¿Existe privacidad? [1]

José Luis Piñar Mañas

Para conmemorar la más gloriosa
de las noches, el Gobierno de Su Majestad
se complace en devolverles a ustedes,
sus leales súbditos, el derecho a la privacidad.
Durante tres días, sus movimientos no serán vigilados
sus conversaciones no serán escuchadas…
y el "haz lo que quieras" será la única ley.
Buenas noches y que Dios les bendiga

Alan Moore y David Lloyd
V de Vendetta

El Presidente y co-fundador (en 1982) de Sun Microsytems, Scott McNealy, llegó a decir ya en 1999 que debemos resignarnos a no tener privacidad: "You already have zero privacy. Get over it"[3]. A veces ha matizado algo su afirmación, en un sentido en mi opinión igual de descorazonador (o más, si cabe): si tenemos privacidad es porque alguien tolera que la tengamos[4].

Soy consciente de que no pocos consideran que el término privacidad no es acertado. Asumo asimismo que es un concepto controvertido, neologismo para unos, barbarismo para otros[5], al que a veces se da un contenido que puede ser confuso[6]. Lo utilizo ahora, sin embargo, conscientemente, como término, además, no coincidente con el de intimidad, cuyos contornos y alcance son más limitados. En cualquier caso, está incluido en el Diccionario de la Real Academia, que define privacidad como "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". El *Oxford English Dictionary* define *Privacy* como "estado en que uno no es observado o disturbado por otros" ("a state in which one is not observed or disturbed by others"). Y, sobre todo, es un concepto con presencia y contenido en el ámbito de las ciencias y de la investigación. Filósofos, sociólogos, psicólogos, arquitectos, ambientalistas, economistas, médicos y

Catedrático de Derecho Administrativo. Ex-Director de la Agencia Española de Protección de Datos

por supuesto juristas se han ocupado de la privacidad como tal. Por eso en los próximos minutos me atreveré a proponer algunas reflexiones sobre la misma. Reflexiones que girarán en torno a tres puntos. Primero, intentaré ofrecer una definición de privacidad; a continuación me referiré a los riesgos reales a los que la privacidad está hoy sometida; por último veremos las soluciones que desde el Derecho pueden ofrecerse para intentar garantizar un nivel mínimo de privacidad. Todo ello, por supuesto centrado en torno al ser humano en cuanto titular del derecho a la privacidad.

I. En torno al concepto de privacidad

Cuando hablo de privacidad no pretendo referirme en general a la "vida privada"[7], sino a un concepto más reciente, que en su configuración actual ha surgido seguramente a finales del siglo XIX. Desde luego no es nada sencillo definir la privacidad. Robert GELLMAN advierte que ninguna definición es posible ("no definition is possible")[8] y Judith Jarvis THOMSON ha dicho que "nadie parece tener una clara idea de lo que es" ("nobody seems to have any very clear idea what it is")[9]. El propio Tribunal Europeo de Derechos Humanos ha señalado que el de privacidad es "un concepto amplio no susceptible de una definición exhaustiva" ("Private life is a broad term not susceptible to exhaustive definition")[10].

Quizá ha sido en el campo de la psicosociología y la filosofía donde con más ímpetu se ha propuesto un concepto de privacidad[11]. Autores como ALTMAN[12], PEDERSEN[13] o NEWELL[14] son referencia obligada. También, por supuesto, en el campo del Derecho[15]. Aquí es obligada la referencia al juez americano Thomas COOLEY que ya en 1888 acuño la conocidísima definición de privacidad como "the right to be let alone" [16], el derecho a ser dejado solo, a ser dejado en paz; definición que hicieron famosa WARREN y BRANDEIS en su también famoso artículo "The Right to Privacy" [17], al que más adelante volveré a referirme. Tal concepto, aunque todavía digno de ser tenido muy en cuenta, ha sido desde luego superado[18]. En este sentido, las aportaciones de WESTIN son sin duda de capital importancia[19]. A él se debe precisamente la definición de privacidad en términos de autodeterminación, de "*self determination*"[20], concepto éste que más tarde fue expresamente asumido por el Tribunal Constitucional Federal Alemán en su conocida sentencia de 15 de diciembre de 1983 sobre el Censo, y que también ha sido utilizado por nuestro Tribunal Constitucional[21], como más adelante veremos.

WESTIN identificó cuatro tipos de privacidad, que PEDERSEN amplió hasta cinco: soledad, aislamiento, reserva, intimidad y anonimato. La primera, la soledad, se refiere a la situación en virtud de la cual los demás no pueden ver u oír lo que una persona está haciendo; el aislamiento implica la existencia de una distancia física para separarnos

de los demás; reserva significa controlar la revelación verbal de información a los otros; y el anonimato se consigue no siendo identificado entre la multitud. También, como señalaba, se habla de intimidad. Intimidad con los amigos e intimidad con la familia, que permitiría estar sólo con un grupo de personas excluyendo a los otros. GARZON VALDES ha distinguido entre lo íntimo y lo privado[22]. Pero lo que identifica por igual a los expresados tipos de privacidad es que en todos ellos el individuo debe poder controlar el nivel de interacción con los otros. La idea del control es la clave esencial de la privacidad, ocupa el papel central. WESTIN, como antes adelantaba, es quizá quien primero y con más énfasis ha resaltado la importancia del control: la privacidad implica libertad para elegir qué se desea comunicar, cuándo y a quién, manteniendo el control personal sobre la propia información[23]. Se ha hablado de la privacidad como "el derecho a controlar la información"[24].

Este poder de control ha de ponerse en íntima relación con el consentimiento, que ha de ser el título esencial que justifique ingerencias en nuestra privacidad. No el único, pues es posible prever supuestos en que, incluso sin consentimiento de la persona, se permita el uso legítimo de la información que le concierna. Pero estamos introduciendo ya elementos jurídicos en la definición que en principio quería tener un alcance más general.

Incluso estudios empíricos han demostrado que para el individuo ese control es capital: se ha constatado que quienes perciben que mantienen el control sobre el uso que se hace de sus datos tras haberlos facilitado a un tercero sienten su privacidad menos invadida que quienes piensan que han perdido el control sobre ellos. De hecho, la violación del derecho de una persona a controlar su esfera privada, sea ésta física o informativa, constituye el factor más importante para que se sienta invadida la privacidad. No es para ello necesario que la información sea más o menos importante o sensible. Una persona puede hacer pública información que le afecte sin que por ello considere violada su privacidad. Pero si pierde el control sobre ella, si alguien se la apropia, entonces pensará que su intimidad ha sido violada[25]. Quien en alguna ocasión ha facilitado o ha permitido el acceso a su propia información no por ello renuncia a su privacidad

Una reciente Sentencia de nuestro Tribunal Supremo[26], analizando el alcance del derecho a la intimidad[27], ha declarado que no es posible "fisgar" (*sic*) en la intimidad de las personas para satisfacer el "chismorreo" (*sic*) de la gente sin el consentimiento del interesado. Ratifica la condena a una revista "del corazón" y subraya que obtener fotografías a una famosa cantante en su finca particular sin su conocimiento y publicarlas sin su consentimiento constituye una intromisión ilegítima en la intimidad. El derecho a la propia imagen, dice la sentencia, tiene un aspecto positivo, que es la facultad del interesado de difundir o publicar su propia imagen, pero esto no elimina "su facultad

de no autorizar o impedir la reproducción de su imagen, siempre que no se encuentre en lugar público, al tratarse de una persona con proyección pública". Analiza también el alcance del consentimiento del afectado: el consentimiento prestado en otras ocasiones anteriores a que se publicasen fotografías tomadas en su finca "no puede suponer que se autorice para lo sucesivo que, de modo subrepticio y utilizando medios ópticos de fotografía capaces de obtener imágenes a notable distancia" se puedan reproducir las escenas captadas. El consentimiento "debe versar sobre la obtención de la imagen y sobre su concreta publicación en un determinado medio de comunicación social". Y deja claro que "los usos sociales no justifican indagar –"fisgar"- en los asuntos que pertenecen a la esfera exclusiva de otros y divulgar su resultado con el fin de satisfacer la curiosidad o el chismorreo de los consumidores de este tipo de revelaciones o comentarios". Como podemos comprobar se pone el acento en el control sobre la propia información, sobre ese poder de disposición a que me refiero.

