

La «autodeterminación informativa» como barrera a la libertad de información y al ejercicio profesional del periodismo

Pepe Rodríguez

Facultat de Ciències de la Comunicació. Departament de Periodisme.

Universitat Autònoma de Barcelona.

Despatx núm. 13. Campus Edifici I

08193 Bellaterra, Cerdanyola

pepe.rodriguez@uab.cat

Resum

La legislación española regula muy estrictamente la posibilidad de obtener, tratar y utilizar datos de carácter personal (especialmente usando tecnología informática), y limita, impide, proscribire y sanciona prácticas profesionales habituales y necesarias para ejercer el periodismo con eficiencia, responsabilidad y calidad. Este artículo analiza la confrontación entre el derecho a la autodeterminación informativa y la libertad de información y aflora la situación de grave inseguridad jurídica en la que debe ejercerse la profesión de periodista bajo la actual legislación de protección de datos de carácter personal.

Paraules clau: Protección de datos, tratamiento de datos personales, informática, libertad de información, autodeterminación informativa, periodismo, censura, web, Internet.

Abstract. *The “informative self-determination” as a barrier for information freedom and for professional practice of journalism*

The Spanish legislation very strictly regulates the possibility of obtaining, treating and using personal data (especially when using computer science technology), and limits, prohibits and sanctions the regular and necessary professional practices of journalism and prevents working with efficiency, responsibility and quality. This article analyzes the confrontation between the right to informative self-determination and information freedom. It also shows the serious legal insecurity in which journalism must be exerted under the present legislation of protection of personal data.

Key Words: Protection of data, personal data processing, computing, freedom of information, informative self-determination, journalism, censorship, Web, Internet.

1. Introducció

El ejercicio del periodismo actual no puede imaginarse sin el uso de la informática, tanto en su dimensión estructural (*software* y *hardware*) como en sus resultados de contenido digital accesible (bases de datos, ficheros, medios digitales, webs, blogs...), pero lo que parece ser una bendición que facilita el trabajo, lleva el germen de una maldición capaz de complicar el trabajo periodístico hasta extremos jurídicos inauditos que llegan a impedir prácticas profesionales que han sido, son y serán habituales y necesarias para poder ejercer el periodismo con eficiencia, responsabilidad y calidad.

A nadie escapa que el periodista necesita trabajar con cientos de datos personales para realizar un trabajo que, dado que el derecho fundamental a la libertad de información y de expresión no puede ser absoluto, está regulado y limitado por no menos de una quincena de leyes que le son aplicables.

También es evidente que la astronómica cantidad de datos personales digitalizados (y digitalizables) que son accesibles puede poner en riesgo la intimidad, el honor o la imagen de las personas que identifican, por lo que debe existir legislación adecuada para impedir los usos ilegítimos o lesivos de esos datos personales accesibles, en particular para poder equilibrar la relación entre los avances tecnológicos y la tutela de las libertades (Pérez Luño, 2005) y evitar que el imparable desarrollo tecnológico aplicable a la gestión de datos vaya mucho más allá de la intimidad para lesionar la privacidad (Freixas Gutiérrez, 2001: 18).

Entre quienes necesitan acceso a «todos» los datos por mor de su profesión, y quienes querrían blindarlos en base a derechos siempre útiles para ocultar conductas dudosas, es inevitable un choque de intereses que los legisladores han intentado resolver regulando la protección de datos de carácter personal, un marco jurídico imprescindible, pero que, en lo que atañe al ejercicio del periodismo, merece una seria reflexión dado que muchas, excelentes, aceptadas y necesarias prácticas periodísticas incumplen esa legislación y son acreedoras de sanciones que pueden llegar a los 600.000 euros.

En este artículo analizaremos la confrontación entre dos derechos fundamentales, la autodeterminación informativa y la libertad de información, partiendo desde la legislación que da cuerpo a la primera y desde algunas sentencias clave que la han sustanciado, para poder reflexionar sobre las muchas limitaciones jurídicas a la práctica del periodismo en relación a la adquisición, tenencia y tratamiento (uso) de datos de carácter personal.

2. El concepto de autodeterminación informativa

En la Constitución española de 1978 ya se previó un marco genérico para poder abordar los posibles abusos de la informática en el uso y tratamiento de datos personales (Art. 18.4). Ese artículo —«la ley limitará el uso de la informática para garantizar el honor...»— fue precoz y visionario, ya que en 1978 no podía imaginarse que la informática alcanzaría un desarro-

llo como el actual. Pensemos que la primera red interconectada, base de Internet, se puso en marcha en noviembre de 1969, pero que hasta 1990 no se desarrollaron los protocolos World Wide Web que permitieron que la Red sea lo que es.

El desarrollo de la tecnología digital, sin embargo, pronto comenzó a preocupar en Europa y se abrió una línea legislativa plasmada en el *Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal*, celebrado en Estrasburgo y ratificado, bajo mínimos, por Suecia (1982), Francia (1983), España (1984), Noruega (1984) y Alemania (1985).

