora de publicar contenidos audiovisuales y gráficos en sus perfiles, dado que en este caso pueden estar poniendo en riesgo la privacidad e intimidad de personas de su entorno. Se recomienda, igualmente, entre otras cosas, no publicar en el perfil de usuario información de contacto físico, que permita a cualquier persona conocer dónde vive, dónde trabaja o estudia diariamente o los lugares de ocio que suele frecuentar[620].

9.4. Autoridades europeas y redes sociales.

Las autoridades europeas sobre protección de datos y privacidad dicta en octubre de 2008, como conclusión de la 30ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en la ciudad de Estrasburgo, una Resolución sobre protección de

618 Ib., pág., 120.

619 Ib., pág., 147.

620 Ib., pág., 165.

la privacidad en los servicios de redes sociales[621]. En la misma advierte que, aunque los servicios de redes sociales aportan un amplio abanico de oportunidades de comunicación, así como el intercambio en tiempo real de todo tipo de información, la utilización de estos servicios puede plantear riesgos para la privacidad de sus usuarios (y de terceras personas): los datos personales relativos a las personas son accesibles de forma pública y global, de una manera y en unas cantidades nunca sin precedentes, incluidas enormes cantidades de fotografías y vídeos digitales.

La Resolución de Estrasburgo establece una serie de recomendaciones en las que incide en: normas y reglamentos sobre privacidad; información sobre usuarios; control de usuarios; configuraciones por defecto que sean respetuosas con la privacidad; seguridad; derechos de acceso; eliminación de perfiles de usuarios; uso del servicio bajo un seudónimo; acceso de terceros e indexabilidad de perfiles de usuario[622]. Recomendaciones que son la base de lo aquí descrito anteriormente en este Capítulo.

Meses después, el Grupo de Trabajo de expertos comunitarios publica un Dictamen, el 5/2009, sobre redes sociales en línea[623]. En sus primeras líneas introduce que se centra en la forma en que el funcionamiento de los sitios de redes sociales cumple los requisitos de la legislación de la UE en materia de protección de datos, y que su objetivo principal es proporcionar orientaciones a los proveedores de SRS en cuanto a las medidas que deben establecerse para garantizar el cumplimiento del Derecho comunitario.

Aclara quién es el responsable del tratamiento de datos en una red social, al indicar que los proveedores de redes sociales son responsables del tratamiento de datos en virtud de la Directiva relativa a la protección de datos, y que proporcionan los medios que permiten tratar los datos de los usuarios, así como todos los servicios «básicos» vinculados a la gestión de los usuarios (por ejemplo, el registro y la supresión de cuentas).

Los proveedores de redes sociales determinan también la manera en que los datos de los usuarios pueden utilizarse con fines publicitarios o

621 Disponible en: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/internacional/common/30_conferen_inter/estrasb_resolucion_esp-sui.pdf>.

622 Ibídem, pág., 3.

623 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf>.

comerciales, incluida la publicidad proporcionada por terceros. Los proveedores de aplicaciones también pueden ser responsables del tratamiento de datos, si desarrollan aplicaciones que funcionan además de las de las redes sociales, y que los usuarios deciden utilizar.

El Dictamen 5/2009[624] relaciona derechos de los usuarios y las obligaciones para los responsables de redes sociales. Para éstos últimos, deja claro el hecho de que la norma europea relativa a la protección de datos se aplica generalmente al tratamiento de datos personales por las redes sociales, aunque su sede se encuentre fuera del territorio comunitario, y que los proveedores de redes sociales se consideran responsables del tratamiento de datos. Las redes sociales no entran en el ámbito de aplicación de la definición de los servicios de comunicaciones electrónicas, y, por tanto, la Directiva sobre conservación de datos no se les aplica[625].

Respecto a las obligaciones que se imponen a las redes sociales, destaca, entre las ocho que se establecen, el deber de informar a los usuarios de su identidad y proporcionarles información clara y completa sobre las finalidades y las distintas maneras en que van a tratar los datos personales, así como el deber de informar y advertir a sus usuarios frente a los riesgos de atentado a la intimidad cuando transfieren datos a las redes sociales.

Establece el Dictamen 5/2009 comunitario que, como mínimo, en la página inicial de la red social, debería figurar un enlace hacia una oficina de reclamaciones, tanto para miembros como para no miembros, que cubra cuestiones de protección de datos[626].

624 Ibídem.

625 Ib., pág., 13.

626 Ib., pág., 14.

10. PRIVACIDAD Y BUSCADORES CIBERNÉTICOS.

10.1. Aumento del riesgo de lo privado por buscadores y redes.

La relación cada vez más estrecha entre los Medios de Comunicación, Internet y las redes sociales ha hecho que se disparen los riesgos para mantener una adecuada protección de la privacidad de los ciudadanos. La dimensión de la privacidad, por tanto, ha cambiado. Para Carreras Serra, el concepto de privacidad, que inicialmente podía confundirse con el de intimidad, adquiere una dimensión mucho más amplia con la incorporación de la informática como técnica imprescindible en todos los ámbitos sociales y económicos de la vida moderna. Estamos ante un nuevo instrumento al servicio del progreso social que puede hacer evolucionar más aceleradamente nuestra civilización, pero en ningún caso debe modificar la concepción de la vida en libertad[627].

Daniel Solove, uno de los grandes especialistas internacionales en asuntos de privacidad, profesor en la Universidad estadounidense George Washington, se refiere no sólo a las noticias, sino también a los simples rumores o comentarios que se difunden en Internet, al afirmar que "*si los rumores son lo suficientemente morbosos, se pueden difundir de forma muy rápida. Y si se difunden, son muy difíciles de eliminar*". Para Solove,[628] el torrente de información libre de Internet "*puede dificultar la libertad y el desarrollo personales, a menos que se establezca un equilibrio entre derecho a la intimidad, libertad de expresión y derecho al anonimato, corremos el riesgo de que la libertad de Internet nos haga menos libres*", y sostiene que la naturaleza transnacional de Internet complica y dificulta el borrado de datos.

10.1.1. Por las redes sociales.

Uno de los problemas más recientes surgidos en 2011 ha sido la fuga de datos desde Facebook, una de las redes sociales que acumula mayor número de usuarios. La situación ha llevado a la Agencia Española de Protección de Datos a investigar si la popular red social ha vulnerado el

627 CARRERAS SERRA, Lluís. '*Las normas jurídicas de los periodistas'*. UOC, Barcelona, 2008, pág. 151.

628 SOLOVE, Daniel. '*El futuro de la reputación: cotilleos, rumores y privacidad en Internet*'. Caravan Book, Universidad de Yale, EEUU, 2007.

principio de seguridad de los datos de los usuarios españoles de esta plataforma como consecuencia de un agujero de seguridad que ha permitido a los anunciantes de Facebook acceder a perfiles, conversaciones, fotos y otros datos privados de los usuarios.

Ha sido a instancias de una petición cursada por la Federación de Consumidores en Acción, Facua, para que investigue la posible vulneración del principio de seguridad que recoge el art. 9 de la Ley Orgánica de Protección de Datos. Esta investigación supone una continuación de la que se inició en octubre de 2010[629], cuando se detectó que varias aplicaciones programadas sobre Facebook habían transmitido a anunciantes y otras empresas datos como los nombres de usuario y, en algunos casos, los de sus amigos. Entonces, y basándose también en las informaciones publicadas en los Medios de Comunicación, que apuntaban que la compañía "habría reconocido recientemente la difusión de datos como el identificador del usuario por problemas técnicos", la Agencia Española de Protección de Datos remitió a la red social un requerimiento para que informase, entre otras cuestiones, sobre si se habían visto afectados los usuarios españoles.

La denuncia de los consumidores se apoya en un informe de la empresa internacional de seguridad Symantec, publicado por el periódico estadounidense "The Wall Street Journal"[630], en el que se dice que algunas aplicaciones de Facebook han filtrado por error durante años códigos que permiten acceder a los perfiles, así como la lectura y escritura de mensajes e información personal, lo que evidencia un auténtico agujero de seguridad en la conocida plataforma de la red social.

10.1.2. Por los buscadores.

Eso en cuanto a las redes sociales, pero no menos grandes son los riesgos que para la privacidad han suscitado los buscadores. Entre ellos, el más popular, Google, que se está viendo obligado a cambiar su modus operandi a la hora de indexar datos personales.

---

[629] Petición en la denuncia de Facua, cursada en octubre de 2010. Véase en la propia web: <https://www.facua.org/es/noticia.php?Id=5361>.

[630] Disponible en la web del periódico estadounidense "*The Wall Street Journal*": <http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html?mod=WSJEUROPE_hpp_MIDDLETopStories>.

Ya en enero de 2011, la Agencia Española de Protección de Datos exigió a Google que procediera a retirar de sus resultados de búsqueda más de un centenar de artículos periodísticos considerados potencialmente difamatorios. Los contenidos afectan a distintas publicaciones online, incluidos contenidos de prensa. Entre los materiales se encuentran contenidos de periódicos como El País o referencias a informaciones de boletines oficiales. La Agencia Española entiende que los contenidos pueden ser difamatorios y solicitó su retirada de los resultados ofrecidos por Google[631].

Los responsables del buscador expresaron su disconformidad con la solicitud del órgano regulador de privacidad español y defiende su papel de intermediario. La compañía considera que no son responsables de los contenidos y que se vulnera la libertad de Internet con la demanda de la Agencia Española de Protección de Datos, argumentando que "*exigir que intermediarios como los motores de búsqueda censuren el material publicado por otros tiene un efecto profundo y negativo sobre la libertad de expresión y no proteger la privacidad de las personas*". El asunto quedó en la mesa de un tribunal de Madrid, aunque Google se niega a retirar los enlaces que le pide la Agencia Española de Protección de Datos[632].

Otro frente que ha tenido Google es el de los coches que realizan las rondas fotográficas del buscador por ciudades de todo el mundo para Street View, su callejero online, se han estrellado contra una barrera legislativa protectora de la privacidad de datos. Varios países europeos, entre ellos España, han abierto investigaciones para determinar hasta qué punto Google ha captado y almacenado datos de navegación procedentes de las redes wifi sin el consentimiento de los usuarios. Esta herramienta, que permite elaborar un servicio cartográfico con instantáneas reales, comenzó en 2008 y, desde entonces, las cámaras han barrido ochenta ciudades de toda Europa.

El buscador estadounidense ha admitido que los automóviles que rastrean las calles han recopilado datos de localización de las redes

631 "*Europa Press*". 'La Agencia de protección de datos solicita a Google la retirada de 100 artículos'. 17/01/2011, Madrid. Disponible en el portal de noticias de la Agencia: <http://www.europapress.es/portaltic/internet/noticia-agencia-proteccion-datos-solicita-google-retirada-100-articulos-20110117103700.html>.

632 'Google se niega a retirar los enlaces que le pide Protección de Datos', "*El País*", 12/06/2012. Disponible en la sección de noticias que éste periódico dedica a tecnología: <http://tecnologia.elpais.com/tecnologia/2012/06/18/actualidad/1339999915_714909.html>.

inalámbricas, como los relativos al identificador de la red -que suele coincidir con el nombre del abonado-, las direcciones MAC -grupo de números que identifican de forma individual cada dispositivo wifi- y datos de tráfico asociado a las redes wifi. Google ha llegado a insinuar que parte de esa información había sido recogida "*por error*".

Con todo, la Agencia Española de Protección de Datos ordenó en mayo de 2010[633] una investigación a fondo ante la posibilidad de que el buscador Google haya vulnerado la ley, e instó a la compañía a bloquear los datos de tráfico asociados a las redes wifi que están almacenados en sus archivos. La Agencia Española investigó por las ciudades rastreadas por los vehículos de Street View y el tipo de datos captados por la controvertida herramienta.

En términos similares se han dirigido a Google la autoridad de protección de datos de Alemania, que ha exigido al buscador que entregue los discos duros en los que se archiva esta información sensible. Reino Unido ha exigido que destruya los datos recogidos y las autoridades italianas han pedido explicaciones por el uso de los ficheros de navegación de sus ciudadanos. Y en nombre de la UE, la comisaria de Justicia, Viviane Reding, ha reclamado a Google que respete las leyes sobre privacidad que rigen en territorio la Unión Europea.

En su defensa, el presidente ejecutivo de Google, Eric Schmidt, admite el "*error*" cometido por los responsables de Street View y lamenta el "*perjuicio*" ocasionado a los usuarios, pero insiste en que los datos recogidos mediante los equipos técnicos instalados en los vehículos cámara no han sido utilizados por la empresa. Google dice estar muy preocupado por la protección de los datos personales, y explica su política de privacidad en una de sus secciones[634].

Los algoritmos que emplea Google para elaborar su lista de resultados cuando un internauta hace una petición de búsqueda están bajo sospecha. La UE coloca como uno de los puntos centrales de la investigación indagar si Google altera los algoritmos que administran la

633 La Agencia Española de Protección de Datos ordenó la investigación en mayo de 2010. Disponible en el apartado de su página web donde indexa sus notas de prensa: <https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/mayo/100519_NP_GOOGLE_WIFI_WEB.pdf>.

634 Véase: <http://www.google.es/jobs/privacy.html>.

ubicación de los enlaces en la primera página del buscador. Google Europa ha estado rechazando de plano mostrar los algoritmos, su secreto mejor guardado, a la Comisión Europea.

El problema de un buscador tan potente como Google y sus conflictos con la privacidad y el manejo de datos personales de sus millones de usuarios se escapa de su ámbito de control, porque también opera con aplicaciones como Gmail, YouTube, Buzz, Street View y otros tantos servicios que se basan precisamente en recolectar datos, hábitos de consumo y preferencias de los usuarios para hacer funcionar una inmensa máquina publicitaria que se lleva la mayor parte del pastel de los anuncios en Internet, lo que le está ya ocasionando denuncias en los juzgados. Alma Whitten, directora mundial de Privacidad de Google, defiende como un factor "*fundamental y crítico*" la protección de la privacidad, al afirmar que "*si la gente no se siente segura usando nuestros servicios dejará de utilizarlos y ese sería nuestro fin*", argumenta[635].

Asegura la máxima responsable de Privacidad de Google que los servicios del buscador y de sus usuarios están seguros "*dentro de lo razonablemente posible*". Afirma en su disertación que "*los datos de Google y los e-mail de nuestros ejecutivos tienen la misma protección que el correo de cualquier usuario de Gmail. Tenemos un sistema integral de protección interna. Lo primero que hacemos es cerciorarnos de que el número de personas que accede a esos datos sea tan pequeña como sea posible. En segundo lugar*, -señala- *controlamos que el uso de esos datos sea apropiado y, en caso, de no serlo sea intervenido rápidamente; y, por último, que todo el mundo que tenga acceso a datos delicados haya recibido la información adecuada y sea consciente del peligro de hacer un uso impropio de ellos*"[636].

Este trabajo de control es llevado a cabo por un equipo de seguridad interna. Se trata de uno de los cinco equipos que trabajan en el área de privacidad, que van desde la gestión del dashboard (panel de control) desde el que un usuario puede acceder a todos los datos que tiene de él Google (aunque no las cookies o aquellos datos internos que sirven de guía a los anunciantes), a los que desarrollan los nuevos servicios, al equipo jurídico y técnico que revisa que están de acuerdo con las normas de privacidad. Pese a ese control, reconoce fallos como el que le ha forzado a llegar a un

635 'Si los usuarios no se sienten seguros será nuestro fin',"*El País*", 02/12/2010, en: <http://elpais.com/diario/2010/12/02/sociedad/1291244402_850215.html>.

636 Ibídem.

acuerdo para cerrar la demanda judicial colectiva por Buzz, una especie de red social asociada a Gmail, que ha llegado a revelar datos sin conocimiento del usuario[637].

Uno de los últimos revuelos, en este sentido, ha sido el escándalo ocasionado en el verano de 2011, en pleno auge de los smartphones, al saberse que Google Maps almacenaba, trataba e incluso cedía a terceros los datos de localización de los terminales de iPhone (también de los iPad) con lo que permitía conocer y difundir a otros la posición casi exacta del ciudadano que posee el aparato.

En nuestro país, una resolución de la Agencia Española de Protección de Datos de marzo de 2011[638], estima que procede la eliminación de los datos personales de una mujer, que habían sido incluidos en un anuncio creado por Google Maps, al considerar que esta herramienta puede afectar a la privacidad de los particulares.

En concreto, un particular solicitó a Google la cancelación de sus datos personales que, según recoge la resolución que hizo pública la Agencia, aparecían vinculados a una agencia inmobiliaria en el servicio de mapas. Pero la empresa no respondió a la solicitud. El interesado acudió entonces, en septiembre de 2010, a la Agencia Española de Protección de Datos solicitando que este organismo se dirigiese a la empresa en su nombre.

Google manifestó que la empresa a la que correspondía reclamar era Google Inc (de Estados Unidos): "*Google Inc. es la única compañía de quien, en su caso, se podría exigir la eventual atención de cualquier derecho, quejas o sugerencias de las personas en relación con los servicios que presta*"[639].

La Agencia Española de Protección de Datos desestimó las alegaciones de Google porque entiende que la empresa "*opera en España mediante una oficina permanente*" y utiliza información (datos personales

637 Ibídem.

638 Resolución nº R/00508/2011 de la Agencia Española de Protección de Datos: <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-01257-2010_Resolucion-de-fecha-16-03-2011_Art-ii-culo-34-RD-1720-b-2007_Recurrida.pdf>.

639 Ibídem, pág. 3.

y direcciones postales) española para prestar el servicio de mapas de Google[640].

El supervisor español y Google mantienen abierta una contienda que ha ido creciendo en tensión en 2011 y 2012. De hecho, la compañía estadounidense ha llegado a lanzar todo un desafío ante las peticiones que le ha dirigido la Agencia Española de Protección de Datos exigiéndole, hasta en 18 resoluciones en sólo seis meses, que no difunda enlaces con datos sensibles. Google se niega a ocultar los datos personales objeto de reclamaciones esgrimiendo que sería censura.

En concreto, Google ha recibido entre julio y diciembre de 2011, 43 solicitudes de organismos gubernamentales, entre ellos la policía, para que eliminara hasta un total de 307 contenidos de sus servicios o resultados de búsqueda. Entre esas reclamaciones, las 14 peticiones de la Agencia de Protección de Datos para que retirase hasta 270 enlaces que, según Google, "*vinculan a blogs y medios de comunicación sobre individuos particulares y personajes públicos, como alcaldes y fiscales*"[641].

Google no retira los enlaces ni facilita más información sobre los blogs, Medios de Comunicación o personas afectadas. Un total de 18 de las solicitudes de retirada de datos personales acompañan requerimiento judicial. Hay también reclamaciones sobre vídeos de YouTube, sobre blogs, y sobre contenidos en Gmail. El buscador dice que ha retirado "*total o parcialmente el 37%*", según su Informe de Transparencia publicado a comienzos de junio de 2012[642].

Más polémica aún ha generado la nueva política de privacidad emprendida por Google, que puso en marcha a comienzos de 2012.

La Unión Europea ha abierto un expediente informativo, con carácter retroactivo, sobre el nuevo proceder del conocido buscador sobre los datos

640 Ib., pág. 17.

641 'Google desafía las peticiones para ocultar datos de España',"*El País*",18/06/2012: <http://tecnologia.elpais.com/tecnologia/2012/06/18/actualidad/1340029341_340406.html>.

642<http://www.google.com/transparencyreport/removals/government/ES/?p=2011-12>.

personales que recaba[643]. La nueva política consiste fundamentalmente en cruzar todos los datos que tiene Google sobre una persona, no sólo los obtenidos desde su buscador, sino también los que tiene por otros servicios, como las cuentas de correo Gmail, de su red social Google+ o de la videoteca YouTube.

Como ya hicieron Facebook[644] o Apple, Google defiende su nueva política de privacidad asegurando que es una mejora para el consumidor, pero los defensores de los derechos de las personas opinan lo contrario.

Para eliminar el histórico personal hay que ir a Google y buscar por Web history, o ir directamente a esta página. Una vez identificada la cuenta del correo Gmail, se entra en una página en inglés y da la opción de "remove", es decir, borrar, un enlace o varios, la actividad por días o como se prefiera. También hay un botón donde directamente se procede al borrado automático de todo el histórico. El mismo procedimiento podrán seguir aquellos interesados que tengan cuenta en YouTube y quieran borrar su histórico de vídeos vistos o emitidos.

En su página en castellano, Google avisa: "*Sin embargo, siguiendo la práctica habitual del sector y de acuerdo con los principios de la política de privacidad de Google, esta compañía mantiene un sistema de registro independiente destinado a tareas de auditoría y a la mejora de la calidad de los servicios que ofrece a los usuarios*". Posteriormente, ha expuesto en su página de política sobre privacidad que "*ha retirado más de 60 políticas de privacidad de los productos de Google para sustituirlas por una sola política mucho más concisa y fácil de leer. La nueva política y las nuevas condiciones reflejan nuestro deseo de ofrecer una experiencia más sencilla al usar nuestros productos*"[645].

---

643 'Europa investiga la privacidad de Google'. Artículo de Antonio García en: <http://www.csospain.es/Europa-investiga-la-privacidad-de-Google-/seccion-Actualidad/noticia-118303>.

644 La red social añadió en 2011 App Passwords y Trusted Friends, dos herramientas de seguridad que ha añadido Facebook para ayudar a sus usuarios a tener más control sobre sus cuentas, incluso que si se han visto comprometidas, y protegerse de aplicaciones maliciosas de terceros. Leer en: <http://www.itespresso.es/facebook-anade-herramientas-de-seguridad-que-impiden-el-hackeo-de-cuentas-55240.html>.

645 La nueva política de privacidad de Google, en vigor desde marzo de 2012: <http://www.google.es/intl/es/policies/>.

La nueva política de privacidad de Google es, como ha dicho la empresa, simplemente un cruce de los datos de los distintos servicios que tenía una persona. No significa que se recaben otros datos que no tenía la empresa, simplemente que va a poder juntarlos, mezclarlos y realizar minería de datos para sacarle un mayor provecho. Pese a todo, será la Unión Europea quien determine si infringe los derechos de sus ciudadanos.

Eli Pariser ex director ejecutivo de MoveOn.org, el grupo que pudo haber sido el primero que convirtió Internet en una herramienta para las acciones masivas políticas, sostiene que lo preocupante ahora es que la Red se haya vuelto muy polarizada, tanto en cuestiones políticas como en otros temas, debido a las herramientas utilizadas por las redes y Medios de Comunicación Sociales. En su libro '*El filtro de burbujas: lo que internet te oculta*', detalla la forma en que Facebook, Google, AOL y muchos otros personalizan la web para sus usuarios. "*La meta manifiesta es facilitar a los usuarios encontrar lo que les interesa en línea, pero el resultado final*", dice Pariser, "*es una silenciosa y sutil burbuja que aísla a los usuarios y les bloquea nuevos descubrimientos y opiniones que dejan de aparecen porque no responden a sus intereses y gustos habituales*"[646]. Y lo cierto es que hasta hace dos o tres años, cuando buscábamos algo con buscadores en Internet, se obtenían los mismos resultados que los demás. Ahora, nos aparecen cosas relacionadas directamente con uno mismo, con nuestras preferencias, nuestros intereses, e incluso con nuestra última ubicación.