El sentido de privacidad, la posibilidad de actuar y expresarse libremente, sin miedo a perder el control sobre la propia información, genera "bienestar físico y psicológico, así como espiritual" como se ha demostrado desde la psicología[28]. La pérdida de la privacidad le producía a William FAULKNER tal sentimiento que pensaba que con ello desaparecía el "sueño americano", el sueño del individuo libre[29]. Se ha afirmado incluso que la función principal de la privacidad es la protección de la estabilidad y del bienestar psicológico de las personas[30]. Estudios recientes, incluso, han empezado ha hablar del llamado *"Síndrome del Show de Truman",* en alusión a la conocida película: el pasado 29 de agosto, hace apenas unos días por tanto, algunos medios se hacía eco de la advertencia que algunos psiquiatras y psicólogos habían hecho afirmando que la sociedad de la vigilancia está provocando un nuevo tipo de psicosis generado por la idea de estar constantemente vigilado por video cámaras o a través de Internet[31].

Nuestro Tribunal Constitucional, en la Sentencia 233/2005, de 26 de septiembre (Fundamente Jurídico 4) afirma que "el derecho a la intimidad personal garantizado por el art. 18.1 CE, en cuanto derivación de la dignidad de la persona reconocida en el art. 10.1 CE, implica "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" (STC 70/2002, de 3 de abril, FJ 10.a; en el mismo sentido la STC 231/1988, de 2 de diciembre, FJ 3)". Incluso el desasosiego y las molestias difícilmente soportables que produce el exceso de ruido se han reconducido hacia su consideración como violación de la intimidad personal y familiar, como ya propusiera hace años entre nosotros Lorenzo MARTIN-RETORTILLO[32]

Esa posibilidad de control sobre la propia información, excluye, desde luego, el control por otros. Somos nosotros mismos los que hemos de poder controlar el grado de privacidad que deseamos tener, y hasta donde queremos abrirnos a los demás sin in-

gerencias externas injustificadas. Como recuerda RODOTA[33], L. M. FRIEDMAN ha señalado que la privacidad se basa en la "tutela de las opciones vitales contra cualquier forma de control público y de estigmatización social"[34] y F. RIGAUX ha llamado la atención acerca de la necesidad de garantizar "la libertad de las opciones existenciales"[35]. La privacidad es una condición de independencia respecto a la influencia y el poder de otros[36].

En definitiva, el fundamento de la privacidad se encuentra en el respeto a la identidad y dignidad de las personas[37], así como a la libertad. No creo que sea tan evidente la diferencia entre los modelos americano y europeo que en cuanto al lugar que ocupa la dignidad en este campo ha señalado WHITMAN[38], que parte de la inexistencia de una común "intuición" acerca de lo que debe entenderse por privacidad. No es cierto, dice, que la privacidad sea un valor absoluto en todo momento y lugar porque hay ejemplos en la historia y en las sociedades de situaciones que hoy consideramos claramente contrarias a la intimidad y que en absoluto eran tenidas como tales. Reconduciendo el dilema a parámetros jurídicos actuales, WHITMAN afirma que los sistemas europeos de protección de la privacidad son, en el fondo, "formas de protección del derecho a ser respetado y a la dignidad personal". En su esencia, el derecho a la privacidad es el derecho a la propia imagen, nombre y reputación; el derecho a controlar la información que se refiera a nosotros mismos, a la autodeterminación informativa, según el concepto acuñado por la doctrina alemana. Por el contrario, América se orienta hacia los valores de la libertad, y sobre todo libertad frente al Estado. El núcleo del derecho, en este caso, es el derecho a la libertad frente a las intrusiones del Estado. El principal riesgo es que "la santidad de nuestros hogares", "the sanctity of [our] homes," se vea amenazada por los poderes públicos. He aquí, para WHITMAN, la diferencia, el contraste entre ambos sistemas: "Por un lado tenemos un Viejo Mundo en el que aparece extraordinariamente importante no perder la propia imagen pública; por otro lado, un Nuevo Mundo en el que lo importante es preservar el propio hogar como fortaleza de la soberanía del individuo"[39]

Como antes decía, no creo que tal planteamiento sea correcto[40]. Ya hemos visto más atrás que, desde la obra de WESTIN, la idea del control sobre la propia información está también en la base de la moderna concepción norteamericana de privacidad. Ésta, allí y en Europa, es esencial para considerar respetada la dignidad del ser humano y para su propia libertad. Stefano RODOTA lo ha demostrado genialmente y hasta la saciedad[41]: sin privacidad, tanto la dignidad como la libertad resultan sustancialmente afectadas hasta el extremo de poder, sencillamente, desaparecer o ser meramente testimoniales.

La privacidad es, pues, condición indispensable para poder afirmar que una sociedad es democrática y respetuosa con los derechos fundamentales, pues sin ella, como acabo de decir, no puede hablarse ni de respeto a la dignidad ni de libertad. La pregunta

entonces es: ¿realmente vivimos en un mundo en el que puede afirmarse que la privacidad existe? ¿Es verdad que las amenazas y tensiones a que está sometida sólo pueden conducirnos, como aventuraba Scott McNEALY, a la resignación ante la idea de que no tenemos privacidad o, si la tenemos, es porque alguien así lo tolera? ¿Cuáles son los ataques a los que hoy está sometida la privacidad?

II. Los ataques a que hoy esta sometida la privacidad

En mi opinión la privacidad está sometida a diversos retos o tensiones que podrían reconducirse a las existentes en relación con la libertad de expresión, con la transparencia y acceso a la información, con los intereses y evolución del mercado y con la lucha por la seguridad ciudadana[42]. A ellas debe añadirse la derivada del siempre creciente interés por apropiarse de información ajena para fines delictivos. En muchas ocasiones la tensión se convierte en amenaza, sobre todo en lo que se refiere a la seguridad, el mercado[43] y las conductas delictivas. Y tienen siempre el común denominador de basarse en la utilización muchas veces torticera de las nuevas tecnologías, lo que al final puede llevarnos a considerar que la verdadera amenaza para la privacidad proviene del avance tecnológico que se produce en la era de la información. En particular, y en aras de una mayor seguridad mundial, la Patriot Act de 2001, aprobada en Estados Unidos tras los terribles y execrables atentados del 11 de septiembre, es una prueba más que evidente de cómo pueden justificarse medidas intrusivas de la privacidad puestas en práctica por los poderes públicos y apoyándose para ello en el uso de nuevas tecnologías, en ocasiones sin conocimiento de los afectados.