Estando el Convenio 108 en fase de aprobación, el Tribunal Constitucional alemán emitió una trascendente sentencia sobre la Ley del Censo, el 15 de diciembre de 1983, en la que se usó ya el concepto de «derecho a la autodeterminación informativa» referido al derecho ciudadano a proteger la intimidad ante el avance de las nuevas tecnologías de la información, sentando la base de la doctrina conocida como «libertad informativa» o «derecho informático», que le otorga al ciudadano la facultad de intervenir activamente, ante entidades públicas y privadas, a fin de conocer, controlar, limitar o impedir el uso de sus datos personales.

El Convenio 108 aportó las definiciones básicas para construir la nueva doctrina, definiendo el dato de carácter personal de manera tan amplia que se correspondía con cualquier dato relacionado con persona identificable. Y entre los «principios a que se obligaban los estados firmantes estaban los fundamentos para desarrollar las normativas sobre protección de datos, como el de “calidad de los datos” (Art. 5) o la prohibición de tratar categorías de datos personales considerados “sensibles”» (Art. 6).

En España, la primera ley específica fue la LORTAD (Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal). Poco después, el espíritu del Convenio 108 y de la LORTAD ya guiaba una resolución del Tribunal Constitucional español, de gran importancia jurisprudencial, que perfilaba el nuevo derecho fundamental a la autodeterminación informativa (STC 254/1993 de 20 de julio de 1993).

Europa continuó y amplió su línea legislativa con dos importantes directivas, la Directiva 95/46/CE del Parlamento Europeo y del Consejo de Europa, de 24 de octubre, 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; y la Directiva 97/66/CE del Parlamento Europeo y del Consejo de Europa sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las comunicaciones.

Esta doctrina entiende por protección de datos «el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad» (Dávila, 1997: 47).

España dio su paso definitivo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), en vigor desde enero de 2000. En ella se incorporaron las recomendaciones fundamentales de las dos directivas citadas. Su reglamento se promulgó por el Real Decreto 1720/2007, 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 (RDLOPD), que acabó con la situación de transitoriedad de la ley (Vilasau, 2008).

Al margen de la clara y meticulosa normativa impuesta por la LOPD y su Reglamento, el Tribunal Constitucional, en su sentencia 292/2000, de 30 de noviembre, dejó asentados los perfiles del derecho de autodeterminación informativa al sentenciar que «el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado [...] Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías [...] Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin [...] De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales [...] Por consiguiente, también alcanza a aquellos 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. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo» (STC 292/2000, FJ 6).

Este derecho fundamental, para el alto tribunal se ejerce mediante el poder de disposición sobre todos los datos personales: «son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele» (STC 292/2000, FJ 7).

Estas restricciones tienen pleno sentido en relación al nuevo paradigma actual en el que la información adquiere un valor económico que puede conllevar un uso y comercialización que afectan directamente los derechos fundamentales de los ciudadanos (Sánchez; Silveira; Navarro, 2003), pero deberían ser objeto de una mirada reguladora específica cuando el tratamiento de datos se enmarca dentro del ejercicio de la libertad de información o de expresión, un aspecto que, sin embargo, no ha merecido la atención debida en la literatura especializada en protección de datos (Bru, 2007; Pouillet y Dinant, 2007; Vilasau, 2008) ni en destacados manuales que la han abordado (Del Peso Navarro, 2000; Vizcaíno Calderón, 2001; Davara, 2001), que si acaso mencionan la libertad de información y de expresión lo hacen sólo en relación a su confrontación con el derecho a la intimidad, pero sin entrar a analizar los muchos y graves conflictos que esta legislación supone para un sector tan importante, social y constitucionalmente, como es el periodismo.

En el mismo caso se está cuando, desde el ámbito de la comunicación, se aborda la libertad de información como sujeto, ya que suele caerse en el olvido de confrontarla con el derecho fundamental a la protección de datos que regula la Ley Orgánica 15/1999. Encontramos este olvido hasta en los más destacados constitucionalistas —«La preeminencia que el derecho a la información pueda llegar a tener respecto de los derechos de la personalidad (honor, intimidad o propia imagen) [...]» (Carrillo, 2006: 117), y ese ninguno con el que se ha tratado a la LOPD desde los expertos en comunicación, juristas o no, se hace patente cuando quiere argumentarse la prevalencia del derecho a la información sobre el derecho a la protección de datos partiendo de la doctrina constitucional por todos conocida y aceptada (Carrillo, 2009) pero obviando lo que, para bien o para mal, impone la LOPD y la doctrina jurídica actual—.

En el ámbito que nos ocupa, estamos con Roig (2009: 44) cuando afirma que «si se desea tener un conocimiento detallado y actualizado de la interpretación de la normativa de protección de datos, es necesario acudir a los dicámenes y estudios jurídicos de la Agencia de Protección de Datos», aunque desde la AEPD tampoco se haya querido entrar en una definición clara de límites en lo tocante al ejercicio profesional del periodismo, quedándose en interpretaciones de la ley de carácter general que, obviamente, son aplicables al periodismo al no haber ninguna excepción que permita lo contrario.