10.2. El derecho al olvido.

Los buscadores convierten el pasado en un presente continuo. Lo cual ha dado lugar a una nueva demanda social, el derecho al olvido, o derecho de cancelación de datos online, que afecta a todo tipo de contenidos y sobre el que trabaja la Unión Europea para concretar una definición y plasmarlo en una norma.

Un ejemplo de lo común sobre el tipo de situación que ha de generar en un derecho ciudadano al olvido ayudará a clarificarlo. Una persona a quien se juzga o se multa en un momento dado genera una información asociada a este hecho que, según la relevancia alcanzada, puede publicarse en Medios de Comunicación, seguramente en periódicos, junto con los boletines oficiales correspondientes. El problema viene cuando estos datos

646 PARISER, Eli: '*Cuidado con la burbuja de filtros en la red*', en: <http://www.ted.com/talks/lang/es/eli_pariser_beware_online_filter_bubbles.html>.

permanecen asociados al nombre de la persona a lo largo del tiempo y aparecen al realizar una simple búsqueda de su nombre en Internet. El denominado derecho al olvido busca evitar estas situaciones.

Pero es esencial discernir qué tipo de información y, para el periodismo, si pueden permanecer las noticias en las hemerotecas de la prensa escrita o si es posible que desaparezcan de las ediciones digitales. Sobre todo, cuando la noticia, además de ser de interés público, es veraz y sobre ella pesa, por ejemplo, una sentencia judicial firme.

Marc Carrillo, catedrático de Derecho Constitucional de la Universidad Pompeu Fabra, explica que la pretensión de un particular de borrar los datos que hacen referencia a su persona en Internet "*es legítima en los casos en los que su aparición en la misma no ha sido por voluntad propia, sino como consecuencia de figurar en un archivo, público o privado, y el motivo de ello carezca de interés público*". Pero, a su vez, matiza que "*esta pretensión decae si, por ejemplo, el particular aparece en la Red como autor de un delito por el que fue condenado por sentencia firme (que ya no es susceptible de recurso). La comisión de un delito siempre es un hecho de interés público*"[647].

En Francia, un tribunal de Montpelier ha reconocido ya el derecho de una ciudadana francesa anónima a que su pasado sea borrado de Internet[648]. La demandante, Marie C., en la actualidad profesora, descubrió que al colocar su nombre o términos como "escuela de Laetitia" en Google, el buscador enviaba al internauta a sitios pornográficos donde se ofrecía un vídeo pornográfico de ella de aficionados. Algunos sitios aseguran que la demandante era en aquel entonces actriz porno "amateur". Tras un largo proceso de solicitudes de la afectada pidiendo al buscador que borrase dichos enlaces y, finalmente, un tribunal francés ha determinado que Google es responsable de un delito de invasión de la intimidad y le ha condenado a que borre cualquier rastro de su privacidad. La profesora exponía en la demanda que mostrar estos enlaces constituía un atentado a su vida privada, tratamiento ilícito de datos personales y un perjuicio a su imagen en la medida que sus alumnos, amigos o familiares podían conocer este episodio del pasado. Se trata, en definitiva, de reconocer el derecho al olvido, pese a que el tribunal rechace que se trate de una ofensa al derecho

647 CARRILLO, Marc: 'Quiero que Internet se olvide de mí'. "*El País*", 07/01/2011, en: <http://elpais.com/diario/2011/01/07/sociedad/1294354801_850215.html>.

648 Francia obliga a Google a cumplir con el derecho al olvido digital: <http://apcpd.blogspot.com.es/2011/03/francia-obliga-google-cumplir-con-el.html>.

a la propia imagen porque Google no es el editor de los sitios que publican el mencionado vídeo.

El posible vacío legal para dar cobertura a esta nueva necesidad ha extendido la preocupación, y la Agencia Española de Protección de Datos libra una batalla en los tribunales con Google España, con motivo de varias denuncias llegadas al organismo por parte de personas que quieren eliminar datos suyos publicados en Internet. Los mismos no están alojados en las páginas de Google, sino que gracias a los sofisticados algoritmos del buscador pueden localizarse de forma inmediata al teclear un internauta el nombre y apellidos de estas personas.

El conflicto consiste en que muchas personas consideran que se les perjudica cuando una noticia publicada en Medio de Comunicación, o bien un documento oficial del Boletín Oficial del Estado, o bien los datos sobre una sentencia ya cumplida, relacionados con su vida pasada, siguen presentes en Internet, aunque sus circunstancias hayan cambiado. Es decir, se hace referencia a un momento de su vida pasada, que puede afectar a su vida en el presente y en el futuro. Es lógico que muchas de estas personas soliciten la retirada del enlace, y que sus datos de carácter personal dejen de estar al alcance de cualquiera.

La Agencia Española de Protección de Datos tiene su enfoque sobre el problema, y afirma que estos datos no pueden borrarse de las fuentes donde se encuentran, como la hemeroteca de un periódico o un organismo oficial, ya que se altera el historial de estas fuentes y, en algunos casos, se atentaría contra la libertad de expresión. Según la Agencia, deben ser los buscadores como Google (aunque también las quejas afectan a Yahoo[649], Lycos[650], Altavista[651], Bing[652] y Terra[653]) los que deben dejar de presentar esos enlaces, ya que son los responsables de que estos documentos sean accesibles de forma rápida y sencilla, por no decir también universal, a lo largo del tiempo.

649 <http://es.yahoo.com/>.

650 <http://www.lycos.es/>.

651 <http://es.altavista.com/>.

652 <http://www.bing.com/>.

653 <http://www.terra.es/>.

Considera la Agencia Española de Protección de Datos que los motores de búsquedas no son una actividad amparada por la libertad de expresión y que, por tanto, deben atender a estas reclamaciones de cancelación y oposición de datos personales por parte de los usuarios. De igual forma, las informaciones públicas sobre ciudadanos anónimos que no tengan relevancia, y su disponibilidad en Internet, pueden complicar la vida a quienes quieran pasar página de un suceso puntual ocurrido en el pasado.

Por medio de diversas resoluciones, la Agencia Española de Protección de Datos ha venido a delimitar criterios para tutelar la procedencia del derecho de cancelación y oposición en servicios de búsqueda. En su mayor parte, las reclamaciones recibidas en este ámbito han tenido su origen en la indexación y recuperación por buscadores de Internet de datos personales contenidos en boletines oficiales y ediciones digitales de Medios de Comunicación. Se trata de situaciones en las que el responsable del sitio web se puede ver impedido a cesar en el tratamiento de los datos, en virtud de exigencia legal, o al encontrase amparado a mantener la información; obligación o amparo que, en todo caso, no es exigible o aplicable al responsable del servicio de búsqueda.

En estos casos, las resoluciones dictadas[654], cuando existen razones individuales y motivadas que lo justifiquen, y así lo ha estimado la Agencia Española, reconocen el derecho de los solicitantes, ordenando a los buscadores a adoptar medidas no sólo para cesar en el tratamiento de la información, sino también para impedir el acceso futuro a la misma a través de su servicio.

La fundamentación jurídica sobre la que se asientan dichas resoluciones[655] parte, de un lado, del sometimiento de los prestadores de estos servicios a la legislación nacional (aun encontrándose el responsable de tratamiento situado fuera del Espacio Económico Europeo, la legislación comunitaria se aplica cuando cuenta con un establecimiento en

654 Todas ellas disponibles en el canal de Resoluciones la Agencia Española de Protección de Datos. Destaca, por resumir sus criterios, la Resolución NºR/02245/2011: <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-00501-2011_Resolucion-de-fecha-27-10-2011_Art-ii-culo-16-LOPD_Recurrida.pdf>.

655 Como explica la Resolución Nº R/00355/2011: <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-01075-2010_Resolucion-de-fecha-07-03-2011_Art-ii-culo-16-LOPD_Recurrida.pdf>.

un Estado miembro o cuando acude a medios situados en éste), y de la ausencia de precepto legal o amparo constitucional a la permanencia de la información en los índices de búsqueda, ni en las páginas que buscadores conservan temporalmente en memoria 'caché'.

Cabe incidir en que en el caso de los buscadores no sólo es la normativa específica de protección de datos la que determina la ley nacional aplicable, sino que dicha normativa resultaría en todo caso aplicable por determinación del tenor literal de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI). Esta norma, que incluye a los buscadores dentro de la definición de 'Servicios de la Sociedad de la Información', establece que los servicios de búsqueda, como servicios de intermediación en los que el prestador del servicio no es, en principio, responsable de los contenidos informativos a los que facilita el acceso, debe eliminarlos o impedir dicho acceso a requerimiento de un órgano competente que cuestione su licitud[656].

Para el que fuera director de la Agencia entre 2007 y 2011, el Catedrático de Derecho Constitucional Artemi Rallo, se hace necesario insistir en los efectos divulgativos multiplicadores que se producen a través de los buscadores y su repercusión en la protección de datos de las personas. En este ámbito, y aun teniendo en consideración la necesaria ponderación de libertades y derechos que pueden entrar en juego, en ningún caso puede entenderse que la libertad de información impone que los datos personales de los posibles reclamantes, cuando concurran motivos fundados, figuren en los índices de los buscadores de Internet para facilitar a los usuarios el acceso a determinadas páginas[657].

Ha habido también que tener en cuenta las posibles acciones que los webmasters pudiesen adoptar encaminadas a hacer efectivo el derecho solicitado por el particular. De ahí que en la mayor parte de estas resoluciones de la Agencia Española de Protección de Datos se recomienda

[656] Resolución de la Agencia Española de Protección de Datos R/01509/2010: <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-00412-2010_Resolucion-de-fecha-16-07-2010_Art-ii-culo-16-LOPD.pdf>.

[657] RALLO, Artemi: '*El derecho al olvido y su protección*'. *Telos*. Madrid, diciembre 2010, disponible en la web de la Fundación Telefónica dedicada a Comunicación: <http://sociedadinformacion.fundacion.telefonica.com/seccion=1266&idioma=es_ES&id=2010110416500001&activo=6.do>.

a estas webs que arbitren las medidas necesarias con el fin de evitar la indexación de los datos del interesado e impedir que sean susceptibles de captación por los motores de búsqueda.

La cuestión que se plantea es si cabe entender la localización de páginas web y su indexación en un buscador de Internet como tratamiento de datos, una duda razonable que ha trasladado la Agencia Española de Protección de Datos a la Audiencia Nacional al recibir la queja de un centenar de particulares que, en 2011, consideraron que su intimidad fue vulnerada en el buscador Google porque sus datos personales se recogieron en sus resultados de búsquedas. En total, a mitad de 2011 había planteadas unas 250 demandas de cancelación de datos en España[658]. Lo que piden es, a fin de cuentas, garantizar su 'derecho al olvido', es decir, que se borre de los índices del buscador información personal que pretenden que desaparezca de Internet.

Las posiciones de las partes son frontalmente opuestas. Por un lado, Google alega que ni la Agencia Española de Protección de Datos ni los tribunales españoles tienen competencia para sancionar a esta compañía porque el almacenamiento de páginas web y su enlace es una actividad que se realiza en Estados Unidos. Mantiene, además, que la responsabilidad sobre la información y datos que publican las webs recae en los editores de las mismas y apela a la libertad de expresión: exigir a un motor de búsqueda que censure el material publicado por terceros atentaría contra este derecho fundamental.

La Agencia Española de Protección de Datos ha llegado a emitir un Informe Jurídico, el 0214/2010, al resolver una consulta que solicita conocer la postura de la Agencia respecto de las sanciones publicadas en los Boletines Oficiales de la Provincia, a las que acceden los buscadores, cuando las personas afectadas, solicitan que dicha información no sea accesible por Internet, otorgando la razón al ciudadano que se enfrenta a Google para que cancele sus datos[659].

---

658 'Un nuevo desafío: el derecho al olvido'. Defensora del Lector, "*El País*", 15/05/2011: <http://elpais.com/diario/2011/05/15/opinion/1305410404_850215.html>.

659 Informe Jurídico 0214/2010 de la Agencia Española de Protección de Datos: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdfs/2010-0214_Publicaci-oo-n-en-Diarios-Oficiales-de-las-notificaciones-y-su-indexaci-oo-n-en-los-motores-de-b-uu-squeda-en-Internet.pdf>.

Para Artemi Rallo, para clarificar la base de un derecho al olvido, es necesario hacer una ponderación de derechos y libertades. Expone que, partiendo del hecho de que la jurisprudencia del Tribunal Constitucional tiende a otorgar una posición preferente a la libertad de expresión frente a otros derechos constitucionales, "*siempre y cuando los hechos comunicados se consideren de relevancia pública (Sentencias del Tribunal Constitucional 105/1983 y 107/1988) y atendiendo a la veracidad de la información facilitada (sentencias del Tribunal Constitucional 6/1988, 105/1990 y 240/1992), la AEPD ha venido a considerar en varias de sus resoluciones que, aunque pudiera tratarse de una información veraz, al no referirse a asuntos públicos de interés general resulta preferente el derecho fundamental a la protección de datos*"[660].

Alude, además, al pronunciamiento en este sentido de la Sentencia de la Audiencia Nacional de 10/11/2006, recogiendo respecto de la libertad a la información veraz que "*ninguna objeción puede hacerse a la finalidad que persigue el derecho a la libertad de información veraz, pero dicho derecho fundamental no es un derecho absoluto, sino que hay que ponerlo en relación con otros derechos fundamentales, como lo es en este caso, el derecho fundamental a la protección de datos al que se refiere la STC 292/2000, de 30 de noviembre de 2000*"[661].

Por todo ello, Rallo recuerda que la Agencia Española de Protección de Datos ha venido a proclamar que ningún ciudadano que no goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la Red sin poder reaccionar ni corregir la inclusión ilegítima de los mismos en un sistema de comunicación universal como Internet[662].

Insiste, de esta manera, en defender el derecho de quienes solicitan la cancelación de referencias privadas en foros, blogs, redes y otros soportes de Internet que vulneren su dignidad personal.

La Audiencia Nacional, ante la avalancha de reclamaciones de ciudadanos que quieren borrar sus datos personales de Internet ha

660 RALLO, Artemi: '*El derecho al olvido y su protección*': op. cit.

661 Ibídem.

662 Ib., pág. 3.

enumerado una serie de dudas jurídicas que ha trasladado al Tribunal de Luxemburgo con la finalidad de determinar la actividad de los buscadores en Internet y su sometimiento a la normativa en materia de protección de datos[663].

La Audiencia quiere saber con determinación de la instancia jurídica superior comunitaria si las leyes que rigen en la UE se pueden aplicar en estos casos contra Google; si los buscadores, cuando indexan la información, están realizando un tratamiento de datos personales, y si la protección de datos incluye el derecho al olvido, es decir, si una persona se puede negar a que informaciones que le afectan (aunque sean lícitas y exactas) sean retiradas porque considere que son negativas o perjudiciales para su dignidad.

El Tribunal de Justicia de la Unión Europea de Luxemburgo debe tener la última palabra para determinar si Google realiza un tratamiento de datos a la hora de indexar páginas web y si los responsables de borrar esa información son las webs o el gigante mundial de los buscadores online. Su pronunciamiento vinculará a todos los juzgados de los Estados miembros de la UE[664].

El periodismo, en todo caso, no debe estar disgustado por la aparición de los buscadores de Internet, que han dado nueva visibilidad a noticias del pasado que, sin su mediación, quedarían escondidas en las hemerotecas. La Agencia Española de Protección de Datos considera que el primer responsable de suprimir o cancelar unos datos es el Medio de Comunicación que contiene la información (webmaster). Pero admite que ello no siempre es posible.

En el caso de los Medios de Comunicación, la supresión de noticias afectaría al derecho a la información. Modificar el contenido de la hemeroteca, sería falsear la historia, sostiene Gerardo Viada, responsable de los servicios jurídicos del diario "El País": "*El problema se ha creado con la aparición de buscadores. Son ellos los que dan acceso a unas*

[663] Comunicación de la Audiencia Nacional al Tribunal de Justicia de la Unión Europea realizada en marzo de 2012: <http://www.poderjudicial.es/portal/site/cgpj/menuitem.0cb0942ae6fbda1c1ef62232dc432ea0/?vgnextoid=a0cca049bd2d5310VgnVCM1000006f48ac0aRCRD&vgnextchannel=3a20f20408619210VgnVCM100000cb34e20aRCRD&vgnextfmt=default>.

[664] Véase el Anexo número 12 de esta Tesis.

informaciones que en nuestro caso solo son accesibles de forma directa para los suscriptores"[665]. Por eso, en los casos que afectan a los diarios, lo que se plantea no es suprimir la información publicada, sino impedir que sea visible a través de los buscadores de Internet. Y eso, técnicamente, pueden hacerlo tanto el medio como el buscador. Pero cada uno de ellos considera que es el otro quien debe resolver este problema.

En diversos casos planteados contra "El País" y contra Google, la Agencia Española de Protección de Datos ha desestimado la reclamación contra el diario y ha mantenido la dirigida contra el buscador.

En los Medios de Comunicación, la casuística que se da es bastante variada. Al menos son cuatro los supuestos susceptibles de reclamación, según explica Milagros Pérez Oliva, Defensora del Lector del diario "El País": "*1) Una noticia verídica sobre conductas o hechos considerados en su momento normales pero que han evolucionado hacia una percepción negativa. 2) Una noticia verídica relacionada con hechos delictivos que están probados. La permanencia en Internet de esta información sí plantea dificultades. 3) Una noticia verídica pero incompleta, bien porque no se han incluido todos los elementos, bien porque no se ha hecho el seguimiento adecuado. Suele ser el caso de personas imputadas en causas judiciales o administrativas y cuya resolución favorable no ha sido objeto de posterior información. 4) Una noticia falsa o errónea que en su momento no fue rectificada y que ahora vuelve, pero con un potencial daño o perjuicio*"[666].

En los dos primeros casos, se hace complicado que el derecho al olvido permita actuar sobre el Medio de Comunicación que contiene la información, debido, sobre todo, a que no puede hacerse responsable de un pasado que emerge. Planteamiento diferente para aquellas noticias ya publicadas que perjudiquen a un ciudadano resulten dañinas porque no se ha hecho el debido seguimiento o el desarrollo posterior de los hechos revela que eran inexactas. Ante esta nueva situación, como medida preventiva, el diario "El País" ha establecido el criterio de que en noticias sobre sucesos y procesos judiciales, se omita el nombre completo de las personas implicadas que no tengan relevancia pública, siempre que ese dato no sea necesario para la información.

---

665 'Un nuevo desafío: el derecho al olvido'. Defensora del Lector, "*El País*", 15/05/2011: op. cit.

666 Ibídem, pág. 1.

El problema está, fundamentalmente, en cómo actuar en el caso de las noticias ya publicadas. Podría darse una solución técnica, según la Defensora del Lector de este diario, consistente en aplicar herramientas como los "robots txt"[667], que hacen que la noticia sea invisible para los buscadores. El problema radica en qué criterios aplicar. Desde "El País", Gerardo Viada observa difícil poder atender estas demandas, al entender que "*resultaría enormemente complejo gestionar la avalancha de solicitudes que podría producirse y mucho más decidir en qué casos estaría justificado impedir la visibilidad y en cuáles no*".

Respecto de las noticias incompletas, los Medios de Comunicación podrían estudiar posibles medidas de autorregulación. Por ejemplo, habilitar un espacio en la edición digital en el que, previa demostración documental, se publicara una nota de la persona afectada comunicando el desenlace, por ejemplo, una sentencia absolutoria. Esa nota quedaría indexada y permitiría que cuando alguien buscase el nombre de esa persona, apareciera junto a la información.

Todo ello está por definir. El derecho al olvido supone un gran desafío para los Medios de Comunicación, pero también una oportunidad para demostrar su capacidad de adaptación a los nuevos tiempos.

10.3. Una nueva protección de la privacidad.

La UE trabaja en la introducción de importantes novedades en la normativa sobre protección de datos, en busca de una mayor protección de la privacidad y poner coto a la recolección y uso indiscriminado de datos personales en toda la Unión Europea. La norma contempla, para empezar, la obligación de las empresas de notificar las violaciones de datos graves en menos de 24 horas.

[667] El estándar de exclusión de robots, también conocido como el protocolo de la exclusión de robots o protocolo de robots.txt es un método para evitar que ciertos bots que analizan los sitios Web u otros robots que investigan todo o una parte del acceso de un sitio Web, público o privado, agreguen información innecesaria a los resultados de búsqueda. Según la definición de 'robots txt' que puede encontrarse en wikipedia: <http://es.wikipedia.org/wiki/Est%C3%A1ndar_de_exclusi%C3%B3n_de_robots>.

Ha sido la vicepresidenta de la Comisión Europea y responsable de la Agenda Digital, Viviane Reding, quien ha presentado en enero de 2012 la reforma general de las normas de protección de datos de la UE de 1995[668]. Esta nueva normativa nace con el objetivo "*de ampliar los derechos a la privacidad en línea e impulsar la economía digital europea*", destaca la Comisión Europea, quien a la hora de modificar la normativa ha considerado que "*el progreso tecnológico y la globalización han modificado profundamente las vías de obtención, acceso y utilización de los datos*". Además, "*los 27 Estados miembros de la UE han aplicado las normas de 1995 de manera diferente, lo que ha creado divergencias en cuanto a su ejecución y cumplimiento*"[669].

El hecho de que haya únicamente un marco legislativo hará que se suprima "*la fragmentación y las costosas cargas administrativas actuales, lo que generará un ahorro de unos dos mil millones de euros anuales. Esta iniciativa contribuirá a reforzar la confianza de los consumidores en los servicios en línea y, con ello, otorgará un impulso muy necesario al crecimiento, la creación de empleo y la innovación en Europa*", en opinión de la responsable comunitaria.

Según la argumentación de Viviane Reading, nos remontamos a unos 17 años atrás, apenas el 1 por ciento de los ciudadanos europeos empleaba Internet, y destaca que "*en nuestros días, se transfieren e intercambian enormes cantidades de datos personales entre continentes y de una punta a otra del mundo en fracciones de segundos. La protección de los datos personales es un derecho fundamental de todos los europeos, quienes, no obstante, a veces sienten que pierden el control sobre sus datos personales. Mis propuestas contribuirán a infundir confianza en los servicios en línea dado que los ciudadanos estarán mejor informados de sus derechos y tendrán un mayor control sobre la información que les atañe. La reforma perseguirá todos estos objetivos al tiempo que facilitará el funcionamiento de las empresas y les permitirá ahorrar costes. La existencia de un marco legal sólido, claro y uniforme a escala de la UE*

[668] Comunicado de la Comisión Europea por el que propone una reforma general de las normas de protección de datos para aumentar el control de los usuarios sobre sus propios datos y reducir los costes para las empresas. Disponible en la página europea: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=1&language=ES&guiLanguage=en>. Se adjunta texto íntegro en el Anexo número 13.

[669] Ibídem, pág. 2.

permitirá liberar el potencial del Mercado Único Digital y fomentar el crecimiento económico, la innovación y la creación de empleo"[670].