Como ya he señalado en otras ocasiones[44], nunca antes como hoy había sido posible, utilizando las tecnologías que están ya al alcance de casi cualquiera, invadir la privacidad de las personas hasta los límites a los que se está llegando. Pensemos que hoy es posible conocer los contenidos de los correos electrónicos, de las llamadas efectuadas o recibidas mediante teléfonos móviles; que pueden tratarse para múltiples finalidades los datos genéticos; que el uso de datos biométricos está casi a la orden del día; que las nuevas tecnologías pueden afectar grave e intensamente a los derechos fundamentales e incluso pueden condicionar el contenido de las normas jurídicas[45]; que mediante dispositivos de radiofrecuencia[46] es posible no sólo controlar las ventas en un centro comercial sino también localizar personas; que la capacidad de los ordenadores personales y sus funcionalidades se incrementan constantemente al tiempo que se reduce el coste de tales innovaciones -como expresa la llamada "Ley de MOORE"[47]- implicando riesgos potenciales para la privacidad y para la protección de datos personales[48]; que cada vez son más los casos en que se exigen tratamientos y transferencias internacionales de datos, así como

retenciones de datos en aras de la seguridad ciudadana; que la sociedad corre el riesgo de verse sometida a una videovigilancia constante[49].

Piénsese por ejemplo[50] en el uso de las tecnologías de radiofrecuencia (RFID), que permiten sin grandes complicaciones localizar a cualquier persona. Dispositivos tecnológicamente muy simples que hace apenas unos años se consideraban ciencia ficción. Isaac ASIMOV incluye esta conversación es su obra *Los Límites de la Fundación:*

Pelorat dijo:

—Me parece, Golan, que el avance de la civilización no es más que un ejercicio en la limitación de la intimidad.

—Quizá tenga razón. Sin embargo, antes o después tenemos que movernos por el hiperespacio o estaremos condenados a permanecer dentro de un radio de uno o dos pársecs de Términus durante el resto de nuestras vidas. Entonces seremos incapaces de emprender viajes interestelares. Además, al pasar por el hiperespacio sufrimos una discontinuidad en el espacio ordinario. Pasamos de aquí allí, y me refiero a un vacío de cientos de pársecs, algunas veces, en un instante de tiempo experimentado. De repente estamos enormemente lejos en una dirección que es muy difícil predecir y, en un sentido práctico, ya no podemos ser detectados.

—Lo comprendo. Sí.

—A menos, naturalmente, que hayan colocado un hiperrelé a bordo. El hiperrelé envía una señal a través del hiperespacio, una señal característica de esta nave, y las autoridades de Términus saben dónde estamos en todo momento. Esto responde a su pregunta, ¿verdad? No habría ningún lugar en la Galaxia donde pudiéramos escondernos y ninguna combinación de saltos por el hiperespacio nos permitiría eludir sus instrumentos.

—Pero, Golan -dijo Pelorat con suavidad-, ¿acaso no necesitamos la protección de la Fundación?

—Sí, Janov, pero no siempre. Usted ha dicho que el avance de la civilización significaba la continua restricción de la intimidad. Bueno, yo no quiero estar tan avanzado. Quiero libertad para moverme a mi antojo sin ser detectado, a menos que quiera protección. De modo que me sentiría mejor, mucho mejor, si no hubiera un hiperrelé a bordo.

— ¿Lo ha encontrado, Golan?

— No, aún no. En todo caso, podría volverlo inoperante de alguna manera.

— ¿Reconocería uno si lo viera?

— Esta es una de las dificultades. Quizá no lo reconociera. Sé cómo suele ser un hiperrelé y sé cómo examinar un objeto sospechoso..., pero ésta es una nave último modelo, diseñada para misiones especiales. El hiperrelé puede haber sido incorporado a su diseño de forma que no de ninguna muestra de su presencia.[51]

Dispositivos, pues, casi invisibles que a distancia nos controlan sin nosotros saberlo. Algo que ya no es un futurible, sino una realidad. El 19 de julio de 2004 el Primer Ministro Británico declaró que existía la intención de "etiquetar y controlar" vía satélite a los cinco mil criminales ingleses más peligrosos[52].

Piénsese también en el uso de datos genéticos, con consecuencias potencialmente gravísimas para las personas[53] pues puede llegarse a situaciones inimaginables de discriminación. No en vano el Congreso de los Estados Unidos, tras más de diez años de debate en la opinión pública y entre las fuerzas políticas, acaba de aprobar una Ley que prohíbe la discriminación por motivos genéticos, una vez aprobada por el Senado[54], basada en una lógica aplastante: nadie puede sufrir consecuencias negativas por algo que, como la herencia genética, está totalmente fuera de su control. Como ocurre con los datos raciales o étnicos, cuyo uso ilegítimo puede también producir situaciones gravemente discriminatorias para las personas[55]

Microsoft ha presentado ante la Oficina de Patentes de EEUU el programa "Monitoring System 500" que podría estar en el mercado dentro de un año y que permite controlar y analizar prácticamente todos los aspectos del comportamiento de los usuarios de equipos informáticos. El sistema opera mediante sensores inalámbricos instalados en el ordenador que permiten la captación y análisis de las palabras y números utilizados por el usuario así como las páginas web visitadas, pero también el ritmo cardíaco, la respiración, temperatura, presión arterial o expresión facial. A partir de la información obtenida, el sistema puede de inmediato (en tiempo real) detectar el estado de ánimo del usuario, sus frustraciones o situaciones de stress, pudiendo ofrecer en su caso las medidas que se consideren convenientes para superar la situación. Incluso podría detectarse información referente a la honestidad del usuario o, en manos de las fuerzas de seguridad, información sobre conductas ilícitas[56].

Mucho más avanzados están los sistemas de reconocimiento facial, face recognition technologies[57], que mediante cámaras de videovigilancia permiten el reconocimiento facial de las personas; sistema ya en aplicación en algunos lugares y que comenzó a implantarse tras los atentados del 11-S.

Hoy a través de los teléfonos móviles es posible localizar prácticamente a cualquier usuario, y lo malo es que puede hacerse sin conocimiento del interesado y por tanto sin su consentimiento. La Universidad de Bath viene experimentando desde hace tres años y ya puede poner en marcha programas de rastreo de personas a través del sistema de conexión Bluetooth[58]

El desarrollo de lo que se ha venido en llamar ubiquitous computing[59] puede llegar a permitir un seguimiento omnipresente de las personas mediante la interconexión de muy diferentes aparatos y sistemas, lo que a su vez permitirá obtener una información completa de aquéllas sin que tengan conciencia de ello.

La nanotecnología permite ya elaborar dispositivos capaces de captar y elaborar información hasta extremos insospechados y de un modo totalmente desapercibido; tal es el caso de los llamados roboflies, o de los nanobots[60].

La evolución tecnológica, además, no puede evaluarse en términos meramente cuantitativos. Una diferencia sustancial de la revolución tecnológica de ahora en relación con la revolución industrial o los avances científicos que se han producido hasta los años ochenta del siglo pasado es que ahora las nuevas tecnologías son capaces ellas mismas de generar conocimiento, lo que tiene una especial trascendencia al hablar de la privacidad y la protección de datos. El Premio Nobel Gerald EDELMAN ha confirmado ya que en el futuro (un futuro además no muy lejano) será posible crear máquinas conscientes, capaces de usar su memoria y aprender y adoptar estrategias.