En síntesis, el derecho de autodeterminación informativa impone que los datos de cualquier tipo sobre los cientos o miles de personas que cualquier periodista tiene en «su» agenda, «su» archivo, «su» ordenador, «su» teléfono móvil... no son «suyos» sino de las personas a las que se refieren e identifican esos datos, y no pueden obtenerse ni usarse sin el consentimiento ni conocimiento de sus legítimos propietarios que, además, retienen siempre el derecho de acceso, rectificación y cancelación de los datos que figuren en cualquier fichero que tenga un periodista.

Las implicaciones de orden práctico, profesional y jurídico que este marco legal tiene para el ejercicio del periodismo son tan enormes como desconocidas para la mayoría de profesionales de la comunicación.

3. El ejercicio del periodismo frente a la Ley Orgánica de Protección de Datos de Carácter Personal

La LOPD es de aplicación «a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado» (Art. 2.1). No establece ninguna excepción aplicable al periodismo (Art. 2.2 LOPD y Art. 2.2 y 2.3 RDLOPD).

Toda la actividad profesional de un periodista está sometida a la LOPD, ya que, por definición, trata datos personales en cualquier fase de su trabajo, antes y después de publicarlo, por lo que la LOPD regula, controla y sanciona toda su actividad profesional.

En relación a las personas, todo lo que trata un periodista, en cualquier formato, sin excepción, son «datos de carácter personal» y la mayoría de ellos, además, son considerados de especial protección y/o de imposible tenencia y tratamiento. Todo lo que posee, obtiene, recibe, envía, elabora, archiva... en cualquier formato, es decir, todo lo que compete a su profesión y posibilidades de ejercerla, es considerado un «fichero» que debe estar sometido a la LOPD y a la función inspectora y sancionadora de la Administración, que es la más exigente de Europa (Martínez, 2007: 60).

Para adentrarse en las implicaciones y alcance de la LOPD es imprescindible conocer las definiciones operativas básicas que la sustentan, concretadas en su artículo 3 (y Art. 5 del RDLOPD). A efectos de este artículo, las definiciones más relevantes son:

— Datos de carácter personal: «cualquier información concerniente a personas físicas identificadas o identificables» (LOPD 3a). «Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables» (RDLOPD 5f).

— Fichero: «todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso» (LOPD 3b).

— 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» (LOPD 3c).

— Afectado o interesado: «persona física titular de los datos que sean objeto del tratamiento» (LOPD 3e).

— Cesión o comunicación de datos: «toda revelación de datos realizada a una persona distinta del interesado» (LOPD 3i).

— Fuentes accesibles al público: «aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que

contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación» (LOPD 3j).

No corresponde aquí realizar un análisis crítico pormenorizado del articulado de la LOPD (a este efecto puede consultarse Rodríguez, 2009a y 2009b), aunque será oportuno revisar brevemente algunas de las normas que más afectan al ejercicio del periodismo.

3.1. Restricciones a la tenencia y «tratamiento» de datos personales que limitan gravemente el ejercicio del periodismo

La LOPD permite crear ficheros de contactos (agenda) y de datos «de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona» (Art. 25). Pero también obliga a notificar a la Agencia Española de Protección de Datos (AEPD) cualquier fichero previamente a su creación (Art. 26.1), un requisito que incumplen la mayoría de agendas y archivos de profesionales y de empresas periodísticas; esos ficheros ya creados pero sin notificar suponen una infracción «leve» [de 601,01 a 60.101,21 euros]... y notificar un fichero periodístico supone enfrentar exigencias de imposible cumplimiento, como algunas del Art. 55.2 del RDLOPD.

«Los datos de carácter personal sólo se podrán recoger [...] 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» (Art. 4.1; y Arts. 8.2 y 8.4 RDLOPD), siendo la AEPD quien, ante denuncia de cualquiera, determinará si los «datos de carácter personal» manejados por un periodista son «adecuados, pertinentes y no excesivos».

Al respecto, Hernán Ortiz (2002: 212) advierte que «a partir de la LOPD no es suficiente que el fin sea legítimo, que ha de serlo, sino que además se exige que los fines sean explícitos y se encuentren determinados porque sólo así puede garantizarse la eficacia y virtualidad de la calidad de los datos».

«Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos» (Art. 4.2 y 8.3 del RDLOPD). Este concepto de finalidad incompatible ha generado muchos procesos judiciales y la doctrina imperante, que lo asimila a «finalidad distinta», abre muchas dudas y problemas en relación al modo como se usan los datos personales en la práctica periodística comúnmente aceptada.