En el comunicado de la Comisión Europea de enero 2012 se resumen los cambios esenciales que introducirá la reforma, que pasan por imponer un conjunto único de normas sobre protección de datos válido en toda la UE que elimine trabas administrativas, lo que permitirá un ahorro cercano a los dos mil millones euros anuales, según los cálculos de las autoridades europeas. Además, la intensificación de la responsabilidad y la obligación de rendir cuentas de todos aquellos que procesen datos de carácter personal en territorio comunitario. Otra novedad que propone la reforma, es que los ciudadanos tendrán un acceso más fácil a sus propios datos y deberán poder transferir sus datos personales de un proveedor de servicios a otro con mayor facilidad. Como gran novedad, la Comisión Europea habla del 'derecho al olvido', para que los usuarios puedan borrar sus datos cuando no existan razones legítimas para conservarlos en Internet[671].

La normativa, que debe pasar por el Consejo Europeo y por el Parlamento, se aplicará a los 27 países pero también a todas las empresas que ofrezcan bienes y servicios a los consumidores europeos, lo que debe suponer que las grandes firmas que recojan datos en Europa deban responder ante el derecho europeo y las autoridades competentes europeas si vulneran las normas de protección de datos, y no escapen de la vigencia de nuestras leyes remitiendo a las del Estado de California (EE UU)[672].

En nuestro país, al igual que ha hecho para los conflictos surgidos en redes sociales, el Instituto Nacional de Tecnologías de la Comunicación, (Inteco), ha elaborado en septiembre de 2008 para los ciudadanos una guía con recomendaciones e información sobre la legalidad vigente dirigida a la protección del honor, la intimidad, y la propia imagen en Internet, haciendo una equivalencia entre la intimidad y la privacidad de las personas, recordando lo que el Tribunal Constitucional ha establecido al respecto.

---

670 Ib., pág. 2.

671 Ib., pág. 3.

672 Casi todas las grandes firmas que recaban datos, como Google, Facebook, Yahoo, etc., tiene su sede social en el Estado norteamericano de California y esgrimen estar sujetas exclusivamente a las leyes estadounidenses.

La guía[673] recoge un análisis exhaustivo sobre cómo actuar ante la publicación de una información o documento en Internet cuyo contenido atente contra el derecho a la intimidad y a la protección de datos de carácter personal de un usuario, conforme a lo dispuesto en la legislación vigente. Analiza, además, la responsabilidad de los proveedores de contenido y de acceso en el caso de una violación de dichos derechos, así como la identificación de los riesgos con los que se puede encontrar un usuario en lo relativo a su privacidad, honor y propia imagen en el empleo de las nuevas tecnologías.

[673] El Instituto Nacional de Tecnologías de la Comunicación la ofrece en su página web: <http://www.inteco.es/Seguridad/Observatorio/guias//guiaManual_honor_internet>.

11. SEGURIDAD NECESARIA EN INTERNET.

11.1. Internet y los datos personales.

La protección de datos personales y los Medios de Comunicación han de ir inevitablemente ligados a la nueva realidad, los nuevos peligros que se asume al abrirse al mundo de Internet y a las nuevas formas de comportamiento, tanto de usuarios, como de quienes ven una oportunidad de aprovechar para obtener beneficios legal o ilegalmente.

El problema de la seguridad se traduce en otro de confianza, y eso hace cuestionar mucho de lo que podemos hacer, a pesar de los avances tecnológicos. En una de las últimas reuniones del G-8, los líderes de los países más desarrollados del mundo han abogado por un Internet más "*civilizado*", según el entonces presidente francés Nicolás Sarkozy, que cumpla con la ley, mientras que responsables de empresas relevantes en Internet, como Mark Zuckerberg, de Facebook, y otros representantes de la Red debatían con pasión sobre el poder transformador de Internet y la necesidad de evitar su regulación en la cumbre que tuvo lugar en París en mayo de 2011[674].

Vittorio Colao, consejero delegado del grupo Vodafone, sostiene en un artículo publicado en "El País", que la visión de Mark Zuckerberg sobre un Internet sin restricciones es precisamente lo que nuestras sociedades necesitan para fomentar el espíritu emprendedor, el crecimiento y la innovación. Pero apunta que el presidente Sarkozy también podría estar en lo cierto cuando afirma que el éxito de todo lo que hacemos en Internet depende de que sepamos preservar el valor de la confianza. "*Si queremos que el comercio electrónico continúe creciendo y se sigan generando puestos de trabajo, necesitamos sentir que podemos confiar en las empresas que operan y que, en cualquier caso, estamos protegidos por la ley. Necesitamos sentir que se protege nuestra intimidad y que nuestros datos personales están seguros*", según Colao[675].

Para el consejero delegado de Vodafone, hay que estar convencidos de que nuestros hijos estarán a salvo en la Red. Los propietarios de

[674] Cumbre del G-8 de Internet celebrada en París en mayo de 2011: <http://es.euronews.com/2011/05/24/paris-acoge-el-g8-de-internet/>.

[675] ¿Es posible que tanto Sarkozy como Zuckerberg estén en lo cierto?, Vittorio Colao, "*El País*", Madrid, 6 de junio de 2011: <http://elpais.com/diario/2011/06/06/economia/1307311206_850215.html>.

contenidos tienen que saber que sus derechos de autor serán respetados y los Gobiernos deben ser capaces de garantizar la seguridad de sus ciudadanos y luchar contra la 'ciberdelincuencia'. Para todo ello es necesario que contemos con una serie de reglas, no para frenar el crecimiento de Internet, sino para asegurarnos que prospera sobre la base del respeto a la propiedad, la privacidad y los derechos humanos y sociales.

Los mayores peligros y riesgos para los datos personales tratados por los Medios de Comunicación vienen multiplicándose desde la inmersión de éstos en Internet y en su interacción con las redes sociales, cuyos problemas de seguridad y preserva de la privacidad están derivando en situaciones que ponen en jaque los derechos de los usuarios.

Uno de los nuevos problemas que se dan en Internet es la usurpación de identidad en las redes sociales, un fenómeno que se dispara. Entre 2010 y 2011, los robos de identidades vinculados a redes sociales han multiplicado por diez los casos registrados, según los datos procedentes de un estudio realizado en 2011 por Microsoft hecho sobre 600 millones de ordenadores en todo el mundo.

Bernard Ourghanlian, director técnico de seguridad de Microsoft, asegura que "*las redes sociales son una verdadera mina de datos y su éxito atrae a los cibercriminales*"[676].

Según el informe[677], hay dos tipos de atacantes: los profesionales pagados por mafias o agencias gubernamentales y los delincuentes individuales. Tanto las mafias como quienes operan con autonomía buscan recolectar datos personales con evidentes objetivos económicos. Por supuesto, destaca el fin de obtener las tarjetas de crédito para robar en las cuentas asociadas. En el caso del espionaje estatal, se trata de conocer la jerarquía de las amistades del personaje investigado. Otro fenómeno que ha crecido es el de la publicidad engañosa o maliciosa que, para llevar a cabo su cometido, propone falsas herramientas de seguridad.

El caso es que las redes sociales se han convertido en una puerta abierta a quienes se proponen robar datos de carácter personal. En 2011, un

[676] Disponible en el blog dedicado al marketing digital: <http//:www.iblog.cl>.

[677] 'La suplantación de identidad se dispara en las redes sociales', "*El País*", Barcelona, 12 de mayo de 2011. Disponible en la sección de Tecnología del diario: <http://tecnologia.elpais.com/tecnologia/2011/05/12/actualidad/1305190862_850215.html>.

error en la seguridad de la red Facebook, permitió que anunciantes pudieran acceder a datos personales de miles de usuarios. Una circunstancia que puede repetirse, teniendo en cuenta que , según un informe de "Symantec"[678], la arquitectura de Facebook, debido a un fallo, permite a distintos anunciantes tener acceso a perfiles, conversaciones, fotos y datos privados de los miembros de la red social, que acumula más datos de los que imaginamos.

Valga de ejemplo el caso de Max Schrems, un estudiante de 24 años residente en Viena, la capital de Austria, que a finales de 2011, amparándose en la legislación europea, envió un correo electrónico a Facebook solicitando que le hicieran llegar una copia de toda la información personal que tuvieran sobre él. La red social respondió afirmativamente a su reclamación y le remitió un CD con los datos que pedía. La sorpresa para este ciudadano llegó cuando al introducirlo en su ordenador descubrió la enormidad de detalles que la página conoce acerca de él[679].

El disco contenía hasta 1.222 archivos en formato PDF con las fechas y el contenido de los mensajes que había enviado y recibido, las personas, marcas y campañas a las que se había adherido, fotografías, direcciones de correo y un sinfín de detalles más que Facebook tiene sobre su persona y que puede utilizar, por ejemplo, para mostrarle anuncios que se ajusten más a sus intereses. Toda una serie de información que este estudiante pensaba que había eliminado hacía tiempo, pero que Facebook continuó manteniendo en sus servidores sin su permiso expreso con el objetivo, cabe suponer, de utilizarla cuando la red estimase oportuno para seguir engordando sus ya enormes cifras de ingresos[680].

Los robos de identidad online acaparan las denuncias de los usuarios. Durante los últimos años, esta tendencia se mantiene, confirmando el robo de identidad como uno de los problemas principales en la red.

---

678 Informe de Symantec sobre seguridad de mayo de 2011, en la web de la empresa: <http://www.symantec.com/connect/blogs/facebook-applications-accidentally-leaking-access-third-parties>,

679 Ver la noticia en: <http://www.abadiadigital.com/articulo/un-estudiante-austriaco-reclama-a-facebook-sus-datos-y-le-envian-1222-pdfs/>.

680 Ibídem.

Los internautas siguen sufriendo el robo de su identidad online año tras año. Los hackers suplantan las identidades para conseguir los datos personales, engañar a otros contactos o incluso realizar operaciones en nombre de los usuarios. Se trata de un problema contra el que se siguen buscando soluciones, pero que durante los últimos años ha supuesto el porcentaje más alto de denuncias de los usuarios.

En concreto, la Comisión Federal de Comercio de Estados Unidos[681] asegura que este tipo de denuncias de robo de identidad online ha acaparado el 15% de las reclamaciones de usuarios en 2011. En total se han contabilizado 1,8 millones de denuncias de este tipo, lo que ilustra la gravedad del problema y lo extendido que está.

Las empresas y servicios online tratan de buscar mecanismos de seguridad para evitar que los hackers consigan suplantar la identidad de los usuarios. Contraseñas más seguras, sistemas de geolocalización que confirmen la ubicación del usuario, avisos de actividad extraña e incluso sistemas de confirmación por reconocimiento de imagen.

11.2. Robo de datos personales.

Problemas de robo de información, cesiones de datos de personas sin su consentimiento y fallos en la seguridad de las plataformas online, que venían siendo casi anecdóticos, se han convertido en auténticas catástrofes para grandes gigantes tecnológicos por no haber tenido una buena previsión en su política de protección de datos.

El año 2011 ha sido el de los escándalos internacionales por robos masivos de datos de carácter personal sufridos por compañías tan conocidas como Sony, TomTom, y Microsoft como propietaria de Xbox.

El robo de datos de Sony, conocido en la primavera de 2011[682], ha llegado a ser de gran impacto para los defensores de la privacidad y los ciudadanos, usuarios en general. Sus plataformas de videojuegos online PlayStation Network y Sony Online Enterteinment (SOE) evidenciaron

681 Véase: < http://www.ftc.gov/bcp/edu/microsites/idtheft/en-espanol/index.html>.

682 'La frágil red de Sony permite el robo de un millón de datos', "*El País*", Barcelona, 4 de junio de 2011: <http://elpais.com/diario/2011/06/04/radiotv/1307138402_850215.html>.

carecer de las medidas de seguridad necesarias para evitar que terceros no autorizados accedieran a la base de datos de sus clientes, donde almacena desde contraseñas hasta datos bancarios. Según los cálculos, más de cien millones de clientes en todo el mundo, algunos de ellos españoles, se vieron afectados por el 'ciberataque'. Sony, que ha culpado al grupo Anonymous del ataque, afronta por ello una avalancha de demandas e investigaciones por parte de los organismos reguladores de la protección de datos en Europa. Francia y Reino Unido se pusieron rápidamente manos a la obra, mientras que la Agencia Española de Protección de Datos dijo que investigará si se ha vulnerado el principio de seguridad de datos recogido en la Ley Orgánica de Protección de Datos.

El robo de datos en TomTom[683]. El gigante de los servicios de navegación se ha visto obligado a pedir disculpas a sus clientes, después de que apareciera en la prensa una denuncia que lo acusaba de haber vendido los historiales de velocidad de sus usuarios a la policía holandesa para que sus agentes multaran a sus conductores. Sin embargo, TomTom ha asegurado que, fruto de un acuerdo, proporcionó los datos anonimizados de sus clientes al organismo holandés equivalente a la Dirección General de Tráfico. Argumentó que quería ayudar a localizar los tramos de carretera donde más se aumenta la velocidad para instalar radares. La compañía insistió en que, en ningún caso, estaba previsto que toda esa información se utilizara para imponer sanciones de tráfico y que la situación no se reprodujo en España.

El robo de datos en Xbox Live[684]. Los problemas de seguridad dieron lugar a que algunos usuarios del juego Modern Warfare recibieran mensajes de phising, que usan engaños para intentar recopilar información personal, principalmente datos bancarios. Microsoft, compañía propietaria de Xbox, aconsejó a sus clientes obviar los mensajes y que, en cumplimiento de su política de seguridad, dice que no solicita nunca nombres de usuario o contraseñas a través de correo electrónico, mensajería instantánea o por teléfono.

En España se da un curioso caso de una empresa que vende datos personales de hasta 36 millones de ciudadanos.

---

683 'TomTom vende datos del GPS a la policía que son usados para multar', véase en: <http://www.ticbeat.com/tecnologias/tomtom-vende-datos-gps-policia-usados-multar/>.

684 'Microsoft se suma a Sony y advierte un posible robo de datos en la Xbox', véase: <http://blog.segu-info.com.ar/2011/04/microsoft-se-suma-sony-y-alerta-de-un.html#axzz1L5KOqkip>.

Efectuando un previo pago de doscientos euros, cualquiera puede acceder a un archivo privado que tiene datos personales de 36 millones de personas residentes en España obtenidos sin su consentimiento del censo electoral y del padrón de municipios. Este archivo, que consta de una orden de inmovilización por parte de la Agencia Española de Protección de Datos y sobre el que pesan 3,5 millones de euros en sanciones, resulta útil, por ejemplo, para las empresas que se dedican al cobro de deudas, y más ahora cuando la crisis económica ha disparado la morosidad[685].

La empresa que vende datos actúa con un plan muy determinado, al observar que la localización de los deudores es uno de los principales escollos de quienes que se dedican el recobro de deudas. En el tiempo transcurrido desde la firma de un contrato hasta que se origina un impago, muchas personas se mudan, cambian de teléfono o se marchan de España. Para dar con un nuevo teléfono de contacto o con una nueva dirección, estas firmas pueden consultar legalmente los archivos públicos, como las guías telefónicas (Páginas Amarillas, Páginas Blancas, QDQ...), el Registro de la Propiedad y el Registro Mercantil.

Desde hace siete años, un ciudadano de Alicante, que tiene identificado la Agencia Española de Protección de Datos, ofrece una solución a todo el que quiera buscar a alguien y, a cambio de una tarifa unos euros, facilita acceso a un archivo que hasta hace poco se llamaba '*Saberlotodo.com*'[686].

Hasta la Agencia Española de Protección de Datos han llegado múltiples denuncias de personas que no se explican de dónde han obtenido sus datos ciertas empresas. Desde 2007[687], la Agencia Española ha abierto

685 'Una empresa vende ilegalmente datos de 36 millones de españoles', "*El País*". Madrid, 5 de abril de 2011: <http://elpais.com/diario/2011/04/05/sociedad/1301954404_850215.html>.

686 Ibídem.

687 La Resolución R/02070/201, del Procedimiento de la Agencia Española de Protección de Datos Nº PS/00146/2011 contra la entidad 'Saberlotodo Internet', resume los criterios para sancionar a la empresa. <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2011/common/pdfs/PS-00146-2011_Resolucion-de-fecha-21-09-2011_Art-ii-culo-37.1.f--LOPD_Recurrida.pdf>.

ocho procedimientos sancionadores contra '*Saberlotodo.com'* y le ha impuesto multas por valor de tres millones de euros por el tratamiento de datos personales sin consentimiento de los afectados y por su cesión a terceras entidades. Además, ha ordenado la inmovilización del fichero, que considera "ilegítimo". Lucas, que se presenta como investigador judicial y que ha trasladado su centro de operaciones a Suiza, ha recurrido estas resoluciones amparándose en un defecto formal: dice que las sanciones tendrían que ir dirigidas contra él mismo, propietario último del fichero, y no contra la empresa '*Saberlotodo*'. La Audiencia Nacional ha confirmado todas las sentencias dictadas por la Agencia Española de Protección de Datos. Y el respaldo ha llegado desde el Tribunal Supremo[688].

Escándalo más impactante ha sido el desmantelamiento en nuestro país, en junio de 2012, de la mayor red española que se dedicaba a recabar y vender datos personales a gran escala, practicando el espionaje en masa. La organización desmantelada por la Policía manejaba, de manera ilegal, declaraciones fiscales de renta, movimientos de cuentas bancarias, historiales médicos, listados de llamadas telefónicas e incluso controles de conversaciones ajenas. Miles de personas eran espiadas con la ayuda de funcionarios situados en zonas sensibles del Estado (Hacienda, Policía, Guardia Civil, Seguridad Social, Sanidad, Inem, Catastro, Tráfico, Registros de la Propiedad, juzgados...) y la de empleados de entidades financieras u operadores telefónicos. A la vista de la enorme cantidad de peticiones que los jefes de la red hacían a sus proveedores —a alguno le exigían 150 expedientes diarios—, se comprende que la policía hable de un tráfico "ingente"[689].

La red de tráfico de datos de carácter personal, desarticulada en la llamada Operación Pitiusa, que imputa a unas 150 personas, la mayoría detectives privados, ha llegado a contar entre sus colaboradores con personal de las compañías de telefonía móvil e intentaba penetrar en el personal de Visa. Un informe de la Unidad de Delincuencia Económica y Blanqueo de Capitales señala que los informantes de la trama "*se prestan a ello a cambio de sustanciales prestaciones económicas, que los peticionarios pagan gustosamente al tratarse de datos confidenciales de primera mano. Los clientes llegan a abonar hasta 30.000 euros por un*

688 Sentencia de Tribunal Supremo, Sala 3ª, de lo Contencioso-Administrativo, de 7 de Mayo de 2012.

689 'Espionaje en masa', Editorial de "*El País*", Madrid, 15 de julio de 2012. Véase: <http://elpais.com/elpais/2012/07/14/opinion/1342291051_771661.html>.

informe completo sobre la posición de una empresa concreta en el mercado"[690].

Internet forma parte ya del día a día de las empresas, incluidos los Medios de Comunicación, pero además de facilitar su funcionamiento, también supone numerosos desafíos para la seguridad de los datos de trabajadores, clientes y proveedores. La pérdida de ficheros de datos personales por robo o extravío puede acarrear diversos problemas, además de cuantiosas multas.

11.3. La Agencia Española de Protección de Datos y la Seguridad.

Con motivo de la celebración del Día Mundial de las Telecomunicaciones y Sociedad de la Información, también conocido como Día de Internet, una iniciativa que cada 7 de febrero, desde 2005, se propone dar a conocer las posibilidades que ofrecen las nuevas tecnologías para mejorar el nivel de vida de los ciudadanos, la Agencia Española de Protección de Datos lanza un llamamiento a los responsables de las empresas y organizaciones que prestan servicios a través de Internet para que adopten medidas urgentes de mejora de sus políticas de privacidad[691].

Muy sensible tras los sonoros casos de Sony, Microsoft y Facebook, la Agencia Española solicita, además, una diligencia mayor en la implantación de medidas de seguridad de los datos de sus usuarios.

En esa línea, la Agencia Española de Protección de Datos, reclama a empresas y organizaciones un compromiso decidido con la adopción de políticas que garanticen la privacidad de los usuarios y la seguridad de los datos en la red, y recuerda que "*la legislación impone obligaciones en materia de seguridad y confidencialidad de la información que las empresas deben respetar en los servicios prestados a través de Internet al igual que en el ámbito off-line*"[692].

---

690 'Espionaje ingente en las entrañas del Estado', "*El País*", Madrid, 13/07/2012, en: <http://politica.elpais.com/politica/2012/07/13/actualidad/1342214158_211012.html>.

691 Comunicado de la Agencia Española de Protección de Datos sobre la seguridad: <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2011/notas_prensa/common/mayo/100517NP_DIA_INTERNET.pdf>.

692 Ibídem, pág. 1.

La Agencia Española coincide, de igual modo, con las autoridades europeas en que el proceso de revisión de la Directiva de protección de datos de 1995, impulsado por Comisión Europea encaminado a adaptar sus disposiciones al mundo de las nuevas tecnologías, fija entre las prioridades y líneas maestras del futuro marco legal europeo, reforzar el control de los ciudadanos sobre los propios datos, e introducir nuevos principios, como la noción de privacidad desde el diseño o 'privacy by design'. Remarca el hecho de que se trata de un principio que "*exige la realización de un análisis escrupuloso de las implicaciones que un servicio de Internet -antes de ofrecerlo a los usuarios- tiene para la privacidad y la adopción de las medidas necesarias para garantizar la seguridad de los datos personales*"[693].

Se trata de ganar confianza ciudadana en la seguridad y privacidad en Internet. Para el supervisor español, la expansión de las aplicaciones tecnológicas requiere de garantías para los ciudadanos que disminuyan la desconfianza existente en la seguridad de la privacidad de Internet. En este sentido, se recuerda que los datos de la encuesta del CIS sobre privacidad y protección de datos realizada a finales de 2009, "*reflejaban una alta desconfianza de los ciudadanos sobre la seguridad y privacidad de Internet. Entre otros indicadores, esta encuesta destacaba que un 56,6% de los ciudadanos españoles consideraban que Internet ofrece una seguridad y privacidad de los datos baja, y más del 70% cree que su uso favorece la intromisión en la vida privada*"[694].

Coincidiendo con el Día de Internet, la Agencia Española de Protección de Datos incluyó un espacio en su página web ofreciendo contenidos de diversa índole relacionados con recomendaciones para quienes quieren darse de alta en servicios (como las redes sociales, portales de contactos o de compra on-line), sobre los problemas que puede generar nuestra navegación en Internet -como las Cookies-, u otros que pueden derivar en publicación de datos en sitios web sin nuestro conocimiento[695].

693 Ib., pág. 2.

694 Ib., pág. 2.

695 <https://www.agpd.es/portalwebAGPD/jornadas/dia_internet_2010/index-ides-idphp.php>.

Trata sobre los riesgos asociados a los servicios que se ofrecen en Internet, como correo Web, buscadores, redes P2P, chats o mensajería instantánea, aunque quizá el ejemplo más significativo es el de las redes sociales, cuyo auge ha provocado un nivel de divulgación de información personal sin precedentes, lo que aparte de ventajas, también entraña riesgos, sobre todo para el colectivo de menores. Por este motivo, la Agencia Española de Protección de Datos viene reiterando la necesidad de que los proveedores de servicios de Internet, como las redes sociales, se comprometan activamente para que la implantación de sistemas de verificación de la edad dejen de ser una asignatura pendiente en el campo de las plataformas sociales.