Pero si lo que acabo de exponer son en parte proyectos de futuro (muy cercano, por lo demás, casi presente), lo cierto es que los supuestos reales de violación de la privacidad son cada vez más notorios y numerosos. Y no sólo en países con bajo nivel de desarrollo. Desde enero de 2005 hasta el 31 de julio de 2008 los fallos de seguridad informática notificados en Estados Unidos han afectado a un total de 234,467,328 ficheros[61]. En Alemania acaba de conocerse que por 850 Euros es posible acceder ilegalmente a más de seis millones de datos personales, entre ellos números de cuentas bancarias, direcciones, teléfonos, etc.[62] Deutsche Telekom, la mayor empresa de Telecomunicaciones de Europa, ha reconocido haber revisado ilegalmente grabaciones de llamadas telefónicas en 2005. En Reino Unido los casos se multiplican: un dispositivo informático con datos personales de 10.000 delincuentes reincidentes y de 84.000 presos internados en las cárceles de Inglaterra y Gales se ha extraviado recientemente en un nuevo caso de pérdida de documentos confidenciales, que ha confirmado el Ministerio del Interior; el Ministerio de Defensa admitió el pasado mes de julio el robo o el extravío de 747 ordenadores portátiles que guardaban información de ese departamento durante los últimos cuatro años; el Gobierno perdió en junio pasado documentos confidenciales en varios trenes de cercanías, algunos de ellos con datos sobre la red terrorista Al Qaeda y sobre Irak; a finales de 2007, igualmente, un disco informático que contenía nombres y números de cuentas bancarias de millones de personas que reciben subsidios en ese país se perdió cuando era enviado por correo desde una oficina gubernamental a otra. En Italia, a primeros del mes de mayo pasado se hicieron públicos durante unas horas en Internet los datos correspondientes a las declaraciones de la Renta de todos los contribuyentes italianos. Además, hace unos meses se hicieron públicas las conversaciones privadas de numerosas personas que habían sido sometidas a escuchas legales e ilegales. Hace apenas unos días se ha sabido que ocho millones de datos (entre ellos el número de cuenta corriente o tarjeta de crédito) de usuarios de la cadena Best Western han sido robados y, parece, puestos a disposición de grupos mafiosos.

Los ejemplos podrían multiplicarse casi hasta el infinito, y muy bien podría decirse que cualquier situación o circunstancia imaginable es ya posible. Pese a resultar un lugar común citarlo en estos casos, es necesario rememorar de nuevo la famosa denuncia orwelliana del Gran Hermano que todo lo sabe y todo lo escruta, sin posibilidad de eludir su insaciable afán de vigilante omnipresente. Vuelve incluso a recuperarse la idea del *Panópticon* de Jeremy BENTHAM, esa cárcel cuyo diseño permite al carcelero vigilar a todos los reclusos sin que estos sepan siquiera que están siendo observados, lo que haría de ellos dóciles sujetos, al saberse constantemente vigilados. Idea que más adelante teorizó Michael FOUCAULT[63] como forma de vigilancia constante y control social[64]. Se habla de la "vigilancia total"[65]. Algo que las nuevas tecnologías pueden hacer realidad[66]. Como Jeffrey ROSEN ha señalado, estamos sometidos a una "mirada no deseada", que puede destruir nuestra privacidad[67]

No son simples *"horror stories"* sobre el carácter intrusivo de las nuevas tecnologías, sobre el uso y abuso de datos personales[68]. Son situaciones reales que deben hacernos reflexionar sobre cómo es nuestra vida en el entorno de las nuevas tecnologías: cómo es nuestra vida, nuestra libertad y nuestra felicidad tras la explosión digital, según han estudiado ABELSON, LEDDEN y LEWIS[69]. Se ha hablado de la muerte de la privacidad en el Siglo XXI[70]. Desde luego es cierto que hay quien, como Amitai ATZIONI, considera que el exceso de privacidad es contraproducente para la sociedad, y, proponiendo un concepto "comunitario de privacidad" (*communitarian conception of privacy*) aboga por un mayor peso del interés general[71]. Pero aún así no es exagerado afirmar, no me canso de repetirlo, que la dignidad y la libertad están en juego. Y que para ello es imprescindible resaltar con decisión y convicción la importancia que tiene la privacidad y el derecho a la protección de datos de carácter personal. No podemos perder nuestra privacidad como consecuencia de la implantación de nuevas tecnologías[72]

Dicho lo anterior, debo hacer dos consideraciones a modo casi de advertencia.

Primera, hay un peligro extraordinariamente grave en relación con la situación que vengo exponiendo: el de considerar que todas esas medidas amenazantes para la privacidad del ser humano son no solo adecuadas, sino absolutamente necesarias para nuestra seguridad, y que por tanto debemos aceptarlas no sólo resignada sino convencidamente. Medidas que poco a poco van incorporándose a nuestra vida cotidiana y que aceptamos como algo inevitable e incluso positivo. Se incorporan a nuestro moderno y normal modo de vida como un integrante más que ya ni se cuestiona. Hace meses un conocido periodista llegó a escribir una pequeña columna titulada "Es nuestra seguridad, estúpidos", en la que abiertamente justificaba la adopción de medidas intrusivas para la privacidad en aras de una mayor seguridad. Venía de alguna manera a recuperar una vez más aquel ya viejo planteamiento de que quien quiere proteger su intimidad es porque tiene algo que ocultar. Quizá en este momento deberíamos recordar con especial convicción

la famosa frase de FRANKLIN: "Quien sacrifica la libertad en aras de la seguridad no merece ninguna de las dos" ("*He who sacrifices freedom for security deserves neither*").

Debemos reaccionar frente a quienes pretenden convencernos que son medidas beneficiosas para la Humanidad y siempre necesarias para garantizar nuestra seguridad, o que son consecuencias inevitables derivadas de nuestra convivencia con la tecnología. La realidad, muy al contrario, es que la alienación que produce el "juego" de otros con nuestra identidad (utilizando información personal, nuestros datos, y convirtiéndonos en uno más de un conjunto de elementos iguales) pone en riesgo la que Erich FROMM llama "libertad positiva", que "como realización del yo, implica la realización plena del carácter único del individuo"[73]. Por otra parte, al ser invadida nuestra privacidad, al ser sometidos a perfiles (al ser subsumidos o clasificados en perfiles) al diseñar nuestra identidad desde fuera como consecuencia del ataque desapercibido de nuestra privacidad, intimidad o datos personales, al ser o sentirnos constantemente vigilados ¿podemos ser espontáneos y por tanto libres en el sentido de FROMM?[74]. Es indudable que un sistema de vigilancia y control constante y omnicomprensivo es contrario a la espontaneidad y por tanto a la libertad. RODOTA ha señalado que "la posibilidad de construir libremente la propia esfera privada, deriva directamente de una situación en la cual no exista un programa que, de diversos modos, se imponga a la persona"[75], y se ha preguntado: "¿en qué se convertirán las ciudades, no ya concebidas como espacios de libertad, sino como lugares de vigilancia permanente?"[76].