Para el Tribunal Supremo: «en relación con la interpretación que deba darse a la expresión “finalidades incompatibles” [...] esta Sala considera que lo que prohíbe el precepto es que los datos de carácter personal se utilicen para una finalidad distinta de aquella para la que han sido recogidos. A estos efectos, y para abundar en la citada equiparación entre la finalidad incompatible y la finalidad distinta, debemos tener en cuenta que ya la STC 292/2000, declaró

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 para fines distintos de los que motivaron la recogida, aún cuando pueda ser compatible con éstos supone una nueva posesión y uso que requiere el consentimiento del interesado”» (SAN 959/2008, FJ 4)¹.

En cuanto a ese preceptivo «consentimiento del interesado», el Art. 6.1 ordena que sea «inequívoco» (documentado) «salvo que la ley disponga otra cosa». Entre las excepciones a ese consentimiento obligatorio, la única aplicable a la práctica periodística es «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».

Para tomar en lo que vale tal «excepción» cabe recordar que la mayoría de datos personales manejados por periodistas proceden de fuentes ajenas al restrictivo listado de «fuentes accesibles al público» del Art. 3j y, por ello, no puede disponerse de ellos sin ese consentimiento «inequívoco» de cada sujeto identificable. Por esta infracción, considerada grave, la AEPD, ha impuesto ya muchas y elevadas sanciones –de 60.101,21 euros–, a menudo por usar datos procedentes de webs (por ejemplo SAN 4399/2008 de 5 de noviembre) y de otras fuentes perfectamente accesibles para todos, pero que la LOPD no considera «fuentes accesibles al público».

La AEPD y la jurisprudencia actual consideran que un web se compone de ficheros automatizados sometidos a la LOPD, y entiende que Internet no es un «medio de comunicación» sino un «canal de comunicación», por lo que no es una fuente accesible al público y, consecuentemente, los datos personales que contiene no pueden tratarse ni usarse sin el «consentimiento del interesado». Esta limitación, gravísima en general, lo es muy especialmente para el ciberperiodismo, una vía profesional de importancia capital, tal como evidencia el panorama informativo actual (Masip, 2003; Sánchez, 2008; Palomo y Meso, 2009) y también el académico (Tejedor, 2008: 618); dejando también en precario esa «democracia horizontal» (Cebrián, 2008: 359) que se postula respecto de la web 2.0.

Sin embargo, y como muestra de la ambigüedad jurídica existente, la Audiencia Nacional en su sentencia 2148/2007, de 24 de abril, discrepante con una resolución de la AEPD, anuló la sanción impuesta –por publicar en un web datos de carácter personal sin consentimiento–, al aceptar que, en ese caso, lo publicado en un web debía considerarse como publicado en un «medio de comunicación».

«A los efectos que aquí nos interesan y en un caso como el presente, en el

1. Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección Primera, Recurso núm. 446/2007, y 449/2007 acumulado, Sentencia 959/2008 de 23 de abril de 2008. Identificador Cendoj: 28079230012008100252.

que una persona publica conscientemente sus datos de carácter personal en su página web, sin establecer ninguna limitación [...] y a la que puede acceder cualquier usuario de la red sin ningún tipo de cortapisa, debe considerarse esa información publicada voluntariamente por el propio afectado en su página web de Internet, como divulgada en un «medio de comunicación», a los efectos del artículo 3.) LOPD que comentamos. El tratamiento de dichos datos, sin haber sido objeto de manipulación o alteración, recogidos de una fuente de acceso público en la que fueron divulgados voluntariamente por el interesado, sin restricciones, no requiere el consentimiento del afectado según la excepción que contempla el apartado 2 del artículo 6 LOPD.» (SAN 2148/2007, FJ 4)².

La normativa de la LOPD, además del consentimiento —que debe ser informado³— obliga a que los datos sean «exactos y puestos al día» (Art. 4.3), una condición imposible de cumplir al ser inevitable que en agendas y archivos periodísticos haya gran cantidad de datos personales inexactos y obsoletos. La infracción es grave y sancionable con entre 60.101,21 a 300.506,05 euros (Art. 44.3.f).

En todo caso, los datos personales de los ficheros deben cancelarse (eliminarse) cuando «hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados» (Art. 4.5); la LOPD proscribire así la práctica de «hacer agenda» propia de todo periodista, ya que conservar los datos adquiridos para futuros contactos *sine die* no se contempla entre las reservas del artículo 8.6 del RDLOPD.

3.2. Los datos personales «especialmente protegidos» como impedimento del periodismo especializado

Para la LOPD «sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que reve-

2. Sentencia 2148/2007 de 24 de abril de 2007 de la Audiencia Nacional, Sala de lo Contencioso, Sección 1, Recurso núm. 304/2005. Identificador Cendoj: 28079230012007100318.
3. Se precisa «consentimiento informado» para los datos guardados en ficheros: «Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco» (Art. 5.1) de todos los derechos que les concede la Ley como propietarios de esos datos; y «cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca [...] dentro de los tres meses siguientes al momento del registro de los datos» (Art. 5.4). «El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa» (Art. 6.1). La LOPD concede el derecho de acceso a los datos guardados en ficheros profesionales a todos los «interesados» que figuren en ellos. «El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos» (Art. 15.1). Al acceso le va unido el derecho de rectificación y cancelación de datos (Art. 16.1).

len la ideología, afiliación sindical, religión y creencias» (Art. 7.2), consecuentemente, son ilegales y sancionables en grado máximo los cientos de datos que figuran en cualquier fichero profesional de un periodista y que identifican a políticos, sindicalistas, clérigos y otros ideologizados profesionales, ya que ningún periodista solicita a sus contactos y sujetos noticiables autorización escrita para archivar sus datos con la referencia ideológica que ya les identifica públicamente ante toda la sociedad.