Ofrece, asimismo, un enlace desde el que se da acceso a guías con recomendaciones a usuarios de Internet, a menores, o sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales. Existe, no obstante, un enlace específico de recomendaciones que incide en la necesidad de crear una cultura para la protección de los datos de los ciudadanos en Internet, especialmente en entornos como las redes sociales. Incorpora también secciones con vídeos y enlaces a otras páginas de interés[696].

11.4. Guía de Inteco con recomendaciones sobre seguridad.

Consciente del aumento de los riesgos que su suceden en la actualidad sobre los datos de carácter personal, y teniendo en cuenta los avances tecnológicos, la cantidad de información que se genera y circula, y las posibilidades al alcance de cualquiera para recabar, copiar y difundir datos, el Instituto Nacional de Tecnologías de la Comunicación (Inteco) ha elaborado varias guías enfocadas directamente a los problemas relacionados con la seguridad, de igual modo que ha hecho con lo relacionado con las redes sociales y con la privacidad.

En concreto, ha realizado en 2011 una guía sobre el almacenamiento y borrado seguro de la información, en la que aborda la gestión del ciclo de vida de la información y el establecimiento de planes, normas y políticas de almacenamiento de la información y de seguridad de los datos, para asegurar un control y gestión de la información eficiente[697].

---

696 Ibídem.

697 <http://www.inteco.es/Seguridad/Observatorio/guias//guia_borrado_seguro>.

Esta guía de Inteco sobre almacenamiento y borrado seguro de datos aborda, entre otras cuestiones, los motivos por los que se debe controlar la información en la empresa, cómo se almacena dicha información en los dispositivos de almacenamiento más comunes, en qué consiste la recuperación en caso de pérdida y qué debe hacerse si se quiere eliminar de modo permanente la información.

Destaca, en este sentido, que una adecuada política de almacenamiento local de datos en los equipos de trabajo, ha de considerarse en la actualidad como una decisión clave en una empresa que quiera estar lo más próxima posible al cumplimiento de la legislación en materia de protección de datos personales y, de cara a evitar posibles sanciones, sugiere que deben establecerse varios modos de operar que considera vitales para llevar un correcto almacenamiento de información:

• Política de almacenamiento de datos.

• Política de recuperación ante pérdidas de información.

• Política de borrado seguro de datos[698].

En su treintena de páginas, esta guía sobre almacenamiento y borrado seguro de datos de Inteco ofrece claves y recomendaciones que resultan idóneas para cualquier Medio de Comunicación que quiera atender el marco legal en materia de protección de datos personales[699].

698 Ibídem, pág. 4.

699 Ib.

12. LOS CÓDIGOS TIPO Y SU VERTEBRACIÓN.

12.1. Hacia los Códigos Tipo. La buena práctica profesional.

Los Códigos Tipo han de constituir una solución de futuro en el tratamiento da datos. En una primera aproximación pueden ser definidos como Códigos Deontológicos, o bien de buena conducta o práctica profesionales. Están regulados en la Ley Orgánica de Protección de Datos de Carácter Personal, si bien sólo dedica a ello un único artículo, el 32[700]. Se trata de acercar posiciones entre las empresas que operan en mismo sector y que tratan mucho con datos personales.

No obstante, han sido objeto de preocupación posterior por parte de nuestro legislador y reciben la dedicación de hasta ocho artículos en el conocido Real Decreto1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)[701], y que define con detalle la naturaleza y objeto de los Códigos Tipo, su iniciativa y ámbito de aplicación, su contenido, los compromisos adicionales que ha de incluir, la garantía de su cumplimiento, la relación de adheridos, la inscripción o depósito y publicidad de lo que se acuerde y las obligaciones posteriores a la inscripción.

La anterior legislación, la Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD)[702], sólo admitió la posibilidad de que los Códigos Tipo pudieran formularse por responsables de ficheros de titularidad privada, quedando de esa manera excluida la posibilidad de que la autorregulación pudiera alcanzar el ámbito de las Administraciones Públicas en sus diferentes niveles organizativos. Fue la promulgación de la Ley Orgánica de Protección de Datos en 1999 la que vino a superar esa restricción que adolecía la LORTAD, admitiéndose

700 B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43094.

701 B.O.E., núm. 17, de 19/1/2008, op. cit., pág. 4124.

702 Ley Orgánica 5/1992, LORTAD, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, publicada en el BOE n. 262 de 31 de octubre de1992, y vigente en nuestro país por espacio de más de siete años, hasta la aprobación y publicación de la actual Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de diciembre.

por tanto desde entonces la formulación de Códigos Tipo en el sector público.

Como explica Javier Hernández Martínez[703], se desprende ya de lo que establece el artículo 32 de la LOPD[704], que estos acuerdos sectoriales o decisiones de empresa, hacen alusión a la política concreta de la compañía en cuanto a cómo llevará a cabo lo establecido por la ley, pero con el matiz de establecer en ellos un plus, o un esmero adicional a la hora de establecer dichas prácticas.

Por ejemplo, si la ley establece o prescribe determinada cautela, en el Código Tipo se incrementará ésta, por lo que el mismo representará un ánimo, por parte del suscriptor del código, de ir un poco más allá de la ley a la hora de respetar los derechos del ciudadano en lo relativo a sus datos de carácter personal.

De la lectura del artículo 32 de la LOPD se observa que contempla con un carácter abierto el contenido de los Códigos Tipo[705], los cuales pueden tener por objeto ampliar o simplemente facilitar el cumplimiento de las obligaciones establecidas en la normativa de protección de datos personales, incrementar las garantías de los ciudadanos, reforzar las estructuras organizativas y técnicas en el tratamiento de los datos y, especialmente, las medidas de seguridad, o bien contemplar procedimientos específicos para la tutela de los principios y derechos exigibles en esta materia.

Una vez elaborado el Código, hay que efectuar su inscripción en el Registro General de Protección de Datos, con sede en Madrid. Una vez llevado a cabo el depósito o inscripción, el Código será sometido a un examen cuya finalidad es que se ajuste a las disposiciones legales y reglamentarias relacionadas con el mismo, pudiéndose denegar su inscripción cuando se considere que no se da ese 'ajuste', ante lo cual, el Director de la Agencia de Protección de Datos requerirá al solicitante a fin de que subsane las deficiencias observadas.

---

703 HERNÁNDEZ MARTÍNEZ, Javier, especialista en Nuevas Tecnologías de la Información de la web: <http://www.proteccionlegal.com>.

704 B.O.E., núm. 298, de 14/12/1999, op. cit., pág. 43094.

705 ALMUZARA ALMAIDA, C.: op. cit., pág. 684.

Hay que dejar sentado que en las Comunidades Autónomas en las que hay Agencia autonómica de Protección de Datos, únicamente los casos de las de las Comunidades de Madrid[706], País Vasco[707] y Cataluña[708], habrá que, en su caso, llevar a cabo la inscripción en tales Agencias, o en los Registros correspondientes dependientes de las mismas, aunque como tales organismos sólo se encargan de lo referido a la Administración que esté bajo dicha Comunidad Autónoma, no influirán para nada para los Códigos de empresas, organismos o instituciones particulares, aunque sí, por el contrario, para aquellos referidos a la Administración autonómica, o local de cada una de esas Comunidades.

A la hora de manejar el hecho de la inscripción de los Códigos Tipo en el Registro General, la Agencia Española de Protección de Datos ha venido manteniendo un criterio bastante restrictivo, con matizaciones importantes, como puede deducirse de las aseveraciones deslizadas en algunas de sus Memorias Anuales. En el balance del año 1996, dijo la Agencia Española de Protección de Datos que revisaba su planteamiento inicial relativo a los Códigos Tipo, para afirmar que si en un principio admitía prácticamente sin objeción cualquier solicitud de inscripción, siempre que no se contraviniera ninguno de los mandatos contenidos en la Ley Orgánica 5/1992 (la vigente en 1996), "*ha parecido más conveniente, con posterioridad, no efectuar inscripciones de dicha naturaleza que no supongan un avance en materia de protección de datos, siquiera desde un determinado aspecto*"[709].

Tres años después, la Agencia Española de Protección de Datos señala en su Memoria anual que se abre a un criterio de flexibilidad más abierto, al referirse a las inscripciones de Códigos Tipo, si bien no deja de aclarar que la evaluación de los mismos debe estar presidida por un criterio de flexibilidad que permita apreciar las circunstancias concurrentes en cada caso concreto, De hecho, añade en ese balance anual de 1999 que la admisión de los Códigos Tipo dependerá del sector de actividad al que se refiera, pudiendo darse la circunstancia de que, en alguno de ellos, dada la

[706] Agencia madrileña de Protección de Datos: <http://www.madrid.org/cs/Satellite?language=es&pagename=PortalAPDCM%2FPage%2FPAPD_home>.

[707] Agencia vasca: <http://www.avpd.euskadi.net/s04-4319/es/>.

[708] Agencia catalana: <http://www.apd.cat/es>.

[709] Memoria de 1996 de la Agencia Española de Protección de Datos.

novedad de la propia normativa, la producción de un efecto pedagógico que facilite su cumplimiento pueda admitirse como un plus de efectividad. En todo caso, concluye la Agencia en esa Memoria de 1999, que "*el análisis de la aceptación de los Códigos Tipo deberá realizarse caso a caso con una valoración específica de las características del sector en el ámbito de la protección de datos*"[710].

Los Códigos Tipo no son obligatorios, y su carácter es deontológico, como expresa el art. 32.3 de la Ley Orgánica de Protección de Datos[711]. De ahí que la LOPD los contempla como algo de confección o elaboración voluntaria, puesto que para cumplir con los preceptos de la ley sólo hace falta respetar lo establecido en ella, pero permitiendo al que quiera elaborar dicho Código aplicar medidas que, respetando el espíritu y finalidad de la ley - preservar, entre otros, los derecho a la intimidad, el honor y a la propia imagen, en relación a su datos personales- traten de aplicar una defensa aún más estricta que la obligada por la ley.

De entre sus ventajas pueden destacarse las que se proyectan de cara al ciudadano, o al consumidor o potencial cliente, pues se le está dando la imagen de que el suscriptor del Código Tipo pone un interés o esmero especiales a la hora de respetar los derechos de los mismos contemplados en la ley. De igual manera, ante la propia Administración, esto es, ante la Agencia Española de Protección de Datos, pues dado que los Códigos han de inscribirse en el Registro General de Protección de Datos, previo examen de los mismos, estaremos ante un conjunto de normas que, si pasan dicho examen, tendrán el visto bueno de la Administración, con lo cual, si pasado el tiempo, la Agencia intenta sancionarnos por alguna práctica de protección de datos que considere ilegal, y esa práctica no se ha separado de lo establecido en el Código Tipo, estaremos actuando con ventaja, y ello es así puesto que la Administración no podría ir contra sus propios actos, o dicho de otra manera: si en su momento aprobó y autorizó ese Código, y ahora considera ilegal su materialización en la práctica, estaría contradiciéndose, incoherencia que iría a favor de quien suscribió el acuerdo entre empresas.

Según recoge Cristina Almuzara Almaida[712], los principios que han de informar y sustentar la elaboración de los Códigos Tipo y el contenido

---

710 Memoria de 1999 de la Agencia Española de Protección de Datos.

711 B.O.E., núm. 298, Madrid, 14/12/1999, op. cit., pág. 43094.

712 ALMUZARA ALMAIDA, Cristina: op., cit., pág. 686.

de los mismos fue objeto de atención en un documento que en junio de 1997 elaboró el Grupo de Trabajo de Expertos comunitarios, bajo el título de '*Primeras orientaciones sobre la transferencia de datos personales a países terceros. Posibles formar de evaluar la adecuación*'[713], en el que recogía además los requisitos de aplicación y de procedimiento, cuyo cumplimiento debería considerarse como un requisito mínimo para que la protección pueda estimarse eficaz.

1. "*Principio de limitación del propósito*". Es decir, deben tratarse los datos únicamente para el fin y el propósito del tratamiento.

2. "*La calidad de los datos y el principio de proporcionalidad*". Evitar que sean inexactos e imprecisos y sean, por tanto, reales.

3. "*El principio de transparencia*". Es decir, proporcionando siempre información sobre el destino de los datos, salvo unas excepciones, las únicas permitidas en este sentido, que deberán ser acordes con el artículo 11, apartado 2 y el artículo 13 de la Directiva 95/46, que establece las excepciones y limitaciones[714].

4. "*El principio de seguridad*". El control sobre los datos irá acompañado de la adopción de las medidas de seguridad técnicas y organizativas pertinentes.

5. "*Los derechos de acceso, rectificación y cancelación*". Que son los derechos básicos, junto al de oposición, que ostenta, en todo momento, el titular de los datos personales objeto del tratamiento.

6. "*Restricciones a las transferencias sucesivas a otros países terceros*". Sólo se permitirán cuando el segundo país tercero también garantice un nivel adecuado de protección. Las únicas excepciones deberán estar al tanto de lo recogido en el artículo 26 de la Directiva[715].

---

[713] Documento "*Primeras Orientaciones sobre las transferencias de datos personales a terceros países-Posibles formas de evaluar su adecuación*", adoptado por el Grupo de expertos del artículo 29 el 26 de junio de 1997. <http://www.informatica-juridica.com/anexos/anexo475.asp>

[714] Diario Oficial de las Comunidades Europeas, núm. 281, de 23 de noviembre de 1995, pág. 42.

[715] Ibídem, pág., 46.

En el mismo documento citado sobre '*Primeras orientaciones'*, elaborado por el Grupo de Trabajo del artículo 29, se reflejan los objetivos de un sistema de protección de datos, que son fundamentalmente tres:

- Conseguir un buen nivel de cumplimiento de las normas. "*Un buen sistema se caracteriza generalmente por un elevado nivel de concienciación entre los controladores y responsables de datos respecto de sus obligaciones y entre los sujetos titulares de los datos respecto de sus derechos y su forma de ejercicio. La existencia de sanciones que se hacen efectivas y que son disuasorias juega un papel importante para garantizar el respeto a las normas en este campo, así como los sistemas de comprobación directa por parte de las autoridades, auditores o funcionarios independientes responsables de la protección de datos."*

- Dar ayuda a los titulares de datos a la hora de ejercer sus derechos. "*Los titulares deberán ser capaces de ejercer sus derechos de forma rápida y eficaz, y sin costes prohibitivos. Para ello deberá existir algún tiempo de mecanismo institucional que permita una investigación independiente de las denuncias."*

- Permitir las condiciones para que se repare adecuadamente a los perjudicados de un incumplimiento de normativa. "*Esto constituye un elemento clave que debe contar con un sistema de arbitraje independiente que permita pagar una compensación e imponer sanciones cada vez que resulte oportuno*"[716].

12.1.1. Sobre cómo autorregularse.

Ante un panorama tan complejo y diverso, las empresas de mayor o menor tamaño que conformen un determinado sector pueden consensuar la autorregulación y el establecimiento de reglas comunes para tratar con datos de carácter personal.

[716] Documento "*Primeras Orientaciones sobre las transferencias de datos personales a terceros países-Posibles formas de evaluar su adecuación*", del Grupo de expertos del artículo 29 el 26 de junio de 1997. Pág., 3.

Cabe entender por Código de Autorregulación, para C. Almuzara, todo aquel "*conjunto de normas de protección de datos personales que se apliquen a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión*"[717]. Estamos relatando una definición en sentido amplio, que estaría abarcando desde un Código de protección de datos voluntario, desarrollado por una pequeña asociación industrial con pocos integrantes, "*hasta los detallados y minuciosos Códigos de Ética profesionales aplicables a sectores profesionales enteros, como puedan ser los conformados por médicos o banqueros, que suelen tener una fuerza casi jurídica*"[718].

El nivel de protección de datos personales de un determinado país puede verse acrecentado además de por las normas de Derecho, por las normas de autorregulación profesionales y sectoriales. En tal sentido, pueden considerarse los Códigos Tipo como un conjunto de normas de protección de datos de carácter personal aplicable a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado básicamente por los integrantes del sector industrial o profesional en cuestión.

Poder evaluar un Código Tipo y su eficacia es viable si tenemos en cuenta el plus de efectividad que su aprobación implica en relación con los principios fundamentales de la protección de datos.

12.1.2. Eficacia del Código Tipo.

El grado hasta el cual pueden hacerse cumplir las normas que contiene es un criterio de gran importancia para juzgar el auténtico valor de ese Código Tipo. Realmente, la cuestión de si la asociación u organismo responsable del Código acordado representa a todos los operadores del sector o únicamente a un pequeño porcentaje de éstos, carece de menor importancia que la fuerza de la asociación de empresas que lo conforman,

[717] ALMUZARA ALMAIDA, C.: op. cit., pág. 688.

[718] Ibídem, pág. 689.

en cuanto a su capacidad de, por ejemplo, imponer sanciones a sus miembros por incumplimiento de lo estipulado[719].

Se suceden diversas razones mas o menos secundarias, no obstante, que hacen que los Códigos Tipo que abarcan un sector industrial o una profesión sean instrumentos de protección bastante más útiles que los desarrollados por pequeñas agrupaciones de empresas dentro de un sector industrial.

En primer lugar, y según C. Almuzara, figura el hecho de que, "*desde el punto de vista del consumidor, resulta ciertamente confuso estar ante un sector empresarial fragmentado y caracterizado por asociaciones o agrupaciones que compiten entre sí y que son rivales, cada una con su propio Código para la protección de datos personales. La coexistencia de varios Códigos Tipo distintos llega a generar un panorama opaco para las personas cuyos datos personales sean objeto de manejo o tratamiento*"[720].

En segundo lugar, en sectores como el caso de las empresas dedicadas al marketing directo es muy frecuente y habitual transferir datos personales entre diferentes empresas y pueden darse situaciones en que la entidad transmisora no esté sujeta al mismo Código de protección de datos que la empresa que recibe esos datos. Lo que supone, para C. Almuzara, "*una gran y nada aconsejable ambigüedad en cuanto a la naturaleza y firmeza de las normas aplicables, como también puede llegar a dificultar en buen a medida la investigación y resolución de las denuncias de los interesados*"[721].

Evaluar la eficacia de un conjunto de reglas autoestablecidas resulta ser un ejercicio bien complicado. Lo fundamental es que se cumplan los tres criterios funcionales de eficacia de protección de los datos de carácter personal para considerar que un Código Tipo proporciona verdaderamente una seguridad adecuada. En resumen:

1. Un buen nivel de cumplimiento general.

2. Ayuda y apoyo a los titulares de los datos personales.

[719] Ib., pág. 689.

[720] Ib., pág. 689.

[721] Ib., pág. 690.

3. Reparación adecuada.

12.1.3. Elementos de su contenido.

La transparencia del Código Tipo es un elemento crucial, esencial. En concreto, deberá redactarse en lenguaje sencillo y ofrecer ejemplos específicos que ilustren sus disposiciones, como establece el art. 73 del Real Decreto 1720/2007[722].

Algo muy importante es que el Código Tipo deberá prohibir la comunicación de datos a empresas que no pertenezcan al sector y que no rijan por aquel, a menos que se prevean otras medidas adecuadas de protección.

Y lo más primordial, ha de garantizar que estén claramente presentes los principios de protección de datos de carácter personal que establece la legislación.

12.1.4. Criterios de la Agencia de Protección de Datos.

Para consolidar la mayor homogeneidad posible en el contenido de los Código Tipo que vayan a elaborarse e inscribirse por grupos de empresas para la defensa y protección de los derechos de los titulares de los datos personales, la Agencia Española de Protección de Datos ha ido asentando una serie de principios o reglas.

12.1.4.1. Criterios formales.

Son varios los criterios de carácter formal, entre los que destaca, en primer lugar, la necesidad de que la solicitud de inscripción de un Código Tipo deberá ajustarse a los requisitos establecidos en el Reglamento 1720/2007 de 21 diciembre de 2007, que desarrolla a la Ley de Protección de Datos de 1999 en sus arts. 73 a 78[723].

Cuestión importante es que, para formular un Código Tipo, es necesario que vaya precedido de documentación suficiente que acredite que el mismo se presenta mediante un acuerdo sectorial, o decisión de empresa,

[722] B.O.E., núm. 17, de 19/1/2008, op. cit., pág. 4124.

[723] Ibídem, págs. 4124 y 4125.

y debe ir con copia de los estatutos que regulen el marco jurídico de las entidades que agrupen a los responsables de ficheros o de los tratamientos de datos.

Describe C. Almuzara[724], que el Código Tipo deberá recoger el compromiso ineludible de sus integrantes adheridos de cumplir con los preceptos legales establecidos en la Ley de Protección de Datos.

12.1.4.2. Criterios de fondo.

Los criterios en cuyo contenido ha de reflejar de fondo el Código Tipo tienen, ante todo, uno que se hace indispensable, como es el de consignar las razones por las que han conducido a la elaboración e implementación de un Código Tipo, enumerando los valores añadidos que consiguen la aplicación y cumplimiento de las reglas.

Deberá señalarse el ámbito de aplicación del mismo, y se singularizarán los ficheros de datos que son objeto del Código Tipo, así como los datos personales a tratar. Identificará los posibles destinatarios de cesiones o transferencias internacionales, y las leyes o previsiones que las amparan en el sector. Ha de permitir, desde luego, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición en condiciones más favorables, estableciendo para ello el procedimiento correspondiente de manera sencilla[725].

Los ficheros que son objeto del Código Tipo deberán cumplir, de igual modo, las previsiones de los artículos 20 ó 26 de la LOPD, según se trate, respectivamente, de ficheros de titularidad pública o de titularidad privada[726].

Otro criterio de fono importante es que el conjunto de reglas deberá dedicar un espacio para las cláusulas informativas que, en cumplimiento del artículo 5 de la Ley de Protección de Datos[727], se introduzcan en los cuestionarios de recogida de los datos.

[724] ALMUZARA ALMAIDA, C.: op. cit., pág. 696.

[725] Ib., pág. 697.

[726] B.O.E., núm. 298, de 14/12/1999, op. cit., págs. 43092 y 43093.

[727] Ibídem, pág. 43089.

A efectos de seguridad, ha de pedir que se elabore un Documento de Seguridad con las medidas de salvaguarda de los datos, y las medidas técnicas adoptadas en relación a Internet: conexiones seguras; cookies y plugins[728]; y evitar grabar datos en páginas estáticas de Internet. Tiene que relacionar, por supuesto, la relación de adheridos.

12.1.5. Los Códigos Tipo en el ámbito comunitario.

A nivel comunitario, el seguimiento de los Códigos Tipo ha sido y es objeto de atención por parte del Grupo consultivo previsto en el artículo 29 de la Directiva 95/46/CE, que analizamos en siguientes capítulos de este estudio. La norma comunitaria los define, de manera general, para los Estados miembros, en su importante y aventurado artículo 27[729].

Este Grupo de autoridades y especialistas en materia de protección de datos en los países miembros de la Unión Europea ha ido emitiendo informes en forma de documentos que han ido jalonando la definición, sentido y finalidad de los Códigos Tipo.