Segunda. En la gran mayoría de las ocasiones, las violaciones a nuestra privacidad nos pasan desapercibidas. No somos ni siquiera conscientes de que se han producido o de que están produciéndose en un momento determinado. Cuando lo cierto es que en la era digital dejamos rastro de casi todo lo que hacemos o decimos, sin ser conscientes tampoco de ello, y sin serlo, por tanto, de que ese rastro puede ser fácilmente seguido, hasta el punto de afirmarse que ninguna faceta de nuestras vidas podrá escaparse de la posibilidad de ser digitalizada[77]. Estoy seguro de que la privacidad de todos los que estamos aquí ha sido hoy mismo amenazada cuando no violada por alguien en algún lugar cercano o remoto. Alguna videocámara, legal o ilegalmente instalada, ha tomado nuestras imágenes; alguien se ha hecho con nuestra dirección de correo electrónico; alguien está utilizando nuestra dirección postal para remitirnos publicidad no deseada. Pero del mismo modo nuestros datos están siendo recabados, sin saberlo, de forma legítima: la ley exige que los operadores de telecomunicaciones retengan los datos de las llamadas que efectuamos o recibimos por nuestros teléfonos móviles; las compañías aéreas deben retener y remitir a Estados Unidos todos los datos de los pasajeros que vayan a volar o ha hacer escala en aquél país; si hacemos una transferencia financiera internacional, los datos de la misma podrán ser consultados por el Departamento del Tesoro de Estados Unidos; cuando nos alojamos en un hotel, nuestros datos son pasados de inmediato a las Fuerzas y Cuerpos de Seguridad.

¿Debemos pues resignarnos a perder la privacidad? ¿Hay algo que podamos hacer?

Ante todo hemos de ser conscientes de que somos nosotros los que primero debemos actuar en defensa de nuestra privacidad. Como vimos más atrás, el control sobre la esfera privada es esencial para considerar respetada nuestra privacidad. En este sentido, son varias las dimensiones de la privacidad en sentido amplio. BURGOON[78] ha distinguido las dimensiones física, social, psicológica y la referente al tratamiento de nuestros datos personales ("information privacy"[79]). Y hay que decir que mientras que el control es más fácil en relación con la privacidad física y social, no lo es tanto respecto a sus dos ulteriores dimensiones. En el caso de la privacidad psicológica y la protección de datos, el acceso por terceros a la información personal puede implicar que el afectado pierda casi definitivamente el control sobre la misma. Esto significa que en relación con cierta información, el individuo sólo tiene la opción de revelarla o no, pues una vez que se pone a disposición de terceros, no tiene posibilidad de recuperarla, lo que hace diferente la gestión de los datos personales respecto a otras dimensiones de la privacidad, pues en este caso es posible cometer "errores irreversibles"[80]. Por eso, como digo, somos nosotros mismos los que primero hemos de poner todas las armas sobre la mesa y adoptar todas las cautelas posibles para proteger nuestra privacidad.

Pero si esa fuese la única solución estaríamos sin duda abocados a la más absoluta de las melancolías, pues poco podemos hacer por nosotros mismos ante la potencialidad de las nuevas tecnologías, que de forma invisible y, como antes decía, ajena a nuestro conocimiento y voluntad, son capaces de recabar información hasta niveles inimaginables. ¿Es entonces posible la defensa y garantía efectiva de la privacidad? ¿Qué podemos hacer, desde nuestra modesta posición, los juristas?

III. ¿Es posible la defensa y garantia efectivas de la privacidad?

Como más atrás ya adelantaba, en 1888 Thomas COOLEY habló ya del "derecho a ser dejado solo", a ser dejado en paz; "the right to be let alone"[81]. En 1890 Samuel WARREN y Louis BRANDEIS publican en la *Harvard Law Review*[82] su famoso artículo "The Right to Privacy". En aquel entonces WARREN y BRANDEIS, impulsados por la necesidad de poner coto a una situación personal en que se había encontrado la esposa de uno de ellos, que sufrió la invasión de su vida privada por diversos periodistas[83], hablaron de un nuevo derecho: "Los cambios políticos, sociales y económicos –expusieron entonces- traen consigo el reconocimiento de nuevos derechos, y el *common law*, en su eterna juventud, acierta a satisfacer las nuevas demandas de la sociedad". Al principio el derecho actuaba sólo frente a las interferencias físicas de la vida y la propiedad. Más tarde se reconoció la naturaleza espiritual del hombre. Gradualmente el objeto de los

derechos se fue ampliando, y ahora el derecho a la vida ha pasado a significar derecho a disfrutar de la vida, que incluye el derecho a que te dejen estar solo. El derecho debe preservarnos frente a las invasiones de los "sagrados límites de nuestra vida privada y doméstica". El derecho a la privacidad supone, pues, el derecho a poder estar solo, con el alcance que cada uno desee, incluso completamente solo, sin sufrir ingerencias no deseadas y sin interferir en el derecho de los demás[84].

La evolución que desde entonces se ha producido ha sido imparable. Los tribunales americanos comenzaron a aplicar y reconocer el nuevo derecho a la privacidad[85], aún más tras las aportaciones de PROSSER y su construcción teórica en torno al concepto de los daños derivados de la invasión de la privacidad (*privacy torts*)[86], mientras que en Europa tanto a nivel constitucional como legislativo y jurisprudencial se ha consolidado ya desde hace años el derecho a la intimidad, a la privacidad y, más recientemente (a partir de los años setenta del pasado siglo) el derecho a la protección de datos.

El derecho al respeto a la vida privada ha sido incorporado a la práctica totalidad de los grandes instrumentos internacionales de reconocimiento de derechos fundamentales. El artículo 12 de la Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1948[87], el artículo 11 de la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica), de 1966[88], el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 19 de diciembre del mismo año 1966[89], el artículo 8 del Convenio Europeo de Derechos Humanos de 4 de noviembre de 1950[90] son ejemplo de ello. Como lo es la Carta de los Derechos Fundamentales de la Unión Europea suscrita en Niza el 7 de diciembre de 2000[91], sobre la que luego volveré. Por otra parte, la práctica totalidad de los textos Constitucionales reconocen asimismo el derecho a la intimidad o privacidad, cuya regulación se deja en manos de legislación específica.

Dicho lo anterior, es posible afirmar que el proceso normativo reciente en relación con la regulación del derecho a la privacidad nace en los años sesenta y setenta del siglo XX.

En 1967 se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar las tecnologías de información y su potencial agresividad hacia los Derechos de las personas, especialmente en relación con su Derecho a no sufrir ingerencias en la vida privada. De tal Comisión Consultiva surgió la Resolución 509 de la Asamblea del Consejo Europa sobre *"los Derechos humanos y los nuevos logros científicos y técnicos"*, que respondía a una inquietud existente en toda Europa.

Es lugar común citar la Ley de Protección de Datos del Estado alemán de Hesse, la primera ley de protección de datos de la historia. En 1973 el Departamento de Salud, Educación y Bienestar de Estados Unidos elabora un Informe sobre las bases de datos telemáticas del Gobierno[92] y propone un Código de buenas prácticas que recogería los principios que han de regir el uso de información por parte del Gobierno (*Fair Infor-*

mation Practices o *Fair Information Principles*): no deben existir bases de datos secretas, se ha de reconocer el derecho de acceso y rectificación de los datos personales, ha de respetarse el principio de finalidad, debe respetarse el principio de calidad y han de adoptarse medidas de seguridad. Un año más tarde, y en base a tal Informe, se aprueba la Privacy Act de Estados Unidos, y van poniéndose las bases de los principios esenciales configuradores del núcleo esencial del derecho a la privacidad. Como se ha señalado, de los *privacy principles* se pasa a las *privacy laws*[93]. Veremos que tales principios fueron en parte el embrión de los que más tarde se recogerían en textos internacionales y en normas europeas y nacionales[94].