Es ilustrativa la sanción de 300.506,05 euros impuesta por la AEPD por tratar un dato político público. Resumiendo lo fundamental, el Tribunal Supremo, en sentencia de 25 de enero de 2006, ratificó tal sanción argumentando lo siguiente⁴:

Hechos: «1.- En el mes de marzo de 1999, D. ..., Director del Gabinete del Viceconsejero de Seguridad del Gobierno Vasco, recibe en su lugar de trabajo un envío publicitario remitido por el Hotel C. V., invitándole a una fiesta. 2.- En el sobre de la invitación aparece el nombre, apellido, dirección profesional y las siglas “PNV”. 3.- La entidad recurrente y propietaria del hotel que envió la invitación es la titular del fichero automatizado denominado “Mailing98.MDB” y “Mailing.MDB”. 4.- En estos ficheros aparecen registrados los siguientes datos del denunciante ante la Agencia de Protección de Datos, D. ..., nombre, apellidos, cargo, partido, institución y domicilio laboral⁵. 5.- En la guía de comunicación del Gobierno Vasco⁶ constan los datos del citado denunciante referentes a su nombre, apellidos, cargo, dirección profesional y de correo electrónico y teléfono. 6.- El nombramiento del denunciante ante la Agencia de Protección de Datos como Director del Gabinete del Viceconsejero de Seguridad, se produjo por Decreto 476/1991, de 30 de agosto, publicado en el Boletín Oficial del País Vasco de 6 de septiembre de 1991».

Razonamiento sancionador: «en el presente caso, y al haberse tratado informáticamente los datos referidos a la pertenencia a un partido político de una persona, la decisión sancionadora resulta adecuada a derecho [...] dado que, en contra de lo afirmado por la recurrente, sí existe el tratamiento de un dato relacionado con la ideología personal y dicho tratamiento se ha producido sin el consentimiento expreso del afectado, [...] resulta en absoluto irrelevante, a los efectos de este motivo de casación, la invocada publicidad sobre la pertenencia del denunciante al partido PNV así como las manifestaciones del mismo dirigidas a la Agencia de Protección de Datos o el resultado de la cuenta de pérdidas y ganancias de la empresa sancionada» (FJ 2).

Ante la alegación del sancionado de falta de dolo y culpa, el Tribunal Supremo fue contundente: «el principio de culpabilidad consiste en la falta de

4. Tribunal Supremo, Sala Tercera de lo Contencioso-Administrativo, Sección Sexta. Sentencia de 25 de enero de 2006.

5. Igual que en cualquier agenda de un periodista, aunque la inmensa mayoría de éstos, además, serían sancionados por no tener registradas sus agendas ante la AEPD.

6. Esta guía, como la mayoría de fuentes de datos usadas por periodistas, no es una «fuente accesible al público» para la LOPD, por lo que usar sus datos es sancionable.

diligencia observada por la entidad recurrente al tratar de forma automatizada un dato relativo a la ideología del denunciante, resultando irrelevantes las invocaciones [...] acerca de la ausencia de intencionalidad o a la existencia del error, y ello por cuanto el elemento culpabilístico del tipo sancionador aplicado concurre cuando se incluye el expresado dato sobre la ideología, no siendo precisa la concurrencia de una intencionalidad específica tendente a revelar datos privados del afectado» (FJ 3).

Todos los periodistas especializados en ámbitos cuyos protagonistas posean «ideología, afiliación sindical, religión y creencias», datos que deben ser reflejados en sus agendas y archivos, incurren en idéntico ilícito administrativo, sancionable con 300.506,05 euros. Máxime cuando el Art. 7.4. afirma taxativamente que «quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual». Tal conducta prohibida es, precisamente, la que debe cultivar con precisión cualquier periodista especializado en política, sindicalismo, religión, esoterismo, antropología, inmigración, sexología y otros ámbitos relevantes (Rodríguez, 2009b: 424-425).

Tampoco pueden mantenerse en agendas y archivos datos identificativos de representantes de colectivos gitanos, africanos, escandinavos, chinos, musulmanes o de cualquier otro «origen racial», ni de colectivos de afectados por cualquier enfermedad causa de asociacionismo, ni de colectivos de homosexuales, transexuales, etc., a tenor del Art. 7.3: «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». Ningún periodista ni medio de comunicación tiene consentimiento escrito de los «afectados» para tener y tratar este tipo de datos.