El primer documento que emitió fue el llamado '*Primeras orientaciones sobre las transferencias de datos personales a terceros países-Posibles formas de evaluar su adecuación*'[730]. Un documento de debate adoptado en junio de 1997 y que un poco más tarde, en 1998, completa con uno sobre evaluación de la autorregulación industrial, al que agrega otro, llamado '*Labor futura en relación con los Códigos de conducta: documento de trabajo sobre el procedimiento de examen de los*

[728] Plugins, según la definición aceptada y publicada actualmente por Wikipedia, es una aplicación informática que interactúa con otra aplicación para aportarle una función o utilidad específica, como pueda ser la de servir como driver (controlador) en una aplicación, para que pueda funcionar un dispositivo en otro programa. Los plugins típicos tienen la función de reproducir determinados formatos de gráficos, reproducir datos multimedia, codificar/decodificar e-mails, filtrar imágenes de programas gráficos...etc. Actualmente se encuentran muy extendidos como una forma de expandir programas de forma modular, de manera que se puedan añadir nuevas funcionalidades sin afectar a las ya existentes ni complicar el desarrollo del programa principal. Muy utilizadas por los medios de comunicación en sus ediciones digitales.

[729] Diario Oficial de las Comunidades Europeas, núm. 281, de 23 de noviembre de 1995, pág. 47.

[730] Puede obtenerse el documento íntegro, junto a otros, en la siguiente web legislativa: <http://www.informatica-juridica.com/anexos/anexo475.asp>.

códigos de conducta comunitarios por el Grupo de Trabajo', aprobado el 10 de septiembre de 1998[731].

Es el documento de junio de 1997 el que constituye la pieza básica en lo relativo al contenido de los Códigos Tipo, y se erige en el punto de referencia de los documentos posteriores, que se remiten a él. Lo que hace es, con carácter breve, explicar los principios de contenido cuya inclusión en un Código Tipo se sugiere desde el Grupo de autoridades comunitarias. Distingue entre principios básicos, que comprende todas las categorías básicas de la normativa de protección de datos, y principios adicionales, que aluden a tipos específicos de tratamientos de naturaleza diversa.

El documento de 14 de enero de 1998[732] es más extenso y enfoca la evaluación de los Códigos Tipo desde una perspectiva distinta, a tal efecto, contiene una metodología de evaluación del Código distinguiendo entre la que tiene en cuenta el contenido y la que se centra en el análisis de su eficacia.

Respecto al documento emitido el 10 de septiembre de 1998[733], ofrece una perspectiva bastante diferente a los anteriores, pues se refiere exclusivamente a los procedimientos que deben seguirse para la presentación y evaluación de Códigos de conducta ante el Grupo del artículo 29 de la Directiva.

12.2. Códigos Tipo inscritos en el Registro General.

Los Códigos Tipo elaborados e inscritos oficialmente en el Registro de la Agencia Española de Protección de Datos y que, por tanto, operan en la actualidad en España. La página web de la Agencia Española los ofrece

[731] Documento adoptado en septiembre de 1998 a nivel comunitario: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp13_es.pdf>.

[732] Véase en: <http://www.informatica-juridica.com/anexos/anexo477.asp>.

[733] Labor futura en relación con los códigos de conducta: documento de trabajo sobre el procedimiento de examen de los códigos de conducta comunitarios por el Grupo de Trabajo.

en su integridad, e incluso agregando las resoluciones emitidas con los criterios seguidos y fundamentos de su aprobación[734].

Hay, en la actualidad, una docena de Códigos Tipo en nuestro país, entre los que cabe destacar el de Comercio Electrónico y Publicidad Interactiva (AUTOCONTROL[735]-AECE[736]-IAB SPAIN[737]), inscrito en noviembre de 2002 y modificado en 2005[738].

Hay inscritos, también, Códigos Tipo de sectores como la farmacia, médicos odontólogos y estomatólogos, hospitales regionales y de seguros del automóvil, entre otros.

12.3. Primeras propuestas en España. Lista Robinson.

La Asociación Española de la Economía Digital ha impulsado la puesta en marcha de una fórmula para, fundamentalmente, evitar la publicidad no deseada, denominada 'Lista Robinson'[739], que no es más que un servicio de exclusión publicitaria gestionado por la citada Asociación Española, creado conforme a lo previsto en la normativa reguladora de la Protección de Datos.

La idea, como reza en su presentación, se enmarca en el ámbito de la publicidad dirigida a nombre de una persona y a una dirección de correo

734 Canal de la Agencia Española de Protección de Datos dedicado a los Códigos Tipo: <https://www.agpd.es/portalweb/canaldocumentacion/codigos_tipo/index-ides-idphp.php>.

735 Asociación para la Autorregulación de la Comunicación Comercial. <http://www.autocontrol.es/>.

736 Asociación Española de Comercio Electrónico y de Marketing Relacional. <http://www.slideshare.net/aecem>.

737 Asociación que representa al sector de la publicidad en medios digitales en España. <http://www.iabspain.net/>.

738 Texto íntegro del Código Tipo de Comercio Electrónico y Publicidad Interactiva: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/common/pdfs/C-OO-DIGO-Comercio-Electr-oo-nico-y-Publicidad-Interactiva.pdf>.

739 Véase en la propia página web de la iniciativa Lista Robinson: <https://www.listarobinson.es/default.asp>.

postal, a una dirección de correo electrónico o a un número de teléfono concreto.

Lo que ofrece, es que cualquier ciudadano puede inscribirse en esa 'Lista Robinson', que es gratuita. Para ello es necesario precisar el medio a través del cual no desea recibir publicidad de entidades con las cuales no mantenga ni haya mantenido algún tipo de relación. De esta manera, las entidades deben consultar la 'Lista Robinson' para no enviar comunicaciones comerciales a aquellas personas inscritas en el servicio cuando lleven a cabo acciones publicitarias dirigidas a personas que no sean sus clientes, socios, usuarios, etc.

La Agencia Española de Protección de Datos ha acogido muy positivamente la propuesta respaldada por la Federación de Comercio Electrónico y Marketing Directo y ha saludado la iniciativa de impulsar este tipo de fichero de autoexclusión "*para que pueda ser un instrumento eficaz y actualizar y ampliar el servicio de Lista Robinson, como instrumento que facilite la aplicación del Reglamento. El resultado final del servicio merece una valoración positiva, que se confirmará con el uso que los ciudadanos y las empresas hagan de la nueva herramienta*"[740].

[740] Valoración de la Agencia Española de Protección de Datos hecha con motivo de la presentación, en junio de 2009, de la iniciativa Lista Robinson, véase en: <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2009/notas_prensa/common/julio/300609_np_listas_robinson_2.pdf>.

13. CONCLUSIONES.

1.

El derecho a la protección de nuestros datos personales, el habeas data, es un derecho fundamental, surgido como un derecho de nueva generación.

Las libertades consagradas entrañan nuevos riesgos para la esfera más íntima de las personas en el nuevo escenario de sociedad de la información y de mayor manejo de datos. La llamada libertad informática es el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.

Se construye así una nueva defensa de la intimidad de las personas, que resulta violada cuando datos referidos a ella son difundidos sin su autorización, pudiendo perjudicarla en su vida personal y social.

Una defensa de nuestros datos personales que no es pasiva, que implica no sólo el simple acceso a los mismos, sino su posible cancelación, rectificación y oposición a su tratamiento, según la voluntad y consentimiento del titular.

Este nuevo derecho debe ocupar y preocupar, sobre todo, a sectores profesionales que, por su actividad, manejan y tratan datos personales con asiduidad y en cantidad, como médicos, abogados, Administraciones Públicas y, especialmente, los Medios de Comunicación Social, tanto en sus ediciones tradicionales, como en sus ediciones digitales.

2.

La libertad de información prevalece sobre el derecho a la protección de datos personales.

El derecho a recibir libremente información veraz por cualquier medio de difusión prevalece frente a otros derechos constitucionales, tal y como ha establecido reiteradamente la jurisprudencia del Tribunal Constitucional, que reconoce esta posición preferente a la libertad de expresión siempre y cuando los hechos comunicados se consideren de relevancia pública y la información facilitada sea veraz.

En esa confrontación de derechos, el de la libertad de información, como regla general, debe prevalecer siempre que la información transmitida sea veraz, y esté referida a asuntos públicos que son de interés general por las materias a que se refieren y por las personas que en ellos intervienen, contribuyendo, en consecuencia, a la formación de la opinión pública, como sostiene el Constitucional.

Lo valora, de igual modo, la Directiva 95/46 CE al referirse, en su Considerando 37, al tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, señalando que "*deben preverse excepciones o restricciones de determinadas disposiciones de la Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones*".

La prevalencia de la libertad de información y de expresión sobre el derecho a la protección de datos es admitida también por la Agencia Española de Protección de Datos en Informes Jurídicos y Resoluciones.

3.

Los Medios de Comunicación deben conciliar, en mayor medida, el derecho a la libertad de información con la aplicación de los principios de protección de datos personales.

En primer lugar, debiera ponderarse escrupulosamente la relevancia pública de la identidad de las personas afectadas por el hecho noticiable para, en el caso de que no aporte información adicional, evitar la identificación mediante la supresión del nombre e incluso, si fuera necesario, de las iniciales y cualquier referencia suplementaria de la que pueda deducirse la identificación, en el caso de que el entorno sea limitado. Junto a ello, no cabe duda de que el desarrollo de Internet y la implantación generalizada de los motores de búsqueda suponen una actualización y divulgación exponencial y permanente de la información en prensa, así como de los datos personales incluidos en la misma como la identidad de las personas.

Los Medios de Comunicación han de considerar la trascendencia que tiene mantener de manera permanente una absoluta accesibilidad de los datos contenidos en noticias cuya relevancia informativa, probablemente, es inexistente en la actualidad. Y tener en cuenta la incidencia sobre la privacidad de las personas que puede derivar de ello.

En este sentido, los Medios de Comunicación podrían usar medidas tecnológicas idóneas para que se evite desde su web la indexación de la noticia por los motores de búsqueda en Internet. De esta forma, aún manteniéndola inalterable en su soporte, ya que no se borraría de sus archivos ni de sus históricos, se evitaría su divulgación indiscriminada, permanente y, en su caso, lesiva.

4.

Los buscadores que operan en Internet ofreciendo datos están sujetos a la Ley española y a la Normativa europea, a pesar de que tengan su sede social principal en Estados Unidos.

La cuestión no admite ya ningún tipo de duda jurídica, y ha sido ya analizada y resuelta por los Tribunales, como la Audiencia Provincial de Madrid, en su sentencia 95/2010, de 19 de febrero, cuyo fundamento jurídico tercero señala, en síntesis, respecto del ámbito territorial de la Ley 34/2002, que ésta es aplicable a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos, o bien en los supuestos en que el prestador de servicios opere mediante un establecimiento permanente situado en territorio español, cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad.

Idéntica aseveración recogen otras sentencias, que estiman acreditado el hecho de que Google, el principal buscador utilizado en nuestro país, opera en España mediante una oficina permanente a través de la cual realiza toda o parte de su actividad dirigida al mercado español. Dicha oficina permanente es Google Spain.

De ahí que Google (como el resto de buscadores) esté sujeto al cumplimiento de todo lo que prescribe la Ley española de Protección de Datos 15/1999 y la Directiva 95/46 CE, así como a toda la normativa estatal y comunitaria.

5.

El impacto negativo que puede provocar en un Medio de Comunicación Social tener que afrontar una sanción tan dura y elevada, motivo suficiente.

Las sanciones establecidas por incumplimientos, por su montante económico, no permiten que las empresas periodísticas puedan acostumbrarse con una actividad ajena al cumplimiento de la Ley de Protección de Datos.

Una ligereza costará muy caro, a tenor de las sanciones que contempla la LOPD, que en la práctica más habitual están siendo de decenas de miles de euros (pueden ser de hasta 600.000 euros las muy graves) por el sencillo hecho de no dar cabida a los derechos de acceso, cancelación, rectificación y oposición a las personas que entran en contacto o guardan alguna relación con el Medio de Comunicación.

No recabar el consentimiento del titular de los datos personales que se poseen derivará en infracción de la normativa española y, por tanto, la televisión, el periódico o la emisora de radio tendrá que atenerse a las consecuencias. Una de estas sanciones puede llegar a desbaratar la economía de una empresa periodística de ámbito local o provincial, es decir, la mayoría de los Medios de Comunicación.

6.

Los Medios de Comunicación con sede en Sevilla tienen declarados e inscritos una serie de ficheros que, en su mayoría, están relacionados con la gestión administrativa y económica del personal de cada empresa.

En pocos casos se constata la realización de ficheros con vinculación directa a la actividad explícita periodística, como puedan ser listado de fuentes de información y/o contactos, o fondos de archivos con entrevistas o testimonios que hayan sido noticia relevante, salvo algún caso excepcional.

Destacar, en tal sentido, el fichero inscrito por la Cadena de emisoras de Radio "Onda Cero" para la gestión de los fondos documentales informativos del Grupo para los programas radiofónicos con contenidos de carácter informativo, como lo más parecido a un fichero de naturaleza periodística. De igual modo, el inscrito por la "Radio Televisión de Andalucía" para la realización de programas de radio y televisión en base a la información recogida de diversos medios tanto propios como externos, tal y como tiene declarado ante la Agencia Española de Protección de Datos.

Lo más adaptado a la nueva dinámica en la que se ven inmersos los Medios de Comunicación al interactuar con lectores, oyentes y televidentes a través de Internet y del teléfono, son los ficheros para gestionar la participación en servicios, concursos, promociones, votaciones y juegos; así como la gestión de premios, publicidad y prospección comercial.

7.

Hacer una inversión no material, pero sí evaluable como auténtico valor añadido puede resultar mucho más importante para la empresa periodística que otras cuestiones.

El lanzamiento de un coleccionable, la venta de un producto, o la promoción de algún objeto para los lectores de un periódico, conlleva en muchos casos una inversión que se hace bastante rentable, desde el punto de vista económico, para el Medio de Comunicación, pero una descuidada política de privacidad y protección de datos personales puede derivar, a largo plazo, en una provisión de cautelas que, además de contar también con su cariz económico a tenor de las sanciones de la Ley de Protección de Datos, supone un verdadero valor añadido a la imagen de la firma.

Al margen del detalle económico, igual o más importante para la empresa periodística puede ser el hecho de ofrecer al ciudadano garantías y protección para sus datos personales, suficientes para dotar de una sensación de seguridad a su público y clientes.

Seguridad y protección, en un mundo lleno de las incertidumbres propias de unas comunicaciones sin fronteras, derivan en mayor confianza, ese valor tan determinante en el desarrollo empresarial de cualquier Medio de Comunicación.

8.

Un acuerdo sectorial para la política de protección de datos personales se hace necesario en la actualidad.

En el ámbito empresarial, donde se hallan irremediablemente inmersos los Medios de Comunicación Social, la solución a afrontar las obligaciones legales en esta materia puede ofrecerla el consenso en torno a unas normas de funcionamiento y comportamientos ante los datos personales, elaborando lo que se denomina un Código Tipo. Ha de constituir una gran solución de futuro.

Pueden ser concebidos como Códigos Deontológicos, o bien de buena conducta o práctica profesionales. Acordar una serie de reglas y cauciones para asegurar derechos y obligaciones de manera uniforme en las empresas periodísticas es hoy por hoy tan útil como necesario.

Buen ejemplo puede constituir el conformado por las empresas del sector de Comercio Electrónico y Publicidad Interactiva, para evitar las comunicaciones comerciales no deseadas, e inscrito formalmente en el Registro de la Agencia Española de Protección de Datos. Apostar por esta nueva cultura no debe demorarse y vendría muy bien a los Medios de Comunicación Social.

9.

Una tarea formativa adaptada a las nuevas necesidades empresariales y profesionales.

La formación entre el personal de las empresas periodísticas que concurren en esta dinámica de tratar con datos de carácter personal es otro factor que no puede eludirse ni demorarse por más tiempo.

Ofrecer y extender el conocimiento de la legislación en esta materia entre las personas que prestan servicios en los Medios de Comunicación de nuestro país es una manera interesante de ir alcanzando una correcta política de privacidad de la intimidad de los usuarios y clientes.

Eso irá permitiendo, además, consolidar una adecuada actuación y comportamiento del Medio de Comunicación de acuerdo con la legislación vigente y, sobre todo, en una mejor y más cuidada atención de los ciudadanos en general.

10.

El derecho al olvido digital se hace necesario, para que los ciudadanos puedan imponer su derecho al borrado de datos personales ante los grandes buscadores que operan en Internet.

El establecimiento del derecho al olvido digital se ha convertido en una necesidad imperiosa para amparar a los ciudadanos ante la divulgación de su identidad o de un hecho relacionado con su persona en ese universo sin fronteras que es Internet.

Se trataría de dar cobertura legal para que, cuando existan razones individuales y motivadas que lo justifiquen, esté reconocido el derecho de los solicitantes que reclaman el borrado de sus datos, ordenando a los buscadores que operan en Internet a adoptar medidas no sólo para cesar en el tratamiento de la información, sino también para impedir el acceso futuro a la misma a través de su servicio. El objetivo sería que puedan eliminarse de la memoria 'caché' de los servidores.

La idea ya la trabaja la Comisión Europea, que admite que ayudará a a los ciudadanos a gestionar mejor todos los riesgos inherentes a la protección de los datos en línea y podrán borrarlos cuando no existan razones legítimas para su conservación.

La Audiencia Nacional ya ha planteado el derecho al olvido ante el Tribunal de Justicia de la Unión Europea mediante una cuestión prejudicial. En Francia, un tribunal de Montpelier ha reconocido ya el derecho de una ciudadana francesa anónima a que su pasado sea borrado de Internet.

14. BIBLIOGRAFÍA.

14.1. Publicaciones unitarias.

14.1 .Impresas.

14.1.1. Libros.

ACED, Cristina: '*Redes sociales en una semana'*. Centro Libros PAPF. Planeta, Barcelona, 2010.

ALCINA FRANCH, J.: '*Aprender a investigar. Métodos de trabajo para la redacción de tesis doctorales. Humanidades y Ciencias Sociales*'. Compañía Literaria, Madrid, 1994.

ALMUZARA ALMAIDA, C. : (Coor.); '*Estudio Práctico sobre la Protección de Datos de Carácter Personal'*. Lex Nova, Valladolid, 2007.

APARICIO SALOM, J.: '*Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*'.Aranzadi, Elcano, Navarra, 2000.

ABAD AMORÓS, Mª. R.: '*La Protección de Datos Personales*' en '*Derecho de laInformación*'AA.VV. Ariel, Barcelona, 2003.

AA. VV.: *'Responsabilidades de los proveedores de información en Internet'*. Comares, Granada, 2007.

BAKER, Stephen: '*Numerati. Lo saben todo de ti*.' Seix Barral, Barcelona, 2009.

BERNAL, A.:'*Los nuevos medios de comunicación y los jóvenes. Aproximación a un modelo ideal de medio*'. Euroditions, Madrid, 2009.

CABRERA, M.A.: '*La prensa online. Los periódicos en la www*'. Cims, Barcelona, 2000.

CAMPUZANO TOMÉ, H.: '*Vida privada y datos personales*'. Tecnos, Madrid, 2000.

CARDOSO, Gustavo.: '*Los Medios en la sociedad en red*'. UOC, Barcelona, 2008.

CARRERAS SERRA, Lluís: '*Las normas jurídicas de los periodistas*'. UOC, Barcelona, 2008.

CASTAÑEDA GONZÁLEZ, A (Coor.): '*Guía práctica de Protección de Datos de Carácter Personal*. Ediciones Experiencia, Barcelona, 2002.

DAVARA RODRÍGUEZ, M.:'*La Protección de Datos en Europa. Principios, Derecho y Procedimiento*.' Grupo Asnef Equifaz. Universidad Pontificia Comillas, Madrid,1998.

DEL CASTILLO VAZQUEZ, Isabel-Cecilia: '*Protección de datos:cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*.' Thomson Civitas, Pamplona, 2007.

DESANTES GUANTER, J. Mª: '*Información y Derecho*'. Colección Actualidad e Información, Santiago de Compostela, 1990.

DESCARTES, R.: '*Discurso del método*'. Libsa, Madrid, 2001.

DRESNER. S. H. '*Panorama de la legislación europea sobre Protección de Datos Personales*'. Informática y Derecho. Números 6 y 7, 2001.

FROSINI V.: '*La protezione della riservatezza nella società informatica*'. Bolonia, 1981.

GARCÍA ESTÉVEZ, Noelia. '*Redes sociales en*

Internet' Editorial Universitas. Madrid , 2012.

HEREDERO HIGUERAS. M. '*La Directiva Comunitaria de Protección de Datos de Carácter Personal*'. Aranzadi. Pamplona, 1997.

JACQUÉ, Jean-Paul: '*Droit institutionnel de l'Union européenne*'. Dalloz, Parution, 2006.

LÓPEZ YEPES, J.: '*La aventura de la investigación científica. Guía del investigador y del director de investigación*'. Síntesis, Madrid, 1995.

MANSILLA ARCOS, P.: '*El Derecho de Información en la Directiva 95/46 sobre Protección de Datos y su aplicación al sector asegurador'*. Actualidad Informática. Aranzadi, núm. 25, octubre, 1997.

MAÑAN PÁEZ, J.: '*Derecho comunitario y nuevas tecnologías: Libro Verde y Directivas de bases de datos*'. Jornadas sobre el Marco Legal y Deontológico de la Informática', Mérida, septiembre, 1997.

MARÍA, Julían: '*Cara y cruz de la Electrónica*'. Espasa Calpe. Madrid, 1985.

MURILLO DE LA CUEVA, P.: '*Informática y Protección de Datos Personales*'. Centro de Estudios Constitucionales, Madrid, 1993.

MURILLO DE LA CUEVA, P.: '*Las funciones de la Agencia de Protección de Datos'*. Agencia Española de Protección de Datos, Madrid, 1996.

NAGEL, E: '*La estructura de la ciencia'*. Paidós, Barcelona, 1989.

PAREJO ALFONSO, L.: *Perfiles del derecho constitucional a la vida privada y familiar*. Cuadernos de Derecho Judicial, Consejo General

del Poder Judicial, Madrid, 1996.

PECES BARBA, G.: '*Derechos Fundamentales'*. Universidad Complutense, Facultad de Derecho, Madrid,1986.

PÉREZ LUÑO, A.E.: '*Encuentros sobre Informática y Derecho 1990-1991*'. Aranzadi, Pamplona, 1992.

PÉREZ MAÑA, Jorge: '*Bases de datos jurídicos. Características, contenido, desarrollo, marco legal*'. Centro Superior de Investigaciones Científicas, Madrid, 1994.

RAMÓN Y CAJAL, S.: '*Reglas y consejos sobre investigación científica. Los tónicos de la voluntad*'. Espasa Calpe, Madrid, 1991.

SALAVERRIA, Ramón: '*Cibermedios, el impacto de Internet en los Medios de Comunicación de España*'. Comunicación Social Ediciones y Publicaciones, Sevilla, 2005.

SANCHEZ BRAVO, A.: '*La protección del derecho A la libertad informática en la Unión Europea*'. Universidad de Sevilla, 1998.

SARABIA SÁNCHEZ, F. J. y otros: '*Metodología para la investigación en marketing y dirección de empresas*'. Pirámide, Madrid, 1999.