El 8 de mayo de 1979 el Parlamento Europeo aprueba una Resolución sobre *"La tutela de los Derechos del individuo frente al creciente progreso técnico en el sector de la informática*". En los años ochenta, desde el Consejo de Europa se dará un respaldo definitivo a la protección de la intimidad frente a la informática mediante el Convenio nº 108 para la Protección de las Personas con respecto al tratamiento automatizado de los datos de carácter personal (1.981). Este Convenio establece los principios y Derechos que cualquier legislación estatal debe recoger a la hora proteger los datos de carácter personal e intenta conciliar el Derecho al respeto de la vida privada de las personas con la libertad de información, facilitando la cooperación internacional en el ámbito de la protección de datos y limitando los riesgos de desviaciones en las legislaciones nacionales.

En fin, también la OCDE publica en 1980 dos importantes Recomendaciones en esta materia: la Recomendación sobre *"Circulación internacional de datos personales para la protección de la intimidad"* y la Recomendación relativa a la *"Seguridad de los sistemas de información",* y unos años más tarde, el 15 de diciembre 1983, el Tribunal Constitucional Alemán dicta su capital Sentencia sobre el Censo en el que, como ya he apuntado más atrás, se reflejan las aportaciones que desde la doctrina (principalmente norteamericana y en particular de la mano de WESTIN) se habían producido en orden a destacar el papel capital que tiene el control sobre la propia información en la configuración del derecho a la privacidad y a la protección de datos. El Tribunal Constitucional Alemán completó los derechos constitucionales de la personalidad a pesar de la inexistencia en la Ley Fundamental de 1.949 de un derecho específico. Sobre la base del derecho a la dignidad humana y al libre desarrollo de la personalidad el Tribunal garantizó la continuidad de las libertades básicas, consagradas con anterioridad, con la formulación de un nuevo derecho, el derecho a la autodeterminación informativa. En la clave de bóveda del ordenamiento de la Ley Fundamental, dice el Tribunal, se encuentra la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre. El derecho general de la personalidad abarca la facultad del individuo, derivada de la autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida, protegiéndole contra la recogida,

el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona. Se garantiza así la facultad del individuo de decidir básicamente por sí sólo sobre la difusión y utilización de sus datos personales. El tratamiento automatizado de datos ha incrementado en una medida hasta ahora desconocida las posibilidades de incidir sobre la conducta del individuo. El que no pueda percibir con seguridad suficiente qué informaciones relativas a su persona son conocidas en determinados sectores de su entorno social y no pueda saber en consecuencia qué se sabe de él, puede coartar substancialmente su libertad de planificar o decidir. Por ejemplo, quien sepa de antemano que su participación en una reunión o iniciativa ciudadana va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de sus derechos fundamentales. De modo que un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, concluye el Tribunal que ya no existe, desde la perspectiva del tratamiento automatizado de datos, ninguno "sin interés".

A partir de esta sentencia, que incorpora a los principios esenciales del derecho a la privacidad el del consentimiento, tal derecho y el derecho a la protección de datos ya no fueron lo mismo en Europa. Aunque todavía faltaba mucho por andar.

En la década de los noventa se incorpora un elemento fundamental al debate. La construcción europea, que requiere ineludiblemente la constitución del mercado interior, exige que se garantice la libre circulación de los datos personales, dado el valor económico que los mismos tienen en las transacciones comerciales, sobre todo en el marco de una economía cada vez más globalizada y transfronteriza. En este escenario se mueve la Directiva 95/46/CE[95] sobre protección de datos, que es sin duda la pieza jurídica más importante que sobre protección de datos existe[96]. Norma que, junto con la jurisprudencia del Tribunal de Justicia dictada sobre la materia[97], ha influido decisivamente en el desarrollo no ya a nivel europeo sino mundial (sin exageración alguna) del derecho a la privacidad y en particular del derecho a la protección de datos[98].

En el año 2000 la situación experimenta un giro copernicano tanto en Europa como en España. Se abre una nueva etapa, en la que ahora nos encontramos, que se basa en la consideración de la protección de datos de carácter personal como un verdadero Derecho fundamental autónomo e independiente del Derecho a la intimidad. Tan radical innovación deriva fundamentalmente de la Jurisprudencia del Tribunal Europeo de Derechos Humanos[99] y de la Carta de los Derechos Fundamentales de la Unión Europea, que consolida definitivamente la diferencia entre el derecho a la privacidad y el derecho a la protección de datos. Al primero dedica un artículo, el 7º[100], mientras que el 8º reconoce de forma expresa y diferenciada el derecho fundamental a la protección de datos de carácter personal[101]. El carácter autónomo del derecho a la protección de datos[102] adquiere así carta de naturaleza al más alto nivel normativo. Privacidad, intimidad

y protección de datos no son conceptos equivalentes. Como ha señalado RODOTA, el reconocimiento de la protección de datos como derecho independiente contribuye a la "constitucionalización" de la persona, que el Preámbulo de la Carta sitúa en el centro de la acción de la Unión Europea[103].

Hay que decir, por cierto, que en virtud del artículo 2º de la Ley Orgánica 1/2008, de 30 de julio, por la que se autoriza la ratificación por España del Tratado de Lisboa, las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán también de conformidad con lo dispuesto en la Carta[104].

En España, ese cambio hacia la consideración del Derecho a la protección de datos como un verdadero Derecho autónomo e independiente viene de la mano de dos importantísimas sentencias del Tribunal Constitucional: las números 290 y 292 de 2000, ambas de 30 de noviembre[105].

La segunda de ellas, en particular, reconoce que el Derecho fundamental a la protección de datos personales deriva directamente de la Constitución y debe considerarse como un Derecho autónomo e independiente. El Fundamento Jurídico Séptimo es sin duda esencial, por lo que creo oportuno transcribirlo:

> 7. De todo lo dicho resulta 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, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del Derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.
>
> Y ese Derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.
>
> En fin, 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[106].

Reconocida ya de forma indudable la existencia de un nuevo derecho, el de la protección de datos, cuya efectividad es esencial para la existencia misma de la privacidad, hay que definir los principios que lo configuran[107]. Tales principios pueden reconducirse a los que quizá son más nucleares en la configuración del derecho: Consentimiento, información, finalidad, calidad de los datos, con especial referencia a la proporcionalidad, seguridad. Principios todos ellos recogidos en la Ley Orgánica de Protección de Datos, artículos 4 y ss., a los que puede añadirse el de utilización leal de los datos y el de minimización en el uso de los datos (éste, por cierto, reconducible, también, en mi opinión, al de proporcionalidad). Principios que para ser efectivos requieren el reconocimiento, garantía y tutela de los derechos de acceso, rectificación, cancelación y oposición (regulados, en nuestro caso, en los artículos 15 y ss. de la LOPD).

Los anteriores principios alcanzan pleno significado desde el reconocimiento de que el derecho a la protección de datos se fundamenta en el poder de disposición de los datos personales por su titular, y en que tales datos son sometidos a tratamiento. Lo que se traduce en que por definición quien trata datos personales trata datos ajenos, no propios, que debe utilizar con estricto respeto a los derechos del interesado. Esta construcción nos reconduce al respeto a la dignidad de la persona, base fundamental de la protección de datos. Y explica perfectamente los principios que antes he mencionado.