En el mismo caso están los periodistas especializados en tribunales, economía o sociedad, dado que: «los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes» (Art. 7.5). Cabe recordar que la LOPD (Art. 3.j) no considera «fuentes de acceso público» las sentencias judiciales ni los Registros «públicos» (mercantil, de la propiedad, etc.) usados habitualmente por periodistas y ciudadanos en general.

4. Libertad de información vs. protección de datos, una confrontación mal resuelta

La confrontación entre el derecho fundamental a la libertad de información y a la autodeterminación informativa es un hecho cotidiano que, sin embargo, está lejos de haber sido resuelto adecuadamente.

El artículo 9 de la Directiva 95/46/CE dispone que: «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».

Pero «la Ley Orgánica 15/1999 sin embargo no recoge expresamente exenciones o excepciones al régimen de tratamiento de datos personales en ella contenida con fundamento en la libertad de expresión o información, por lo que será preciso ponderar los intereses en conflicto para poder determinar cuál de ellos debe prevalecer [...] Serán las circunstancias concretas de cada caso las determinantes de la prevalencia de uno u otro derecho. Para ello debemos atender a la naturaleza de la información que se facilita, la finalidad perseguida, el [medio] utilizado, el número de destinatarios posibles, la existencia de intereses generales en la obtención de ese tipo de información y su afectación al derecho a la propia imagen en su manifestación de autodeterminación informativa» (SAN 5744/2008, FJ 7)⁷.

Según Lucas Murillo (2007: 22) «las leyes, al menos las dictadas en España, han trazado un marco general de protección de datos que, si bien tiene la ventaja de contar con normas abiertas susceptibles de ser aplicadas a una multiplicidad de supuestos de hecho, en cambio, tiene que afrontar la dificultad que representan las particularidades de algunos ámbitos especialmente complejos, necesitados, por tanto, de una consideración singular, con la que no contamos».

Esa dejación del legislador para regular exenciones y excepciones para los «fines exclusivamente periodísticos» permitida por la Directiva 95/46/CE, obliga a judicializar la práctica profesional de los periodistas hasta extremos absurdos y tremendamente onerosos para éstos, aportando inseguridad jurídica a los profesionales y a todos cuantos quieran ejercer su derecho a la libertad de información y de expresión.

Estamos con Martínez (2007: 55) cuando afirma que «ello conduce a situaciones complejas, ya que no parece existir ninguna duda sobre la prevalencia del derecho a la información cuando, con motivo de la difusión de una información por un medio de comunicación social, exista un tratamiento de datos personales. Sin embargo, ¿qué ocurrirá cuando el ejercicio de este derecho se produzca en un boletín de información sindical o en el blog de un ciudadano? Parece evidente que si se dan las condiciones exigibles para un correcto ejercicio del derecho a la información, éste debería prevalecer [...] Estamos de nuevo ante un conflicto, cuya solución parece aparentemente clara, pero que obliga a ponderar en cada ocasión los bienes en presencia».

Pero lo que parece claro no lo es y los procedimientos sancionadores ante lo que parecía un legítimo ejercicio de la libertad de información se acumulan en la AEPD y en las Salas de lo Contencioso.

7. Audiencia Nacional, Sala de lo Contencioso, Sección Primera, Sentencia 5744/2008 de 1 de octubre de 2008, sobre Recurso 1/2007. Identificador Cendoj: 28079230012008100734.

Mientras la LOPD define muy restrictivamente qué es un medio de comunicación y una fuente accesible al público, marcando la pauta a las resoluciones sancionadoras de la AEPD, ésta, desde otras resoluciones, hace suya una doctrina más abierta y aparentemente contradictoria con la base de muchas de sus sanciones:

«La expresión “cualquier medio” recogida en el precepto constitucional del Art. 20.d. de la CE —derecho “a comunicar o recibir libremente información veraz por cualquier medio de difusión”— permite aceptar todo posible medio de reproducción o de difusión. La falta de especificación hace que sea admisible cualquier procedimiento de divulgación [...] El Tribunal Constitucional declaró que “no hay inconveniente en entender que el derecho de difundir las ideas y opiniones comprende en principio el derecho de crear los medios materiales a través de los cuales la difusión se hace posible.” (STC 12/1982). 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 (STC 105/1983, STC 107/1988) y atendiendo a la veracidad de la información facilitada (STC 6/1988, STC 105/1990, STC 240/1992).»

Según lo anterior, parece que la AEPD entremezcla dos derechos de naturaleza muy diferente, el de la libertad de información y el de la libertad de expresión, agrandando más, si cabe, la confusión, ya que, por ejemplo, no considera que un web o un blog sean medios de comunicación, sino meros ficheros automatizados sometidos a la LOPD, sancionando gravemente a quienes usan esos «canales» pensando que están ejerciendo su derecho a la libertad de información.