SIERRA BRAVO, R.: '*Tesis doctorales y trabajos de investigación científica. Metodología general de su elaboración y documentación*'. Paraninfo, Madrid, 1996.

SOLOVE, Daniel. '*El futuro de la reputación*: *cotilleos, rumores y privacidad en Internet*'. Caravan Book. Universidad de Yale, EEUU, 2007.

SUÑE LLINAS, Emilio: '*Tratado de Derecho Informático, Introducción y Protección de Datos*

personales'. Facultad de Derecho de la Universidad Complutense, Madrid., 2000.

VELEIRO, Belén: '*Protección de Datos de Carácter Personal y Sociedad de la Información*'. Estudios Jurídicos. Ministerio de la Presidencia, Madrid, 2008.

VIGURY PEREA, A.: '*Intimidad sobre Informática. La protección de datos personales: Perspectiva desde el Derecho comparado*'. La Ley, abril, 1999.

14.1.2. Cibernéticas.

14.1.2.1. Portales.

https://www.agpd.es/portalweb (Agencia Española de Protección de Datos)

http://www.borrmart.es/

https://www.camaras.org/publicado (Cámaras de Comercio españolas)

http://ec.europa.eu/justice_home/fsj/privacy

http://es.wikipedia.org/

http://eur-lex.europa.eu/LexUriServ

http://www.icemd.com (Instituto de Márketing Directo y Comercio Electrónico)

http://www.inteco.es (Instituto Nacional de Tecnologías de la Comunicación)

http://www.itu.int (Unión Internacional de Telecomunicaciones)

http:/www.legitec.com

http:/www.marsh.es

http://observatorio.inteco.es

http://www.proteccionlegal.com

http://www.samuelparra.com/protecciondedatos

http://xribas.typepad.com/xavier_ribas/2008/07

http://www.whitehouse.gov/sites/

14.2. Publicaciones periódicas.

14.2.1. Impresas.

14.2.1.1. Diarios.

“Abc”.

Agencia Europa Press.

Boletín Oficial del Estado (BOE).

“Cinco Dias”.

Diario Oficial de la Unión Europea **(**DOUE**)**.

Diario “La Ley”.

“El Economista”.

“El Mundo”.

“El País”.

"La Vanguardia".

14.2.1.1. Semanales.

Sunday Times, Serie A.

14.2.2. Cibernéticas.

14.2.2.1. Diarios.

www.elpais.com

www.elmundo.es

www.online.wsj.com

14.2.2.2. Ediciones no diarias.

Recomendación del Grupo Bangemann al Consejo Europeo, 26 de mayo de 1994.

15. ANEXOS.

ANEXO 1.

FALTAS LEVES, GRAVES Y MUY GRAVES

FALTAS LEVES

• No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

• No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

• No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

• Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la Ley Orgánica 15/1999.

• Incumplir el deber de secreto establecido en el artículo 10 de la Ley Orgánica 15/1999, salvo que constituya infracción grave.

FALTAS GRAVES

• Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "BOE" o Diario oficial correspondiente.

• Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

• Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

• Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la Ley Orgánica 15/1999 o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

• El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

• Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la Ley Orgánica 15/1999 ampara.

• La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

• Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

• No remitir a la Agencia de Protección de Datos las notificaciones previstas en la Ley Orgánica 15/1999 o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

• La obstrucción al ejercicio de la función inspectora.

• No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

• Incumplir el deber de información que se establece en los artículos 5, 28 y

29 de la Ley Orgánica 15/1999, cuando los datos hayan sido recabados de persona distinta del afectado

FALTAS MUY GRAVES

• La recogida de datos en forma engañosa y fraudulenta.

• La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

• Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

• No cesar en el uso legítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

• La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

• Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

• La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

• No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

• No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

ANEXO 2.

GUÍA PARA EL CIUDADANO SOBRE EL DERECHO A LA PROTECCIÓN DE DATOS

Coincidiendo, en enero de 2011, con la celebración del Día de la Protección de Datos en Europa, la Agencia Española ha publicado una Guía con información y consejos prácticos sobre el derecho fundamental a la protección de datos dirigida a los ciudadanos, que explica de forma simplificada cómo actuar cuando se solicitan nuestros datos personales, e ilustra sobre cómo defender nuestros derechos, pero también a aprender a usar y manejar de forma responsable los datos de otras personas.[741]

Bajo el epígrafe "Cuando me piden los datos", la Guía recoge, que cuando se solicitan datos de carácter personal a los ciudadanos, éstos tienen derecho a saber por qué, para qué y cómo van a ser recopilados sus datos personales y a decidir acerca de su uso. Igualmente, recuerda que con carácter general los datos personales sólo pueden recogerse y emplearse, salvo excepciones, si los ciudadanos han dado su consentimiento.

En el apartado "Cómo deben tratarse los datos", se recogen los principios que deben garantizar y respetar quienes recopilan y almacenan datos de los ciudadanos. En este sentido, la guía recuerda que sólo se podrán recopilar datos personales cuando éstos sean adecuados y no excesivos en relación con la finalidad para la que se obtienen; así como que la empresa, entidad u organización responsable de guardar los datos debe garantizar su seguridad y el secreto de los mismos.

La Guía destina un apartado a explicar los derechos que pueden ejercer los ciudadanos para controlar el uso que se hace de sus datos, es decir, de acceso, rectificación, cancelación y oposición. A renglón seguido, se responde a la pregunta "No han respetado mis derechos: ¿qué puedo

[741] El documento, compuesto por cincuenta y cuatro páginas, está disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO_OK.pdf>.

hacer?", donde se explica al ciudadano que puede solicitar la tutela de la Agencia Española si estos derechos no son respetados.

Aborda, asimismo, las posibles dudas de los ciudadanos sobre si pueden emplear datos de otras personas y qué hacer en estas situaciones. Por ejemplo, en el entorno de las redes sociales es muy común que tratemos información de familiares y amigos, e incluso de personas con las que no tenemos relación directa. En este sentido, se alerta de la existencia de riesgos que deben ser tenidos en cuenta, como resulta ser tan frecuente el hecho de publicar datos personales en Internet a disposición de cualquiera, que pueden escapar a nuestro control y ser muy difíciles de borrar posteriormente.

En el apartado "¿Qué cosas debo saber sobre algunos tratamientos de datos?", se incluyen reglas y consejos a tener en cuenta sobre los derechos de los ciudadanos en ámbitos concretos y generan mayores números de denuncias y reclamaciones de ciudadanos ante la Agencia Española, como son Internet, la recepción de publicidad o la inclusión en los comúnmente llamados ficheros de morosidad.

Respecto a los más jóvenes, se destacan los derechos y reglas existentes para proteger a colectivos sensibles como menores, como la necesidad de tener más de 14 años para poder registrarse en una red social, o la necesidad de contar con la autorización de los padres o tutores legales cuando no alcancen esta edad, son algunas de estas reglas.

Dentro de este apartado son relacionados los requisitos que deben respetarse para poder incluir los datos personales de deudores en ficheros de morosidad, uno de los ámbitos que genera mayor número de denuncias en la Agencia Española, como la necesidad de que la información contenida en dichos ficheros resulte veraz, adecuada y proporcional.

La Guía contiene, finalmente, un apartado con los siguientes consejos y recomendaciones:

- Los ciudadanos tienen derecho a que se les informe adecuadamente cuando una empresa, administración, o página web solicita y recoja sus datos. No deben olvidar leer esta información y muy especialmente las políticas de privacidad en Internet.

- Tienen la capacidad de decidir si otorgan su consentimiento cuando se vayan a usar sus datos; cuando no se puedan negar a facilitar sus datos personales tienen derecho a recibir información que explique el carácter obligatorio de esa solicitud.

- Los ciudadanos tienen derecho a que las entidades que utilicen sus datos los traten de forma adecuada, garantizando entre otros principios, que los datos se encuentren actualizados, que se utilicen sólo para las finalidades para las que fueron recogidos, así como la seguridad y el secreto.

- Tienen derecho a saber qué organizaciones han inscrito sus ficheros y los datos básicos sobre los mismos ante el Registro General de Protección de Datos.

- Los ciudadanos pueden controlar el uso que se hace de su información ejerciendo los derechos de acceso, rectificación, cancelación y oposición al tratamiento. Si estos derechos no son respetados puede solicitar la tutela de la Agencia Española de Protección de Datos.

- La primera garantía para la protección de tu derecho fundamental a la protección de datos depende de su propia conducta. Si facilita datos personales sin leer previamente la información sobre privacidad, si no aprende a configurar tu perfil en una red social, si expone información personal en Internet, se expones a riesgos.

- Debe respetar el derecho fundamental a la protección de datos de los demás y no publicar o tratar su información personal sin su consentimiento.

- Los niños son especialmente vulnerables respecto del tratamiento de sus datos. Es necesario formarles adecuadamente para que aprendan a proteger su privacidad y nunca debe confiarse en quienes no cumplan de modo riguroso con las normas específicas aplicables a los menores.

- En las redes sociales nuestra privacidad se encuentra particularmente expuesta debemos comprobar las condiciones de uso de cada red, aprender a configurar nuestro perfil y a actuar respetando los derechos de los demás.

- La información sobre solvencia es fundamental para el funcionamiento de la economía y para garantizar nuestra capacidad para contratar bienes y servicios. Por ello, se recomienda ser muy diligentes y asegurarnos al contratar que se garantizan nuestros derechos.

ANEXO 3.

FICHEROS DECLARADOS POR EL DIARIO "ABC" DE SEVILLA

Razón Social: ABC SEVILLA, S. L.

Nombre del fichero:
TOP TALENT.
Finalidad: INVENTARIO DIRECTIVO DEL GRUPO VOCENTO PARA FACILITAR LA GESTION DE RECURSOS HUMANOS.
Dirección:
CALLE ALBERT EINSTEIN (ISLA DE LA CARTUJA).
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
SUSCRIPTORES SEVILLA.
Finalidad:
SEGUIMIENTO Y CONTROL DE LOS SUSCRIPTORES FACTURACION ESTADISTICAS.
Dirección:
CL ALBERT EINSTEIN (ISLA DE LA CARTUJA).
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
RELACIONES EXTERNAS SEVILLA.
Finalidad:
LISTADO DE PERSONAS PARA REALIZAR INVITACIONES ACTOS REUNIONES ORGANIZADOS POR LA EMPRESA.
Dirección:
CL ALBERT EINSTEIN (ISLA DE LA CARTUJA).
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
PREVENCION RIESGOS LABORALES SEV.
Finalidad:
REGISTRO / CONTROL DE LAS PERSONAS Y EMPRESAS QUE PRESTAN SERVICIOS DE TIPO LABORAL EN NUESTRAS INSTALACIONES PARA PREVENCION DE RIESGOS LABORALES.
Dirección:
CL ALBERT EINSTEIN (ISLA DE LA CARTUJA).
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
PERSONAL SEVILLA.
Finalidad:
GESTION DE PERSONAL Y PAGO DE NOMINAS.
Dirección:
CALLE ALBERT EINSTEIN S/N (ISLA DE LA CARTUJA).
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
FORMACION PROFESIONAL SEVILLA.
Finalidad:
SEGUIMIENTO Y CONTROL DE LA ASISTENCIA DE LOS EMPLEADOS A LOS CURSOS ORGANIZADOS POR LA EMPRESA USO ESTADISTICO DE SEGUIMIENTO Y DE CONTROL.
Dirección:
CL ALBERT EINSTEIN (ISLA DE LA CARTUJA).
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
CONTROL DE PRESENCIA EN SEVILLA.
Finalidad:
CONTROL DE LAS PERSONAS QUE ACCEDEN A LAS INSTALACIONES DE LA EMPRESA.
Dirección:
CL ALBERT EINSTEIN (ISLA DE LA CARTUJA).
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
CONTROL DE ACCESO Y VIDEOVIGILANCIA EN SEVILLA.
Finalidad:
DATOS IDENTIFICATIVOS DE LAS PERSONAS QUE ACCEDEN AL EDIFICIO E IMAGENES DE SISTEMA DE VIGILANCIA.
Dirección:
CL ALBERT EINSTEIN (ISLA DE LA CARTUJA).
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
CLIENTES DE PUBLICIDAD SEVILLA.
Finalidad:
SEGUIMIENTO Y CONTROL DE LAS PERSONAS QUE HACEN ANUNCIOS EN PUBLICACIONES DE LA SOCIEDAD FACTURACION ESTADISTICAS.
Dirección:
CL ALBERT EINSTEIN (ISLA DE LA CARTUJA).
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
CLIENTES DE DISTRIBUCION SEVILLA.
Finalidad:
SEGUIMIENTO Y CONTROL DE LOS CLIENTES DE DISTRBUICION PUNTOS DE VENTA Y TRANSPORTISTAS DE PRENSA FACTURACION Y ESTADISTICAS.
Dirección:
CL ALBERT EINSTEIN (ISLA DE LA CARTUJA).
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
ACREEDORES Y DEUDORES SEVILLA.
Finalidad:
CONTROL DE LOS ACREEDORES/DEUDORES POR DISTINTOS CONCEPTOS DE LA SOCIEDAD VENTA DE PRODUCTOS ATIPICOS.
Dirección:
CL ALBERT EINSTEIN (ISLA DE LA CARTUJA).
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

ANEXO 4.

FICHEROS DECLARADOS POR EL DIARIO "EL CORREO DE ANDALUCÍA"

Razón Social: EL CORREO DE ANDALUCIA, S. L.

Nombre del fichero:
USUARIOS WEB.
Finalidad:
GESTION DE USUARIOS REGISTRADOS A TRAVES DE WEBSITE DE LA EMPRESA PARA LA PARTICIPACION EN CONCURSOS O PROMOCIONES Y SUSCRIPCION A BOLETINES.
Dirección:
AV. AMERICO VERSPUCIO, 39.
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
HEMEROTECA.
Finalidad:
BASE DE DATOS DOCUMENTAL PARA SU USO DENTRO DE LA ACTIVIDAD PERIODISTICA.
Dirección:
AV DE LA PRENSA 1.
Código Postal - Población:
41007-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
CONTROL HORARIO.
Finalidad:
CONTROL HORARIO DE LOS TRABAJADORES DE LA EMPRESA.
Dirección:
AV. AMERICO VESPUCIO 39.
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
SEGURIDAD.
Finalidad:
SEGURIDAD Y VIDEOVIGILANCIA DE LAS INSTALACIONES DE LA EMPRESA.
Dirección:
AV. AMERICO VESPUCIO 39.
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
TIENDA ON LINE.
Finalidad:
GESTION DE LAS RELACIONES COMERCIALES VIA WEB.
Dirección:
AV. AMERICO VESPUCIO, 39.
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
SUSCRIPCIONES.
Finalidad:
DATOS DESTINADOS A LA REALIZACION DE UNA GESTION INTEGRAL DE LOS SUSCRIPTORES INCLUYENDO EL COBRO Y DISTRIBUCION DEL PERIODICO ASI COMO EL ENVIO DE COMUNICACIONES COMERCIALES.
Dirección:
AV AMERICO VESPUCIO 39.
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
RECURSOS HUMANOS.
Finalidad:
GESTION INTEGRAL DE LOS RECURSOS HUMANOS DE LA EMPRESA.
Dirección:
AV AMERICO VESPUCIO 39.
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
CONTROL DE ACCESO AL EDIFICIO.
Finalidad:
REGISTRO DE LAS PERSONAS QUE ACCEDEN AL CENTRO DE TRABAJO CON EL FIN DE GARANTIZAR LA SEGURIDAD DE LAS DEPENDENCIAS DE LA EMPRESA.
Dirección:
AV AMERICO VESPUCIO 39.
Código Postal - Población:
41092-SEVILLA.
Provincia - País: SEVILLA-ESPAÑA.

Nombre del fichero:
CONTABILIDAD.
Finalidad:
GESTION CONTABLE Y ADMINISTRATIVA DE CLIENTES Y PROVEEDORES.
Dirección:
AV AMERICO VESPUCIO 39.
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
COLABORADORES.
Finalidad:
DATOS DESTINADOS A REALIZAR UN REGISTRO HISTORICO DE COLABORACIONES ASI COMO EL PAGO A LOS COLABORADORES.
Dirección:
AV AMERICO VESPUCIO 39.
Código Postal - Población:
41092-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
ANUNCIANTES.
Finalidad:
FICHERO DESTINADO AL ENVIO DE CORRESPONDENCIA Y MAILINGS INFORMATIVOS SOBRE ACCIONES EDITORIALES Y PUBLICITARIAS DEL PERIODICO.
Dirección:
AV AMERICO VESPUCIO 39.
Código Postal - Población:
41092-SEVILLA.
Provincia - País: SEVILLA-ESPAÑA.

ANEXO 5.

FICHEROS DECLARADOS POR EL "DIARIO DE SEVILLA"

Razón Social: JOLY DIGITAL, S. L. U.

Nombre del fichero:
ANUNCIANTES.
Finalidad:
GESTION DE CLIENTES (ANUNCIANTES).
Dirección:
CALLE RIOJA 14-16.
Código Postal - Población:
41001-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
CANDIDATOS.
Finalidad:
GESTION DE LA SELECCION DE PERSONAL.
Dirección:
CALLE RIOJA 14-16
Código Postal - Población:
41001-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
MARKETING.
Finalidad:
DATOS PERSONALES RECABADOS PARA LA REALIZACION Y GESTION DE CONCURSOS PROMOCIONES SORTEOS Y ANALOGOS.
Dirección:
CALLE RIOJA 14-16.
Código Postal - Población:
41001-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
NOMINAS PERSONAL Y RECURSOS HUMANOS
Finalidad:
GESTION DE NOMINAS RECURSOS HUMANOS PREVENCION DE RIESGOS LABORALES Y CONROL DE ACCESO A INSTALACIONES
Dirección:
CALLE RIOJA 14 16
Código Postal - Población:
41001-SEVILLA
Provincia - País: SEVILLA-ESPAÑA

Nombre del fichero:
PROVEEDORES.
Finalidad:
GESTION DE PROVEEDORES.
Dirección:
CALLE RIOJA 14-16.
Código Postal - Población:
41001-SEVILLA.
Provincia - País:
SEVILLA-ESPAÑA.

ANEXO 6.

FICHEROS INSCRITOS POR "RADIO NACIONAL DE ESPAÑA"

Razón Social: RADIO NACIONAL DE ESPAÑA, S.A.

Nombre del fichero:
AGENDARI.
Finalidad:
CONSULTA DE DATOS PARA LA LOCALIZACION DE INVITADOS PARA INTERVENCIONES EN PROGRAMAS RADIOFONICOS.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País: MADRID-ESPAÑA.

Nombre del fichero:
CERTIFICACIONES.
Finalidad:
CREACION MODIFICACION CONSULTA ELIMINACION E INFORMES DE LAS CERTIFICACIONES (DATOS GENERALES ECONOMICOS DE DESCUENTO ECONOMICOS RETRIBUTIVOS Y BAJAS DE SUSPENSION E I L T).
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28023-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
CONTRATOS.
Finalidad:
CREACION MODIFICACION QUE AFECTARA A LA VARIACION DE DATOS PROPIOS DE UN CONTRATO Y A LA CANCELACION Y APERTURA DE NUEVAS CONDICIONES CONSULTA ELIMINACION SUSPENSION DE CONTRATOS INDICANDO LAS CAUSAS DEL MISMO E INFORMES.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28023-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
DATA PERSONAL RNE.
Finalidad:
GESTION DE PERSONAL ELABORACION NOMINA BOLETIN COTIZACION A LA SEGURIDAD SOCIAL CERTIFICADO RENTA.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
NOMINAS.
Finalidad:
OBTENCION Y TRATAMIENTO DEL CALCULO DE NOMINA Y DESCUENTOS DE SEGURIDAD SOCIAL PARA LA POSTERIOR OBTENCION DE INFORMES RECIBOS TC1 TC2 TC4/5 CERTIFICADOS DE HACIENDA.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28023-MADRID.
Provincia - País: MADRID-ESPAÑA.

Nombre del fichero:
ORDENES VIAJES.
Finalidad:
CONTROL DE LOS VIAJES EFECTUADOS DE SUS PAGOS PETICIONES A AGENCIAS DE LOS DATOS ECONOMICOS QUE SE ENVIAN A CONTABILIDAD Y DE JUSTIFICACION AUSENCIAS EMISION DE INFORMES Y ESTADISTICAS.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28023-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
PERSONAL COLABORADOR.
Finalidad:
CONOCIMIENTO ACTUALIZADO DE LOS DATOS DE AQUELLOS COLABORADORES QUE VIAJEN CAPTURA A TRAVES DE LA MATRICULA.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
PERSONAL DATA.
Finalidad:
CONOCIMIENTO ACTUALIZADO DE LOS DATOS PERSONALES DE AQUELLAS PERSONAS SUSCEPTIBLES DE VIAJAR CAPTURA AUTOMATICA A TRAVES DE LA MATRICULA.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28223-POZUELO DE ALARCON.

Nombre del fichero:
PRODATA0.
Finalidad:
PROMOCION INTERNA DEL PERSONAL POR CAMBIO DE CATEGORIAS LABORALES.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
PROINST0.
Finalidad:
VALIDACION DE LA OPCION DE PROMOCION RECOJE PUNTUACIONES ACTUALIZA MARCA DE PROMOCIONADOS INFORMES Y ESTADISTICAS.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
REPRESENTANTES.
Finalidad:
CONSTITUCION Y MANTENIMIENTO DE LOS DATOS IDENTIFICATIVOS DE REPRESENTANTES PARA EL POSTERIOR CALCULO DE NOMINA DE SUS REPRESENTADOS Y OBTENCION DE INFORMES.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28023-POZUELO DE ALARCON.
Provincia - País: MADRID-ESPAÑA.

Nombre del fichero:
RESUMEN Y EMISORAS.
Finalidad:
CONTROL CONJUNTO VIAJES SERV CENTR Y EMISORAS ESTIMACIONES CONTABLES ANTICIPADAS Y EMISION DE INFORMES.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28023-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
RNE DEANOM.
Finalidad:
DETERMINACION DE LA PLANTILLA DE NOMINA (FIJOS+CONTRATADOS) DE RNE MENSUALMENTE OBTENCION DEL LIBRO DE INFORME.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
RNE PLAPER.
Finalidad:
DETERMINAR LA PLANTILLA (FIJOS+CONTRATADOS)DE RNE MENSUALMENTE OBTENCION DEL LIBRO DE INFORME(DISTRIBUCION DE PLANTILLA SEGUN SU SITUACION EN LA EMPRESA LISTADOS DE ALTAS BAJAS Y MODIFICACIONES).
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28223-POZUELO DE ALARCON.

Nombre del fichero:
RNE CCOO TXT.
Finalidad:
CONOCIMIENTO CUOTAS COTIZADAS DE LAS PERSONAS DE RNE AFILIADAS A CC OO.
Dirección:
PRADO DEL REY S/N.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
SUSRACLA.
Finalidad:
DISTRIBUCION DE LA REVISTA DE PROGRAMACION DE RADIO CLASICA LA 2 DE RNE A LOS SUSCRIPTORES QUE LO HAN SOLICITADO.
Dirección:
CL PRADO DEL REY S/N.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
AFILIADOS AL GRUPO DE EMPRESA RNE.
Finalidad:
GESTION DE LA PERTENENCIA Y ACTIVIDADES DE LA ASOCIACION.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:MADRID-ESPAÑA.