En efecto, si los datos sometidos a tratamiento son datos ajenos y su utilización ha de hacerse en el marco del respeto a la dignidad de la persona y a su poder de disposición sobre los datos, es lógico que cuando se recaben datos deba informarse al interesado (arts. 10 y 11 de la Directiva 95/46/CE; art. 5º de la LOPD y arts. 18 y 19 del Reglamento). Que el tratamiento deba estar amparado en un título que habilite su utilización, siendo esencial el consentimiento del titular de los datos (art. 7 de la Directiva y art. 8 de la Carta Europea de Derechos Fundamentales; arts. 6, 7 y 11 de la LOPD; arts. 12 a 17 del Reglamento). Que los datos sólo puedan utilizarse para la o las finalidades legítimas para las que fueron recabados (art. 6.1.a de la Directiva; art. 4 de la LOPD; arts. 8º y 9º del Reglamento), y que ha de respetarse el principio de proporcionalidad y mínima ingerencia en su tratamiento, así como uso leal y lícito (art. 6 de la Directiva; y, de nuevo, art. 4 de la LOPD y arts. 8º y 9º del Reglamento). Y que deben tratarse con seguridad (arts. 16 y 17 de la Directiva; art. 9 de la LOPD; arts. 79 y ss. del Reglamento). Todo ello, además, como he señalado, garantizado a su vez por el reconocimiento a los titulares de los datos de los derechos de acceso, rectificación, cancelación y oposición (arts. 12 y sigs. de la Directiva; arts. 15 y ss. de la LOPD; arts. 23 y ss. del Reglamento),

imprescindibles para garantizar ese derecho de disposición de los datos que está en la base misma del sistema.

Además, la Carta Europea de Derechos Humanos, siguiendo ya la tónica de textos anteriores, da un paso capital a favor de otro de los principios que ya son inherentes a la protección de datos: el principio que podría denominarse de control independiente. En efecto, al disponer que "*El respeto de estas normas [de protección de datos] quedará sujeto al control de una autoridad independiente*" está exigiendo la existencia de tal autoridad como requisito para considerar que el derecho a la protección de datos está suficientemente garantizado. De modo que se presume que, faltando esa autoridad, no es posible en ningún caso considerar aceptable el marco jurídico regulador del derecho. Precisamente uno de los puntos esenciales de las decisiones de adecuación que hasta ahora ha aprobado la Comisión Europea en relación con la protección ofrecida por terceros países es la de la existencia de una autoridad independiente de control.

En cuanto a la privacidad propiamente dicha, se ha dejado firmemente sentado que es un derecho que ha de reconocerse a todas las personas. El Tribunal Constitucional, así lo ha recordado, por ejemplo, en relación con los presos. En las Sentencias 89/2006, de 27 de marzo, y 89/1987, de 3 de junio ha señalado que "una de las consecuencias más dolorosas de la pérdida de la libertad es la reducción de lo íntimo casi al ámbito de la vida interior, quedando, por el contrario, expuestas al público e incluso necesitadas de autorización muchas actuaciones que normalmente se consideran privadas e íntimas", lo que exige preservar especialmente los ámbitos de intimidad no concernidos por la pena o la medida y por su ejecución, y de declarar "ilegítimas, como violación de la intimidad y por eso también degradantes, aquellas medidas que la reduzcan más allá de lo que la ordenada vida de la prisión requiere"[108].

También ha subrayado el Tribunal (Sentencia 233/05, F.J. 4, último párrafo) que "para que la afectación del ámbito de intimidad constitucionalmente protegido resulte conforme con el art. 18.1 CE, es preciso que concurran cuatro requisitos: en primer lugar, que exista un fin constitucionalmente legítimo; en segundo lugar, que la intromisión en el derecho esté prevista en la ley; en tercer lugar (sólo como regla general), que la injerencia en la esfera de privacidad constitucionalmente protegida se acuerde mediante una resolución judicial motivada; y, finalmente, que se observe el principio de proporcionalidad, esto es, que la medida adoptada sea idónea para alcanzar el fin constitucionalmente legítimo perseguido con ella, que sea necesaria o imprescindible al efecto (que no existan otras medidas más moderadas o menos agresivas para la consecución de tal propósito con igual eficacia) y, finalmente, que sea proporcionada en sentido estricto (ponderada o equilibrada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto) [SSTC 207/1996, de 16 de diciembre, FJ 4; y 70/2002, de 3 de abril, FJ 10 a)]". En la Sentencia 89/2006, de 27

de marzo, el Tribunal ha señalado: "En este sentido, hemos destacado (SSTC 66/1995 y 55/1996) que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: "si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"" (STC 207/1996, de 16 de diciembre, FJ 4.e)".

Vemos por tanto que el artículo 18 de la Constitución de 1978, en sus cuatro apartados, es el punto de referencia entre nosotros[109]. Y con él, las leyes que lo han desarrollado, de entre las que me permitiría destacar 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, con sus modificaciones[110], los diversos preceptos del Código Penal referentes al tema, y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, complementada por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la misma[111]. Además, son múltiples las leyes que directa o indirectamente regulan aspectos relacionados con la privacidad[112].

Desde el Derecho, pues, se articulan instrumentos de reacción frente a las constantes amenazas a que está sometida nuestra privacidad, sobre todo, como vengo insistiendo, frente al uso de las nuevas tecnologías. No en vano las primeras leyes sobre protección de datos nacen precisamente en los años setenta del sigo XX, cuando comienza a implantarse el uso de los primeros computadores o cerebros electrónicos, que ahora nos parecen absolutamente rudimentarios. El legislador supo reaccionar a tiempo y, a través de textos internacionales, leyes nacionales, y de la jurisprudencia se han ido fijando las reglas del juego que, con el valor de lo jurídico –no siempre suficientemente efectivo, hay que decir- pretenden evitar la desaparición de la privacidad y la protección de datos.

Pero, ¿es suficiente la respuesta del derecho tal como acabo de exponerla? BENNETT y RAAB consideran que las leyes de protección de la privacidad y de protección de datos sólo pueden tener un "impacto marginal" en el desarrollo de la sociedad de la vigilancia[113]. HOLTZMAN considera que las leyes de protección de datos "no funcionan particularmente bien"[114]. RULE considera incluso que en no pocas ocasiones las leyes que regulan el derecho a la privacidad son utilizadas para legitimar la introducción de nuevos sistemas de vigilancia[115]. LAPERRIÈRE ha señalado que la legislación de protección de datos parece una solución del pasado[116]. GELLMAN se ha preguntado directamente si el derecho a la privacidad realmente funciona[117].

Tales críticas provienen del otro lado del Atlántico, de la doctrina Norteamericana. Pero no cabe duda de que algo de verdad hay en lo que dicen. Porque parece evidente que el recurso a la ley, a la heterorregulación no es quizá por sí sólo remedio suficiente para garantizar de forma efectiva nuestro derecho a la privacidad y, más en particular, a la protección de datos de carácter personal.