Un ejemplo de este proceder es la sanción impuesta a una asociación por publicar en su web los nombres de funcionarios públicos condenados y/o encausados por cometer los delitos contra los que lucha esa entidad:

«Debe precisarse que las concretas conductas sancionadas, nada tienen que ver ni con la libertad de expresión, ni con el derecho a la información, en relación a la tortura y a la denuncia de tan execrable práctica. La probada publicación vía Internet de lo que sin duda y como hemos dicho constituye un fichero (art. 3 de la LORTAD) con los nombres y apellidos de funcionarios públicos denunciados por la comisión de delitos de maltrato o tortura no es una manifestación de los derechos a la libre expresión, y a la información que no puede atribuirse sin más la actora, con la mera remisión a sus fines sociales, sino una clara vulneración del derecho fundamental consagrado en el apartado 4 del art. 18 de la Constitución [...] infringiendo el art. 11 de la Ley 15/99, cuyo artículo 3, en su apartado i) define la cesión o comunicación de datos como “toda revelación de datos realizada a una persona distinta del interesado”.» (STS 3164/2008, FJ 9)⁸.

8. Tribunal Supremo, Sala de lo Contencioso, Sección Sexta, Sentencia 3164/2008, de 26 de junio de 2008, sobre Recurso 6818/2003. Identificador Cendoj: 28079130062008100199.

En otro caso, ya citado, en el que también se publicaron datos personales en un web, la Audiencia Nacional (Sentencia 2148/2007, de 24 de abril), anuló la sanción de la AEPD tras razonar que lo publicado en la web cuestionada debía tenerse como publicado en un «medio de comunicación».

Hay acuerdo en considerar que la libertad de información, cuando cumple los requisitos constitucionales, debe primar sobre la autodeterminación informativa, pero la ambigüedad, contradicciones y vacíos legislativos someten a periodistas y ciudadanos a una inseguridad inadmisibile.

Es exacta la afirmación de Carrillo (2006: 115) en el sentido de que entre las señas de identidad del derecho a la información en el constitucionalismo del Estado liberal puede verse que «la consecuencia de este proceso de constitucionalización de la información ha sido el cambio experimentado en la posición del periodista en el proceso informativo. De acuerdo con la jurisprudencia constitucional, el periodista actúa como un sujeto y como un instrumento de la libre expresión, condición que si bien no atribuye al periodista un privilegio especial sí le permite disponer de una protección jurídica adicional».

Pero, en el mejor de los casos, si bien la libertad de información y/o de expresión podría proteger el ejercicio profesional del periodista tras haber publicado su trabajo (en un «medio de comunicación»), éste queda desprotegido en lo fundamental para poder ejercer el periodismo con eficacia y responsabilidad, ya que la LOPD prohíbe y sanciona gran parte de los usos y necesidades que tiene cualquier periodista respecto a la confección y mantenimiento de su agenda y archivos de trabajo (Rodríguez, 2009*b*).

A más abundamiento, en esa limitación jurídica al acceso y tratamiento de datos que todo periodista responsable precisa, se evidencia un «arbitrario, demagógicamente pro-intimidad y clientelar desarrollo legislativo de las regulaciones españolas en materia de acceso a la información pública» (Dader, 2001: 164) y, no por casualidad, «resulta paradójico que las trabas empleadas para negar a periodistas o ciudadanos corrientes el derecho a acceder de forma clara a los archivos administrativos, o incluso a elaborar sus propias bases de datos relacionales, desaparecen, en ocasiones, cuando los implicados son grandes agrupaciones del sector empresarial» (Dader, 2001: 165).

Esta situación de desprotección se agrava todavía más al considerar que para defenderse de una sanción de la AEPD debe acudir al litigio contencioso contra la Administración, asumiendo un alto coste económico ya que, aunque se gane, jamás puede recuperarse lo gastado en el proceso.

El ejercicio del periodismo debe tener límites jurídicos robustos, y sin duda ya los tiene, pero un marco como la actual LOPD puede reducir una actividad fundamental para la salud democrática a mera práctica anecdótica, inhibiendo la información en favor de la superficialidad, la opinión y la propaganda.

Expertos en protección de datos hace tiempo que expresan su temor ante excesos que deberían evitarse: «basta con ver algunos de los temas sobre los que se ha pronunciado el Grupo de Trabajo del artículo 29, las directivas dictadas en relación con el tratamiento de datos de tráfico en las comunicaciones y algunos informes jurídicos dictados por la Agencia Española de Protección de Datos para verificar hasta qué punto se corre el riesgo de reducir la mayor

parte del artículo 18 de la Constitución española a la idea de protección de datos. Es necesario ser conscientes de que, pese a la contundencia del aparato de tutela y sanción que ampara este derecho, ello no supone ni que la protección de datos sea la técnica más eficaz, ni la más adecuada» (Martínez, 2007: 58).