Nombre del fichero:
ATENCION MEDICA.
Finalidad:
GESTION DE LA ATENCION MEDICA Y DE LA SALUD DEL PERSONAL DE LA EMPRESA Y BENEFICIARIOS.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
BANCO DE DATOS.
Finalidad:
GESTION DE PUESTOS DE TRABAJO VACANTES CON PERSONAS QUE HAN REALIZADO PRACTICAS O PRUEBAS ESPECIFICAS EN LA EMPRESA.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
BASE EXTERNA DE CANDIDATOS Y ASPIRANTES.
Finalidad:
GESTION DEL PROCESO DE SELECCION DE PERSONAL PARA CATEGORIAS NO ACOGIDAS AL CONVENIO COLECTIVO Y NO PRESENTES EN EL BANCO DE DATOS DE SELECCION DE CONTRATACION.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
BECARIOS.
Finalidad:
GESTION Y CONTROL DE LOS ESTUDIANTES QUE REALIZAN PRACTICAS EN RNE.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
BENEFICIARIOS.
Finalidad:
GESTION Y CONTRO DE LAS AYUDAS Y PRESTACIONES GRACIABLES QUE SE OTORGAN POR PARTE DEL GRUPO RTVE A TRABAJADORES Y OTROS COLECTIVOS.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
CLIENTES.
Finalidad:
GESTION Y MANTENIMIENTO DE LA RELACION CON CLIENTES.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
CLIENTES Y PROVEEDORES POTENCIALES.
Finalidad:
CAPTACION DE CLIENTES Y EVALUACION DE PROVEEDORES CON LOS QUE NO SE TIENE UNA RELACION CONTRACTUAL PERO QUE SE CONSIDERAN A EFECTOS DE FUTURAS TRANSACCIONES.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
COLABORADORES Y ARTISTAS.
Finalidad:
GESTION Y DESARROLLO DE LA RELACION ENTRE LOS COLABORADORES Y ARTISTAS Y LA CORPORACION RADIO TELEVISION ESPAÑOLA INCLUYENDO LA GESTION DE NOMINAS.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
EMPLEADOS.
Finalidad:
GESTION DEL PERSONAL FIJO Y CONTRATADO ADSCRITO A RNE GESTION DE NOMINAS FORMACION DEL PERSONAL PRESTACIONES SOCIALES PROMOCION Y GESTION DEL EMPLEO CONTROL HORARIO GESTION DE FONDOS DE PENSIONES.
Dirección: AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.

Nombre del fichero:
OYENTES.
Finalidad:
GESTION DE LAS RECLAMACIONES Y PREGUNTAS DE LOS OYENTES DE LOS DISTINTOS PROGRAMAS DE RADIO.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
PREVENCION LABORAL.
Finalidad:
EVALUACION DE LOS RIESGOS A LOS QUE ESTAN SOMETIDOS LOS TRABAJADORES COMO CONSECUENCIA DEL PUESTO Y EL LUGAR DE TRABAJAO EN CUMPLIMIENTO DE LA NORMATIVA DE PREVENCION DE RIESGOS LABORALES.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
PROVEEDORES.
Finalidad:
GESTION Y MANTENIMIENTO DE LA RELACION CONTRACTUAL CON LOS PROVEDORES DE RNE.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
RECLAMACIONES JUDICIALES LABORALES.
Finalidad:
GESTION Y SEGUIMIENTO DE LAS RECLAMACIONES LABORALES REALIZADAS EN VIA JUDICIAL.
Dirección:
AVENIDA RADIO TELEVISION, 4.
Código Postal - Población:
28223-POZUELO DE ALARCON.
Provincia - País:
MADRID-ESPAÑA.

ANEXO 7.

FICHEROS DECLARADOS POR LA "CADENA SER"

Razón Social: SOCIEDAD DE SERVICIOS RADIOFONICOS UNION RADIO, S. A.

Nombre del fichero:
SERVICIO MEDICO Y DE PREVENCION.
Finalidad:
CONTROL Y GESTION DE LA SALUD DE LOS TRABAJADORES Y DEL RIESGO LABORAL DE SU PUESTO DE TRABAJO OBTENCION DE ESTADISTICAS DIVERSAS.
Dirección:
C/ GRAN VIA, 32.
Código Postal - Población:
28013-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Razón Social: SOCIEDAD ESPAÑOLA DE RADIODIFUSION, S. L.

Nombre del fichero:
CMD.
Finalidad:
CENTRALIZAR LAS BASES DE DATOS DEL GRUPO PRISA; ENVIO DE INFORMACION COMERCIAL.
Dirección:
C/ GRAN VIA, 32.
Código Postal - Población:
28013-MADRID.
Provincia - País: MADRID-ESPAÑA.

Nombre del fichero:
PREVENCION DE RIESGOS LABORALES.
Finalidad:
CONTROL Y GESTION DE LA SALUD DE LOS TRABAJADORES Y DEL RIESGO LABORAL DE SU PUESTO DE TRABAJO.
Dirección:
C/ GRAN VIA, 32.
Código Postal - Población:
28013-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Razón Social: PRISA RADIO, S. L.

Nombre del fichero:
CONTABILIDAD.
Finalidad:
GESTION ECONOMICA CONTABLE FISCAL ADMINISTRATIVA DE CLIENTES COBROS Y PAGOS AL IGUAL QUE SERVIR DE HISTORICO DE RELACIONES COMERCIALES.
Dirección:
C/ GRAN VIA, 32.
Código Postal - Población:
28013-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
PREVENCION DE RIESGOS LABORALES
Finalidad:
CONTROL Y GESTION DE LA SALUD DE LOS TRABAJADORES Y DEL RIESGO LABORAL DE SU PUESTO DE TRABAJO
Dirección:
C/ GRAN VIA 32 8
Código Postal - Población:
28013-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
RECURSOS HUMANOS.
Finalidad:
GESTION DEL PERSONAL CONTROL Y ASIGNACION DE PUESTOS DE TRABAJO PROMOCION GESTION DE LAS NOMINAS Y SELECCION DE CANDIDATOS.
Dirección:
C/ GRAN VIA, 32.
Código Postal - Población:
28013-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
SEGURIDAD.
Finalidad:
CONTROL DE SERVICIOS DE SEGURIDAD DE LA EMPRESA GESTION DE INCIDENCIAS CONTROL DE ACCESOS DE INSTALACIONES.
Dirección:
C/ GRAN VIA, 32.
Código Postal - Población:
28013-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Razón Social: COMUNICACION RADIOFONICA, S. A.

Nombre del fichero:
COLABORADORES Y AGENTES.
Finalidad:
EL FICHERO SE UTILIZA PARA EL CONTROL Y MANTENIMIENTO DE LAS COMPRAS A PROVEEDORES Y DE LAS COLABORACIONES RECIBIDAS.
Dirección:
C/ GRAN VIA, 32.
Código Postal - Población: 8013-MADRID.

Nombre del fichero:
CONTABILIDAD.
Finalidad:
GESTION COMERCIAL Y DE LOS COBROS Y PAGOS CORRESPONDENCIA VARIA OBTENCION DE ESTADISTICAS DIVERSAS.
Dirección:
C/ GRAN VIA, 32.
Código Postal - Población:
28013-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Razón Social: ANTENA 3 DE RADIO, S. A.

Nombre del fichero:
CONCURSOS.
Finalidad:
GESTION DE SORTEOS PROMOCIONES Y CONCURSOS.
Dirección:
C/ GRAN VIA, 32.
Código Postal - Población:
28013-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
PREVENCION DE RIESGOS LABORALES.
Finalidad:
CONTROL Y GESTION DE LA SALUD DE LOS TRABAJADORES Y DEL RIESGO LABORAL DE SU PUESTO DE TRABAJO.
Dirección:
C/ GRAN VIA, 32.
Código Postal - Población:
28013-MADRID
Provincia - País:
MADRID-ESPAÑA

ANEXO 8.

FICHEROS DECLARADOS POR LA "CADENA COPE"

Razón Social: RADIO POPULAR, S. A., CADENA COPE.

Nombre del fichero:
MARKETING DIRECTO.
Finalidad:
USO DE LOS DATOS DE LOS PARTICIPANTES EN DETERMINADAS INICIATIVAS PROMOVIDAS POR LA SOCIEDAD PARA SU UTILIZACION EN ENVIOS DE COMUNICACIONES DE PRODUCTOS Y SERVICIOS.
Dirección:
ALFONSO XI, 4.
Código Postal - Población:
28014-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Razón Social: RADIO POPULAR, S. A., CADENA DE ONDAS POPULARES ESPAÑOLAS.

Nombre del fichero:
EMPLEADOS.
Finalidad:
GESTION DE NOMONAS Y RECURSOS HUMANOS; GESTION DE PERSONAL; FORMACION DE PERSONAL; PRESTACIONES SOCIALES Y PREVENCION DE RIESGOS LABORALES.
Dirección:
ALFONSO XI, 4.
Código Postal - Población:
28014-MADRID.

Nombre del fichero:
PARTICIPACION CIUDADANA.
Finalidad:
GESTION DE LOS DATOS DE LOS INTERESADOS QUE APOYAN LAS INICIATIVAS DE LA ENTIDAD.
Dirección:
ALFONSO XI, 4.
Código Postal - Población:
28014-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
ACCIONISTAS Y CONSEJEROS.
Finalidad:
LA FINALIDAD DEL FICHERO ES LA GESTION DE LOS ACCIONISTAS Y CONSEJEROS DE LA SOCIEDAD REALIZACION DE COMUNICACIONES Y PAGO DE DIVIDENDOS.
Dirección:
ALFONSO XI, 4.
Código Postal - Población:
28014-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
CANDIDATOS.
Finalidad:
SU FINALIDAD ES LA IDENTIFICACION Y GESTION DE LOS CANDIDATOS A EMPLEO EN LOS PROCESOS DE SELECCION DE LA SOCIEDAD.
Dirección:
ALFONSO XI, 4.
Código Postal - Población:
28014-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
CLIENTES.
Finalidad:
GESTION ECONOMICA Y CONTABLE GESTION ADMINISTRATIVA GESTION DE CLIENTES GESTION DE FACTURACION COBROS Y PAGOS PUBLICIDAD FIDELIZACION DE CLIENTE.
Dirección:
ALFONSO XI, 4.
Código Postal - Población:
28014-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
CLIENTES POTENCIALES.
Finalidad:
LA FINALIDAD DEL FICHERO ES LA GESTION DE CLIENTES POTENCIALES CON FINES PROMOCIONALES DE INFORMACION Y PUBLICIDAD.
Dirección:
ALFONSO XI, 4.
Código Postal - Población:
28014-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
CONTACTOS.
Finalidad:
GESTION Y MANTENIMIENTO DE RELACIONES EXTERNAS DE PERSONAS DE CONTACTO DE LA SOCIEDAD.
Dirección:
ALFONSO XI, 4.
Código Postal - Población:
28014-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
CONTROL DE ACCESO.
Finalidad:
LA FINALIDAD DEL FICHERO ES EL CONTROL DE ACCESO Y MANTENIMIENTO DE LA SEGURIDAD DEL EDIFICIO DONDE SE ENCUENTRAN LAS OFICINAS DE LA SOCIEDAD.
Dirección:
ALFONSO XI, 4.
Código Postal - Población:
28014-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
PROGRAMAS.
Finalidad:
GESTION DE CONCURSOS Y SORTEOS Y PARTICIPANTES EN LOS PROGRAMAS GRABACION DE EMISIONES Y PROGRAMACION FIDELIZACION DE OYENTES.
Dirección:
ALFONSO XI, 4.
Código Postal - Población:
28014-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
PROVEEDORES.
Finalidad:
GESTION ECONOMICA Y CONTABLE GESTION ADMINISTRATIVA GESTION DE PROVEEDORES GESTION DE PAGOS Y DE COBROS.
Dirección:
ALFONSO XI, 4.
Código Postal - Población:
28014-MADRID.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
USUARIOS DE INTERNET.
Finalidad:
GESTION DE LOS DATOS RELATIVOS A LOS USUARIOS DE LA PAGINA WEB DE LA ENTIDAD; YA SEA PORQUE INTRODUCEN COMENTARIOS A NOTICIAS O PORQUE SOLICITEN RECIBIR UN NEWSLETTER DIARIO DE NOTICIAS.
Dirección:
ALFONSO XI, 4.
Código Postal - Población:
28014-MADRID.
Provincia - País:
MADRID-ESPAÑA.

ANEXO 9.

FICHEROS DECLARADOS POR "ONDA CERO RADIO"

Razón Social: UNIPREX, S. A.

Nombre del fichero:
ACCIONES.
Finalidad:
GESTIONAR LA PARTICIPACION EN SERVICIOS; CONCURSOS; PROMOCIONES; VOTACIONES Y JUEGOS; ASI COMO LA GESTION DE PREMIOS; PUBLICIDAD Y PROSPECCION COMERCIAL.
Dirección:
AVENIDA ISLA GRACIOSA, Nº 13 (EDIFICIO ANTENA 3).
Código Postal - Población:
28703-SAN SEBASTIAN DE LOS REYES.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
PROGRAMAS.
Finalidad:
PARTICIPACION EN CONCURSOS PROMOCIONES PROGRAMAS Y SORTEOS ASI COMO LA GESTION Y ENVIO DE REGALOS Y PREMIOS.
Dirección:
AVENIDA ISLA GRACIOSA, Nº13 (EDIFICIO ANTENA 3).
Código Postal - Población:
28703-SAN SEBASTIAN DE LOS REYES.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
MALOS HUMOS.
Finalidad:
SE UTILIZARA COMO CONTENEDOR TEMPORAL DE TODOS LOS DATOS FACILITADOS A UNIPREX S A U PARA LA GESTION DE LA PLATAFORMA MALOS HUMOS PROCEDIENDO A SU ELIMINACION TRAS SU TRATAMIENTO Y UNA VEZ CUMPLIDA SU FINALIDAD.
Dirección:
AVENIDA ISLA GRACIOSA, Nº 13 (EDIFICIO ANTENA 3).
Código Postal - Población:
28703-SAN SEBASTIAN DE LOS REYES.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
CLIENTES.
Finalidad:
LA FINALIDAD DEL FICHERO ES LA GESTION DE LOS CLIENTES DE UNIPREX PARA MANTENER LA RELACION COMERCIAL Y REALIZAR LA GESTION DE COBROS A LOS MISMOS.
Dirección:
AVENIDA ISLA GRACIOSA, Nº13 (EDIFICIO ANTENA 3).
Código Postal - Población:
28703-SAN SEBASTIAN DE LOS REYES.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
NOMINA.
Finalidad:
FICHERO QUE CONTIENE LOS DATOS PARA LA GESTION Y MANTENIMIENTO DE LA NOMINA FORMACION EVALUACION DEL DESEMPEÑO DESARROLLO DE PLANES DE CARRERA BENEFICIOS SOCIALES SELECCION DEL PERSONAL Y DECLARACION DE ACCIDENTES LABORALES.
Dirección:
AVENIDA ISLA GRACIOSA, Nº13 (EDIFICIO ANTENA 3).
Código Postal - Población:
28703-SAN SEBASTIAN DE LOS REYES.
Provincia - País: MADRID-ESPAÑA

Nombre del fichero:
PERSONAL.
Finalidad:
GESTION Y MANTENIMIENTO DE LAS DIFERENTES ACTIVIDADES DESARROLLADAS POR EL PERSONAL DE UNIPREX Y VINCULADAS A SU RELACION LABORAL CON LA EMPRESA.
Dirección:
AVENIDA ISLA GRACIOSA, Nº13 (EDIFICIO ANTENA 3).
Código Postal - Población:
28703-SAN SEBASTIAN DE LOS REYES.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
PROVEEDORES.
Finalidad:
LA FINALIDAD DEL FICHERO ES LA GESTION DE LOS PROVEEDORES DE UNIPREX PARA MANTENER LA RELACION COMERCIAL Y REALIZAR LA GESTION DE PAGOS A LOS MISMOS.
Dirección:
AVENIDA ISLA GRACIOSA, Nº13 (EDIFICIO ANTENA 3).
Código Postal - Población:
28703-SAN SEBASTIAN DE LOS REYES.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
RELACIONES PUBLICAS.
Finalidad:
REALIZAR COMUNICACIONES REGALOS O INVITACIONES A ACTOS SOCIALES Y MANTENER UNA BASE DE DATOS DE RELACIONES PUBLICAS.
Dirección:
AVENIDA ISLA GRACIOSA, Nº13 (EDIFICIO ANTENA 3).
Código Postal - Población:
28703-SAN SEBASTIAN DE LOS REYES.
Provincia - País: MADRID-ESPAÑA.

Nombre del fichero:
REQUERIMIENTOS.
Finalidad:
GESTION CONTABLE FISCAL Y ADMINISTRATIVA DE LOS REQUERIMIENTOS PROVENIENTES DE ORGANISMOS OFICIALES.
Dirección:
AVENIDA ISLA GRACIOSA, Nº13 (EDIFICIO ANTENA 3).
Código Postal - Población:
28703-SAN SEBASTIAN DE LOS REYES.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
SERVICIO MEDICO.
Finalidad:
GESTION Y CONTROL DE LAS REVISIONES MEDICAS Y DE LA ASISTENCIA MEDICA DIARIA QUE SE REALIZA A LOS EMPLEADOS DE UNIPREX ASI COMO OBTENCION DE ESTADISTICAS PARA LA PROPIA EMPRESA.
Dirección:
AVENIDA ISLA GRACIOSA, Nº13 (EDIFICIO ANTENA 3).
Código Postal - Población:
28703-SAN SEBASTIAN DE LOS REYES.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
SUGERENCIAS.
Finalidad:
GESTION DE LAS SUGERENCIAS CONSULTAS OPINIONES SOLICITUDES O COMENTARIOS DE CUALQUIER CLASE ENVIADOS POR LOS OYENTES Y USUARIOS DE LA WEB DE UNIPREX CON EL FIN DE MEJORAR NUESTRA OFERTA RADIOFONICA Y EL SERVICIO A NUESTROS USUARIOS.
Dirección:
AVENIDA ISLA GRACIOSA, Nº13 (EDIFICIO ANTENA 3).
Código Postal - Población:
28703-SAN SEBASTIAN DE LOS REYES.
Provincia - País: MADRID-ESPAÑA.

Nombre del fichero:
FONDOS DOCUMENTALES.
Finalidad:
REALIZAR LA GESTION DE LOS FONDOS DOCUMENTALES INFORMATIVOS DE UNIPREX PARA LOS PROGRAMAS DE RADIO CON CONTENIDOS INFORMATIVOS.
Dirección:
AV ISLA GRACIOSA (EDIFICIO ANTENA 3), 13.
Código Postal - Población:
28700-SAN SEBASTIAN DE LOS REYES.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
LDAP.
Finalidad:
FACILITAR LA COMUNICACION ENTRE EMPLEADOS SEGURIDAD LOGICA Y GESTION/ADMINISTRACION DEL LDAP CORPORATIVO.
Dirección:
AV ISLA GRACIOSA (EDIFICIO ANTENA 3), 13.
Código Postal - Población:
28700-SAN SEBASTIAN DE LOS REYES.
Provincia - País:
MADRID-ESPAÑA.

Nombre del fichero:
REGISTRO DIRECCIONES IP.
Finalidad:
REGISTRO DE LAS DIRECCIONES IP DE LOS USUARIOS QUE ACCEDEN AL PORTAL DE INTERNET DE UNIPREX SEGUN ESTABLECE LA LSSI PARA LOS PRESTADORES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACION.
Dirección:
AV ISLA GRACIOSA (EDIFICIO ANTENA 3), 13.
Código Postal - Población:
28700-SAN SEBASTIAN DE LOS REYES.
Provincia - País: MADRID-ESPAÑA.

Nombre del fichero:
REGISTRO USUARIOS INTERNET.
Finalidad:
REGISTRO DE USUARIOS DE INTERNET GESTIONAR SU PARTICIPACION EN LAS DIFERENTES SECCIONES Y CONCURSOS DE LAS WEB S DE LAS QUE ES TITULAR UNIPREX S A Y EL ENVIO DE PROMOCIONES COMERCIALES QUE PUEDAN RESULTAR DE SU INTERES.
Dirección:
AV ISLA GRACIOSA (EDIFICIO ANTENA 3), 13.
Código Postal - Población:
28700-SAN SEBASTIAN DE LOS REYES.
Provincia - País:
MADRID-ESPAÑA.

ANEXO 10.

FICHEROS INSCRITOS POR LA "RTVA"

Razón Social: AGENCIA PUBLICA EMPRESARIAL DE LA RADIO Y TELEVISION DE ANDALUCIA

Nombre del fichero:
BASE DATOS REGISTRO DE PROGRAMAS.
Finalidad:
DATOS DE LA PERSONA QUE PRESENTA UN PROYECTO EN EL REGISTRO PARA CONTACTOS POSTERIORES.
Dirección:
CARRETERA SAN JUAN – TOMARES, KM 1.3.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
CLIENTES DE PUBLICIDAD DE RADIO.
Finalidad:
GESTION DE CLIENTES.
Dirección:
CARRETERA SAN JUAN – TOMARES, S/N.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
CONCURSO OPOSICION LIBRE.
Finalidad:
RECOGER LAS SOLICITUDES PARA EL CONCURSO DE OPOSICION LIBRE DE RTVA DEL AÑO 2008 Y PUBLICACION DE LOS AVANCES Y LISTADOS DE LA MISMA.
Dirección:
CARRETERA SAN JUAN – TOMARES, KM 1.3.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
DATOS DE USUARIOS QUE CONTACTAN CON EL DEFENSOR DE LA AUDIENCIA.
Finalidad:
DATOS PERSONALES DE LOS USUARIOS QUE CONTACTAN CON EL DEFENSOR DE LA AUDIENCIA PARA PRESENTAR QUEJAS SUGERENCIAS Y PREGUNTAS.
Dirección:
CARRETERA SAN JUAN – TOMARES, KM 1.3.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
DATOS DEL PERSONAL DE CONTRATAS DE RTVA.
Finalidad:
DATOS DEL PERSONAL QUE TRABAJA EN LAS CONTRATAS DE RTVA.
Dirección:
CARRETERA SAN JUAN – TOMARES, KM 1.3.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
DATOS MEDICOS DE PERSONAL.
Finalidad:
HISTORIAL MEDICO DE LOS EMPLEADOS DE RTVA.
Dirección:
CARRETERA SAN JUAN – TOMARES, KM 1.3.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
FONDOS DOCUMENTALES DE RADIO Y TELEVISION.
Finalidad:
REALIZACION DE PROGRAMAS DE RADIO Y TELEVISION EN BASE A LA INFORMACION RECOGIDA DE DIVERSOS MEDIOS TANTO PROPIOS COMO EXTERNOS.
Dirección:
CARRETERA SAN JUAN – TOMARES, KM 1.3.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
GESTION DEL TRIBUNAL DEL CONCURSO OPOSICION LIBRE.
Finalidad:
GESTIONAR LAS SOLICITUDES PARA EL CONCURSO DE OPOSICION LIBRE DE RTVA DEL AÑO 2008 POR PARTE DEL TRIBUNAL DE RTVA.
Dirección:
CARRETERA SAN JUAN – TOMARES, KM 1.3.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
PROVEEDORES.
Finalidad:
PROVEEDORES PROFESIONALES Y CLIENTES PARA LA GESTION CONTABLE FISCAL Y ADMINISTRATIVA DE COBROS Y PAGOS.
Dirección:
CARRETERA SAN JUAN – TOMARES, KM 1.3.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
RECURSOS HUMANOS.
Finalidad:
PAGO DE LA NOMINA DE LOS TRABAJOADORES COTIZACIONES SEGURIDAD SOCIAL RETENCIONES IRPF BOLSAS DE TRABAJO Y GESTION DE RECURSOS HUMANOS.
Dirección:
CARRETERA SAN JUAN – TOMARES, KM 1.3.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
SOCIOS.
Finalidad:
PARTICIPACION EN LAS ACTIVIDADES DEL CLUB INFANTIL DE LA BANDA DEL SUR PATROCINADO POR CANAL SUR TV.
Dirección:
CARRETERA SAN JUAN – TOMARES, KM 1.3.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
TIENDA CANAL SUR TV.
Finalidad:
SOLICITUD DE COMPRA DE PRODUCTOS PROPIOS DE CANAL SUR TV.
Dirección:
CARRETERA SAN JUAN – TOMARES, KM 1.3.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
VIDEOVIGILANCIA SEGURIDAD RTVA.
Finalidad:
VIDEOVIGILANCIA EN LOS HALLS DE ENTRADA EN LAS DISTINTAS SEDES DE RTVA.
Dirección:
CARRETERA SAN JUAN – TOMARES, KM 1.3.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

Nombre del fichero:
BASE DE DATOS DE ESPECTADORES PARA PROMOCIONES.
Finalidad:
RECOGIDA DE DATOS DE ESPECTADORES QUE ENVIAN AUDIOS O VIDEOS PARA CAMPAÑAS DE PROMOCIONES.
Dirección:
CARRETERA SAN JUAN – TOMARES, S/N.
Código Postal - Población:
41920-SAN JUAN DE AZNALFARACHE.
Provincia - País:
SEVILLA-ESPAÑA.

ANEXO 11.

Recomendaciones que deberán ser observadas por todas las compañías implicadas en la producción y realización de programas de televisión, al objeto de adecuar éstas a los principios de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y a la normativa que la desarrolla.

PRIMERA: INFORMACIÓN EN LA RECOGIDA DE DATOS

1. De conformidad con lo establecido por el artículo 5 de la LOPD, los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) del carácter
obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

2. Esta información deberá ser facilitada con carácter previo independientemente de la vía a través de las cual se recaben datos personales, ya sea a través de líneas telefónicas, mensajes SMS, correo postal, Internet o cualquier otra. Cuando el medio utilizado no permita el
contacto simultáneo con el interesado en el momento en el que éste facilita sus datos, el responsable se asegurará de que se le suministra la citada información en el momento en que se da publicidad al procedimiento por el que se recibirán los datos.

3. La citada información se facilitará cualquiera que sea la tecnología utilizada para el almacenamiento de los datos, ya se trate de ficheros de audio o ficheros convencionales de texto en formato ASCII o cualquier otro.

4. Esta misma información se suministrará independientemente de la tipología de datos personales que se recaban, entendiéndose a estos efectos que, en el contexto que nos ocupa, el número de teléfono (fijo o móvil) es por sí mismo un dato personal de carácter identificativo y que, por tanto, la información asociada al mismo puede concernir a una persona física identificable.

5. De acuerdo con lo que establece el apartado 2 del artículo 5 de la LOPD, esa misma información debe figurar en forma claramente legible cuando se utilicen cuestionarios u otros impresos para la recogida, por lo que en tales casos no basta la comunicación verbal de tales advertencias.

6. En el caso de que los datos personales vayan a ser inicialmente incorporados a los ficheros de distintos responsables, se referirá a cada uno de ellos toda la información anteriormente especificada.

SEGUNDA: CONSENTIMIENTO DEL AFECTADO

De acuerdo con lo que dispone el apartado 1 del artículo 6 de la LOPD, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa o sean de aplicación las excepciones previstas en el apartado 2 del mismo artículo. A este respecto, se entenderá que cuando el afectado facilita voluntariamente sus datos consiente en el tratamiento de los mismos en los términos y condiciones de los que ha sido convenientemente informado en el momento de la recogida.

TERCERA: USOS Y FINALIDADES

1. Tal y como dispone el apartado 1 del artículo 4 de la LOPD, los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. No se recabarán datos personales cuyo conocimiento por parte del responsable no esté justificado por la finalidad para la que se recaban y de la cual el usuario no haya sido previamente informado. En particular, no se recabarán datos personales a través de líneas 906 cuando éstos no vayan a

ser utilizados para la finalidad comunicada y su recogida sólo éste motivada por cuestiones promocionales.

3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquella que ha justificado su recogida. A este respecto debe recordarse que la Sentencia 292/2000 del Tribunal Constitucional ha señalado que "*el derecho a consentir la recogida y tratamiento de los datos personales no implica en modo alguno consentir la cesión de tales datos a terceros [...] Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando puedan ser compatible con éstos supone una nueva posesión y uso que requiere el consentimiento del interesado*". Así, para que tales datos puedan ser usados para una finalidad distinta, es imprescindible obtener previamente el consentimiento inequívoco del afectado.

CUARTA: CANCELACIÓN DE DATOS

1. Según prevé el apartado 5 del artículo 4 de la LOPD, los datos de carácter personal serán cancelados a propia iniciativa del responsable del fichero cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados. Igualmente serán cancelados cuando así lo solicite el interesado.

2. Esta obligación se extiende a cualquiera de los ficheros o tratamientos especificados en la Recomendación Primera, siempre y cuando los datos de carácter personal no deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

QUINTA: DATOS DE SALUD Y DE VIDA SEXUAL

De conformidad con lo establecido en el apartado 3 del artículo 7 de la LOPD, los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.

SEXTA: ACCESO A LOS DATOS POR CUENTA DE TERCEROS

1. De conformidad con lo dispuesto en el apartado 1 del artículo 12 de la LOPD, la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

2. En el citado contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de la LOPD que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. Estas obligaciones se extenderán a todas aquellas entidades que, como encargados del tratamiento, participen en la realización de los programas de televisión. A este respecto, el prestador del servicio no podrá utilizar los datos para fin distinto del que conste en el contrato, ni subcontratar la gestión del servicio con terceros, salvo que lo haga en nombre y por cuenta del responsable.

5. En particular, la colaboración de distintas entidades en la atención de líneas telefónicas en situaciones de congestión de red deberá regularse en todo caso de acuerdo con lo expresado en los apartados anteriores.

SÉPTIMA: COMUNICACIÓN DE DATOS

1. Según dispone el apartado 1 del artículo 11 de la LOPD, los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. A este respecto se tendrán en cuenta, sin embargo, las excepciones previstas en el apartado 2 del citado artículo, y en particular, la referida a la situación en la que el tratamiento responda a la

libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este último caso, la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

2. De acuerdo a lo que establece el apartado 3 del mismo artículo y en consonancia con lo expresado por el apartado 2 de la Recomendación Primera, será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar. En este sentido, cuando los datos personales recabados vayan a ser comunicados a otras compañías (incluso cuando éstas pertenezcan al mismo grupo empresarial) deberá informarse al usuario, de tal forma que éste pueda conocer explícitamente las finalidades determinadas a las que se destinarán los datos.

OCTAVA: MOVIMIENTO INTERNACIONAL DE DATOS

1. De conformidad con lo establecido por el artículo 33 de la LOPD, no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la Ley Orgánica, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos. A este respecto, se tendrán en cuenta las excepciones previstas en el artículo 34 de la LOPD. En particular, cuando sea de aplicación la legislación española sobre protección de datos, conforme al artículo 2.1 de la LOPD, y además el fichero que contiene datos personales (recabados a través de Internet o por cualquier otra vía) se halle ubicado en el territorio de un Estado no miembro de la Unión Europea o respecto del que no se haya declarado por la Comisión de las Comunidades Europeas la existencia de un nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo, será precisa la autorización previa del Director de la Agencia de Protección de Datos, a menos que la transferencia internacional se fundamente en alguno de las excepciones comprendidas en los apartados a) a j) del artículo 34 de la LOPD antes citados. En todo caso, la transferencia internacional se deberá notificar a la Agencia de Protección de Datos para su inscripción en el Registro General.

2. De acuerdo con lo que establece el artículo 5 de la LOPD, cualquier responsable de un fichero o tratamiento que se proponga transferir datos de carácter personal fuera del territorio español deberá haber informado a los afectados de quiénes serán destinatarios de los datos, así como de la finalidad que justifica la transferencia internacional y el uso de los datos que podrá hacer el destinatario.

3. El deber de información a que se refiere el apartado anterior no será de aplicación cuando la transferencia internacional tenga por objeto la prestación de un servicio al responsable del fichero, por parte de un tercero al que se le haya encargado el mismo en los términos establecidos por el artículo 12 de la LOPD.

4. Con independencia de lo anterior, en el caso de que la transferencia se legitime mediante la obtención del consentimiento inequívoco del afectado, el responsable del fichero se asegurará de que éste ha sido previamente informado de los extremos citados en el apartado 2.

NOVENA: SEGURIDAD DE LOS DATOS

1. De acuerdo con lo establecido por el artículo 9 de la LOPD, el responsable del fichero y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones determinadas en el Reglamento que desarrolla la LOPD.

3. Se considera una buena práctica la adopción de medidas que eviten que la información circule por Internet de forma inteligible y, por tanto, susceptible de ser conocida o manipulada por terceros.

ANEXO 12.

COMUNICADO: LA AUDIENCIA NACIONAL, PIONERA ALPLANTEAR EN EUROPA EL "DERECHO AL OLVIDO" EN INTERNET.

Madrid, 2 de marzo de 2012.- La Sala de lo Contencioso-administrativo de la Audiencia Nacional plantea al Tribunal de Justicia de la UE una cuestión prejudicial de interpretación sobre la protección de datos de un particular frente a Google. Con su resolución, la AN describe jurídicamente la situación creada ante las nuevas tecnologías que traspasan fronteras y límites temporales y que se han desarrollado con posterioridad a las normativas vigentes. Es la primera vez que un tribunal plantea esta cuestión ante el Tribunal de Justicia de la UE y la decisión del Tribunal de Luxemburgo vinculará a todos los tribunales de los Estados miembros donde existen reclamaciones similares.

El auto de la Sección Primera plantea de fondo si un particular tiene derecho a reclamar la supresión y bloqueo de informaciones en los buscadores de Internet relativas a su persona y que, con las nuevas tecnologías, podrán ser localizadas "a lo largo de toda su vida y la de sus descendientes".

Nueve preguntas al Tribunal de Justicia de la UE

Los magistrados resumen en nueve preguntas todas las dudas jurídicas que se han encontrado al abordar el caso de un particular que, al teclear su nombre en Google encontraba el enlace con un anuncio en un periódico de tirada nacional, de la subasta de un inmueble por un impago a la Seguridad Social. El afectado afirmaba que el embargo ya se había solucionado y resuelto desde hace años y, pese a ello, esa referencia seguía apareciendo en el buscador.

La Agencia Española de Protección de Datos acogió la petición de tutela del afectado y requirió a Google Spain SL y Google Inc. que

retiraran los datos del denunciante de su índice. Sin embargo, consideró que la información de la subasta aparecida en el periódico debía mantenerse por tener una justificación legal.

La Sala entiende que el recurso plantea "el problema referido a las obligaciones que tienen los buscadores de Internet en la protección de datos personales de aquellos afectados que no desean que determinadas informaciones, publicadas en páginas web de terceros y que contienen sus datos personales y permiten relacionarles con la misma, sean localizadas, indexadas y sean puestas a disposición de los internautas de forma indefinida".

La primera duda que se plantean los jueces es si la normativa comunitaria y nacional en materia de protección de datos se puede aplicar en este caso o, si como sostiene la empresa Google Inc., los afectados deberían acudir a los tribunales de California (EEUU) donde está domiciliada la empresa matriz del grupo.

Se pregunta también la Sala si los buscadores, cuando indexan la información, están realizando un tratamiento de datos personales, si son responsables de ese tratamiento y deben atender por tanto a los derechos de cancelación y/o oposición del afectado de forma directa, aunque la información se mantenga en la fuente originaria por considerarse lícita.

Finalmente, los jueces preguntan al Tribunal de Luxemburgo si la protección de datos incluye que el afectado se niegue a que una información referida a su persona se indexe y difunda, aun siendo lícita y exacta en su origen, pero que la considere negativa o perjudicial para su persona.

ANEXO 13.

COMISIÓN EUROPEA – COMUNICADO DE PRENSA:

La Comisión propone una reforma general de las normas de protección de datos para aumentar el control de los usuarios sobre sus propios datos y reducir los costes para las empresas.

Bruselas, 25 de enero de 2012 – La Comisión Europea ha propuesto hoy una reforma general de las normas de protección de datos de la UE de 1995 con objeto de ampliar los derechos a la privacidad en línea e impulsar la economía digital europea. El progreso tecnológico y la globalización han modificado profundamente las vías de obtención, acceso y utilización de los datos. Además, los 27 Estados miembros de la UE han aplicado las normas de 1995 de manera diferente, lo que ha creado divergencias en cuanto a su ejecución y cumplimiento. Mediante un único acto legislativo, se suprimirán la fragmentación y las costosas cargas administrativas actuales, lo que generará un ahorro de unos 2 300 millones EUR anuales. Esta iniciativa contribuirá a reforzar la confianza de los consumidores en los servicios en línea y, con ello, otorgará un impulso muy necesario al crecimiento, la creación de empleo y la innovación en Europa.

«Hace 17 años, menos de un 1 % de los europeos usaba Internet. Hoy en día se transfieren e intercambian enormes cantidades de datos personales entre continentes y de una punta a otra del mundo en fracciones de segundos», ha declarado Viviane Reding, Comisaria de Justicia de la UE y Vicepresidenta de la Comisión. «La protección de los datos personales es un derecho fundamental de todos los europeos, quienes, no obstante, a veces sienten que pierden el control sobre sus datos personales. Mis propuestas contribuirán a infundir confianza en los servicios en línea dado que los ciudadanos estarán mejor informados de sus derechos y tendrán un mayor control sobre la información que les atañe. La reforma conseguirá todos estos objetivos al tiempo que facilitará el funcionamiento de las empresas y les permitirá ahorrar costes. La existencia de un marco

legal sólido, claro y uniforme a escala de la UE permitirá liberar el potencial del Mercado Único Digital y fomentar el crecimiento económico, la innovación y la creación de empleo».

Las propuestas de la Comisión actualizan y modernizan los principios consagrados en la Directiva sobre protección de datos de 1995 con el fin de preservar los derechos a la privacidad en el futuro. Constan de una Comunicación en la que se exponen los objetivos de la Comisión y dos propuestas legislativas: un Reglamento que establece un marco general de la UE para la protección de datos y una Directiva sobre la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos y en relación con las actividades judiciales correspondientes.

Los cambios esenciales introducidos por la reforma son los siguientes:

- Se impondrá un conjunto único de normas sobre protección de datos válido en toda la UE y se eliminarán requisitos administrativos innecesarios como los requisitos de notificación para las empresas. Esto les supondrá un ahorro cercano a 2 300 millones EUR anuales.

- En lugar de la disposición actual que obliga a todas las empresas a notificar todas las actividades de protección de datos a los supervisores de protección de datos (requisito que ha generado a las empresas trámites y costes por un valor de 130 millones EUR anuales) el Reglamento intensifica la responsabilidad y la obligación de rendir cuentas de todos aquellos que procesen datos personales.

- Por ejemplo, las empresas y organizaciones deberán notificar a la autoridad nacional de control toda violación de datos grave lo antes posible (siempre que sea posible en un plazo de 24 horas).

- Las organizaciones tendrán como interlocutora única a una autoridad nacional de protección de datos en el país de la UE donde tengan su sede. Del mismo modo, los ciudadanos podrán dirigirse a la autoridad de protección de datos de su país, incluso cuando sus datos sean tratados por una empresa ubicada fuera de la UE. Siempre que el tratamiento de los datos exija el consentimiento del interesado, deberá dejarse claro que dicho consentimiento debe obtenerse explícitamente y no presuponerse.

- Los ciudadanos tendrán un acceso más fácil a sus propios datos y deberán poder transferir sus datos personales de un proveedor de servicios a otro con mayor facilidad (el derecho a la «portabilidad de los datos»), lo que aumentará la competencia entre servicios.

- El «derecho al olvido» ayudará a los ciudadanos a gestionar mejor los riesgos inherentes a la protección de los datos en línea: los usuarios podrán borrar sus datos cuando no existan razones legítimas para conservarlos.

- Deberán aplicarse las normas de la UE a toda empresa activa en el mercado de la UE que ofrezca sus servicios a ciudadanos de la UE y procese datos personales en terceros países.

- Se proporcionarán refuerzos para las autoridades nacionales independientes de protección de datos para que efectúen una mejor aplicación de las normas de la UE en su territorio. En efecto, tendrán la potestad de multar a las empresas que quebranten las normas de protección de datos de la UE. Este tipo de sanciones puede representar hasta 1 millón EUR o un 2 % del volumen de negocios anual global de una empresa.

- Una nueva Directiva aplicará ciertos principios y normas generales de protección de datos a la cooperación policial y judicial en materia penal. Esas reglas se aplicarán a las transmisiones de datos nacionales e internacionales.

Las propuestas de la Comisión entran ahora en la fase de discusión ante el Parlamento Europeo y los Estados miembros de la UE (a través del Consejo de Ministros). Entrarán en vigor dos años después de su adopción.

Contexto.

Por datos personales se entiende cualquier información, ya sea de carácter privado, profesional o público, que se refiera a una persona. Puede consistir en un nombre, una foto, una dirección electrónica, datos bancarios, mensajes publicados en redes sociales, información médica o la dirección IP de un ordenador. La Carta de los Derechos Fundamentales de la UE declara que toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan en todos los aspectos de su existencia: en su hogar, en su lugar de trabajo, al hacer compras, al recibir tratamiento médico, en una comisaría de policía o en Internet.

En la era digital, la obtención y el almacenamiento de información personal son esenciales. Los datos son utilizados por todo tipo de empresas, desde compañías de seguros y bancos hasta medios de comunicación sociales, pasando por motores de búsqueda. En un entorno globalizado, la transferencia de datos a terceros países se ha convertido en un importante factor de la vida cotidiana. En línea no hay fronteras y la computación en nube permite que los datos se envíen desde Berlín para procesarse en Boston y almacenarse en Bangalore.

El 4 de noviembre de 2010, la Comisión fijó una estrategia para reforzar las normas de protección de datos de la UE (IP/10/1462 y MEMO/10/542). Sus objetivos eran proteger los datos personales en todos los ámbitos de actuación, incluido el orden público, reduciendo al mismo tiempo los trámites engorrosos para las empresas y garantizando la libre circulación de datos dentro de la UE. La Comisión solicitó reacciones a sus ideas y llevó a cabo una consulta pública por separado para revisar la Directiva sobre protección de datos (95/46/CE).

Las normas sobre protección de datos de la UE se destinan a proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, el derecho a la protección y a la libre circulación de los datos. Esta Directiva sobre protección de datos general se complementa con otros instrumentos jurídicos como la Directiva sobre la privacidad y las comunicaciones electrónicas, para el sector de las comunicaciones. Existen además disposiciones específicas para la protección de los datos personales en el marco de la cooperación policial y judicial en materia penal (Decisión Marco 2008/977/JAI).

El derecho a la protección de los datos personales se reconoce explícitamente en el artículo 8 de la Carta de los Derechos Fundamentales de la UE y en el Tratado de Lisboa. La base jurídica de las normas de protección de datos en el marco de todas las actividades reguladas por el Derecho de la UE se recoge en el artículo 16 del Tratado de Funcionamiento de la Unión Europea[742].

[742] Reforma de la protección de datos:
<http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm>.
Portada del sitio web de Viviane Reding, Comisaria de Justicia y Vicepresidenta de la Comisión de la UE: <http://ec.europa.eu/reding>.
Comisión Europea, protección de datos: <http://ec.europa.eu/justice/data-protection>.
Sala de Prensa de la Dirección General de Justicia de la Comisión Europea: <http://ec.europa.eu/justice/news/intro/news_intro_en.htm>.

ANEXO 14.

CÓDIGOS TIPO INSCRITOS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

*Código Tipo: CÓDIGO TIPO DE TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL PARA ESTABLECIMIENTOS SANITARIOS PRIVADOS DE LA PROVINCIA DE SEVILLA.
Nuevo - Fecha Inscripción: 11/11/2011

* Código Tipo: CÓDIGO TIPO DEL FICHERO DE AUTOMÓVILES DE PÉRDIDA TOTAL, ROBO E INCENDIOS.
Fecha inscripción: 5/09/2011

* Código Tipo: FARMAINDUSTRIA
Fecha Inscripción: 17/06/2009

* Código Tipo VERAZ-PERSUS.
Fecha Inscripción: 19/12/2006
Fecha adecuación al RLOPD: 30/10/2009

* Código Tipo del Sector de la Intermediación Inmobiliaria. Asociación Empresarial de Gestión Inmobiliaria (AEGI).
Fecha Inscripción: 29/12/2004
Fecha adecuación al RLOPD: 08/02/2010

* Código Tipo de la Asociación Catalana de Recursos Asistenciales (ACRA)
Fecha Inscripción: 27/12/2004
Fecha adecuación al RLOPD: 29/12/2009

* Código Tipo Universidad de Castilla-La Mancha
Fecha Inscripción: 14/07/2004
Fecha adecuación al RLOPD: 16/11/2009

* Código Tipo de Odontólogos y Estomatólogos de España
Fecha Inscripción: 12/07/2004 (modificado en diciembre de 2006)
Fecha adecuación al RLOPD: 22/12/2009
Resolución de Inscripción

* Código Tipo de Confianza On-Line
Fecha Inscripción: 07/11/2002 (modificado en noviembre de 2005)
Fecha adecuación al RLOPD: 29/12/2009

* Código Tipo de Unió Catalana D'Hospitals
Fecha Inscripción: 12/07/2002 (modificado en julio de 2004)
Fecha adecuación al RLOPD: 16/11/2009

* Código Tipo de Agrupación Catalana de Establecimientos Sanitarios
Fecha Inscripción: 28/12/2001
Fecha adecuación al RLOPD: 03/11/2009

* Código Tipo de Fichero Histórico de Seguros del Automóvil (UNESPA)
Fecha Inscripción: 11/10/2000
Fecha adecuación al RLOPD: 16/11/2009

CÓDIGOS TIPO INSCRITOS EN REGISTROS AUTONÓMICOS DE PROTECCIÓN DE DATOS E INCLUIDOS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS:

* Código Tipo para las entidades locales adheridas a EUDEL (Asociación de Municipios Vascos-Euskadiko Udalen Elkartea)
Fecha Inscripción: 16/07/2009