5. Bibliografía

- CARRILLO, M. (2006). *El derecho fundamental a la libertad de expresión: entre la sociedad y el poder*. Ponencia presentada al VII Congreso Internacional de Historiadores de la Comunicación. *Treballs de Comunicació*. Núm. 21, pág. 113-124.
- CARRILLO, M. (2009). «El juez ante el interés informativo» [en línea]. *El País.com*, 30/12/09. [Fecha de consulta: 31/12/09]. http://www.elpais.com/articulo/opinion/juez/interes/informativo/elpepuopi/20091230elpepiopi_5/Tes.
- CEBRIÁN HERREROS, M. (2008). «La Web 2.0 como red social de comunicación e información». *Revista Estudios sobre el Mensaje Periodístico*. Núm. 14, pág. 345-361.
- BRU, E. (2007). «La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. Núm. 5, pág. 78-92. [Fecha de consulta: 05/10/2009].
- DADER, J. L. (2001). «La democracia débil ante el populismo de la privacidad: terror panóptico y secreto administrativo frente al periodismo de rastreo informático en España». *Anàlisi*. Núm. 26, pág. 145-168.
- DAVARA RODRÍGUEZ, M. A. (1997). *Manual de Derecho Informático*. Madrid: Editorial Aranzadi.
- DAVARA RODRÍGUEZ, M. A. (2001). *Nueva guía práctica de protección de datos*. Madrid: Asnef.
- DEL PESO NAVARRO, E. (2000). *Ley de Protección de Datos. La nueva Ley LOR-TAD*. Madrid: Díaz de Santos.
- FREIXAS GUTIÉRREZ, G. (2001). *La protección de datos de carácter personal en el Derecho español: aspectos teóricos y prácticos*. Barcelona: Editorial Bosch.
- HERNÁN ORTÍZ, A. I. (2002). *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*. Madrid: Dykinson.
- LUCAS MURILLO DE LA CUEVA, P. (2007). «Perspectivas del derecho a la autodeterminación informativa». En: «VIII Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. Núm. 5, pág. 18-32. [Fecha de consulta: 05/10/2009].
- MARTÍNEZ MARTÍNEZ, R. (2007). «El derecho fundamental a la protección de datos: perspectivas». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. Núm. 5, pág. 47-61. [Fecha de consulta: 05/10/2009].
- MASIP MASIP, P. (2003). «Presencia y uso de internet en las redacciones catala-

- nas». *Zer*. Núm. 14, pág. 29-42.
- PALOMO, B.; MESO AYERDI, K. (2009). «Perfil y comportamiento de los autores de los blogs destacados en los ciberdiarios de Vocento». *Anàlisi*. Núm. 38, pág. 99-116.
- PÉREZ LUÑO, A. E. (2005). *Internet y la garantía de los derechos fundamentales. Estudios Jurídicos sobre la Sociedad de la Información y Nuevas Tecnologías*. Conmemorativo del XX Aniversario de la Facultad de Derecho de la Universidad de Burgos. Núm. 1, pág. 11-39.
- POULLET, Y.; DINANT, J.-M. (2007). «Hacia nuevos principios de protección de datos en un nuevo entorno TIC». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. Núm. 5, pág. 33-46. [Fecha de consulta: 05/10/2009].
- RODRÍGUEZ, P. (2009a). «El periodismo bajo la Ley Orgánica de Protección de Datos de Carácter Personal». *Cuadernos de Periodistas*. Núm. 16, pág. 67-88.
- (2009b). «La agenda profesional del periodista ante la Ley Orgánica de Protección de Datos de Carácter Personal». *Revista Estudios sobre el Mensaje Periodístico*. Núm. 15, pág. 409-429.
- ROIG, A. (2009). «E-privacidad y redes sociales». En: «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. Núm. 9, pág. 42-52. [Fecha de consulta: 05/10/2009].
- SÁNCHEZ CARBALLIDO, J. R. (2008). «Perspectivas de la información en Internet: ciberdemocracia, redes sociales y web semántica». *Zer*. Núm. 25, pág. 61-81.
- SÁNCHEZ, A.; SILVEIRA, H.; NAVARRO, M. (2003). *Tecnología, intimidad y sociedad democrática*. Barcelona: Icaria.
- TEJEDOR CALVO, S. (2008). «La enseñanza del ciberperiodismo en las materias de producción periodística en las licenciaturas de Periodismo». *Revista Estudios sobre el Mensaje Periodístico*. Núm. 14, pág. 617-630.
- VILASAU, M. (2008). «El fin de la situación de transitoriedad: la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal ya tiene desarrollo reglamentario» [artículo en línea]. *IDP. Revista de Internet, Derecho y Política*. Vol. 7. UOC. [Fecha de consulta: 05/10/2009].
- VIZCAÍNO CALDERÓN, M. (2001). *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid: Cívitas.

Pepe Rodríguez es doctor en Psicología por la Universidad de Barcelona, licenciado en Ciencias de la Información por la Universidad Autónoma de Barcelona, profesor del máster de Comunicación Empresarial del IL3 de la Universidad de Barcelona y profesor del Departamento de Periodismo y Ciencias de la Comunicación de la Universidad Autónoma de Barcelona.