Lo anterior en absoluto debe interpretarse en el sentido de que la ley es un instrumento ineficaz. En Europa, en los sistemas del *Civil Law*, seguimos creyendo en la bondad de la ley. Sobre todo si consideramos que estamos ante derechos fundamentales cuya regulación debe reservarse precisamente a la ley. Además, la interpretación que de la ley hacen los jueces y tribunales permite avanzar en el reconocimiento de los derechos y en una nueva configuración de los mismos adaptada a la nueva realidad social y, también, tecnológica. El Derecho, ante los avances tecnológicos, sigue evolucionando para hacer frente a nuevos y sofisticados ataques que pueden amenazar su contenido y razón de ser. En este sentido, y vuelvo al Tribunal Constitucional Alemán, tan importante como ejemplar es su Sentencia de 27 de febrero de 2008[118]. La sentencia es fruto del recurso interpuesto contra la reforma de la ley de los servicios de inteligencia del Estado de Renania del Norte Westfalia, en virtud de la cual se permitía expresamente que tales servicios pudiesen utilizar de forma secreta *spywares* troyanos para espiar los ordenadores de cualquier sospechoso: penetran en los ordenadores y captan todo tipo de información, que luego puede ser analizada. El Tribunal declara inconstitucional la reforma y configura, por primera vez, lo que se ha considerado ya como un nuevo derecho fundamental a la protección de la confidencialidad e integridad de los sistemas tecnológicos de información. El Tribunal de Karlsruhe da así un paso más en el reconocimiento, primero, del derecho a la autodeterminación informativa (en 1983 como ya sabemos) y más tarde del derecho a la protección absoluta de la zona nuclear ("core area") del comportamiento privado ("private conduct of life"). El Tribunal llega al siguiente razonamiento: "De la relevancia del uso de los sistemas tecnológicos de información para expresar la personalidad y de los peligros que para la personalidad representa tal uso, deriva una necesidad de protección que es significativa para los derechos fundamentales. El individuo depende de que el Estado respete las expectativas justificables de confidencialidad e integridad de tales sistemas de cara a la irrestricta expresión de su personalidad"[119]. Los sistemas de información protegidos por este nuevo derecho son todos aquellos (ordenadores personales, PDAs, teléfonos móviles…) que solos o interconectados con otros pueden contener datos personales del afectado de modo que el acceso al sistema permite hacerse una idea sobre aspectos relevantes del comportamiento vital de una persona o incluso obtener una imagen representativa de su personalidad[120]. Este derecho a la integridad y confidencialidad de los sistemas tecnológicos de información, que tendría la consideración de verdadero derecho constitucional, sólo puede ser restringido en casos muy limitados.

Sólo en casos de evidencia de un peligro concreto para la vida, la integridad física o la libertad de las personas, así como para los fundamentos del Estado, los poderes públicos pueden hacer uso de técnicas de registro online. Técnicas que, en consecuencia, no pueden ser utilizadas en las investigaciones relacionadas con delitos "normales" ni en la actividad genérica de los servicios de inteligencia. Y que en cualquier caso requieren la adopción de medidas para proteger el núcleo central de la vida privada ("core area of private conduct of life"), que incluye la información relativa a las relaciones y los sentimientos personales. Por ello, el Tribunal señala que en caso de que de forma accidental se recabasen datos referidos a esa área vital, deben ser suprimidos de inmediato sin que puedan ser utilizados en ningún caso.

Es decir, el derecho a la privacidad alcanza también a los dispositivos informáticos que utilizamos y que forman parte ya de nuestra propia vida, que contienen información que nos identifica y que puede dar una imagen de nuestra personalidad.

Es éste, pues, un paso de gigante en la evolución del derecho a la privacidad y a la protección de datos. Pero los problemas siguen siendo muchos y las herramientas con que contamos no siempre son eficaces. Por eso es necesario buscar nuevas soluciones complementarias.

En este sentido la autorregulación es un instrumento que parece extraordinariamente útil y oportuno. De hecho el modelo norteamericano pivota en gran medida en torno a la autorregulación, a los códigos de conducta, a las políticas de privacidad[121]. Y también en Europa se ha apostado decididamente por esta vía. Así lo hace la Directiva 95/46/CE; así lo hacen las leyes de los Estados miembros de la Unión Europea; y así lo hace la Ley Orgánica de Protección de Datos de 1999, sobre todo tras la aprobación del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, cuyos artículos 71 a 78 contienen una muy razonable regulación de los llamados códigos tipo[122].

También resulta imprescindible reforzar la posición de las autoridades independientes de protección de datos. Ya hemos visto cómo el de control independiente es uno de los principios configuradores del contenido esencial del derecho a la protección de datos[123]. La existencia de tales entidades es requisito imprescindible para que la Unión Europea reconozca respecto de un tercer país que cuenta con un nivel adecuado de protección lo que facilita sobremanera la transferencia internacional de datos. No hace mucho las autoridades de Reino Unido, Alemania y Francia han reclamado mayores competencias y un sistema más riguroso de control y tratamiento de la información.

Por otra parte, la privacidad y el derecho a la protección de datos han de enfrentarse a procesos de globalización y de construcción de instrumentos que permitan garantizar al máximo su eficacia frente a ataques que no saben de límites fronterizos y que provienen en innumerables ocasiones de países en los que no hay en absoluto un marco jurídico de

la protección de la intimidad y en los que por tanto es imposible intentar siquiera poner en marcha mecanismo efectivos de *enforcement*[124]. Uno de los mayores obstáculos que hoy se presentan para conseguir una efectiva garantía y tutela de la privacidad es la falta de instrumentos jurídicos que afirmen la extraterritorialidad de las conductas ilícitas de tratamiento informatizado de la información, en relación con las cuales el territorio físico no tiene, sencillamente, trascendencia alguna.

Así mismo es muy necesario tener en cuenta que numerosas normas y actividades, públicas y privadas, tienen un considerable impacto sobre la privacidad y el derecho a la protección de datos, que no siempre es identificado por quines elaboran unas o llevan a cabo las otras. Es más, me atrevería a afirmar que la gran mayoría de las disposiciones que se adoptan, legales o reglamentarias, tienen una repercusión directa o indirecta sobre los derechos que ahora analizamos. Por ello creo que sería imprescindible introducir mecanismos y/o procedimientos de evaluación de impacto sobre la privacidad[125]. En el ámbito de las nuevas tecnologías cada vez se habla con más frecuencia de la *Privacy Impact Assessment* (*"PIA"*) como metodología que identifica las cuestiones relativas a la privacidad y los potenciales riesgos que para la misma pueden venir asociados con la implantación de nuevas tecnologías[126]. Se trata, pues, de integrar la protección de datos y la privacidad en la actuación de las organizaciones y en el proceso normativo.

En fin, se habla ya de un nuevo principio de la privacidad, el llamado "*Privacy by Design*"[127] en virtud del cual las consideraciones sobre privacidad deben ser incorporadas previamente al diseño de los sistemas informáticos, incluyendo medidas de seguridad para los componentes físicos, así como políticas y protocolos sobre privacidad. Tal modo de actuar, además, ahorrará tiempo y esfuerzos a largo plazo[128]. Principio que en realidad pone en relación el derecho y la técnica, algo esencial en el desarrollo de la privacidad y la protección de datos[129].

IV. Conclusion

En efecto, y ya concluyo, cuando hablamos de la necesidad de contar con un marco jurídico de garantía de la privacidad y de la protección de datos es imprescindible partir de un diálogo constructivo entre el derecho y la técnica. Se ha dicho que las leyes sólo son posibles si van de la mano de la realidad social y tecnológica, no contra ellas[130].

En un apasionante diálogo entre Natalino IRTI y Emmanuele SEVERINO[131] el primero mantiene que la técnica puede ser capaz de condicionar el derecho, pero no es capaz de hacer desaparecer la diferencia entre "la regla y el regulado", es decir, entre derecho y técnica[132]. El Derecho "actúa siempre como principio ordenador respecto a la materia regulada"[133]. SEVERINO, sin embargo va mucho más allá. A partir de su tesis

de la "inevitabilidad del dominio de la técnica", mantiene que "el hombre está destinado a abandonar la ilusión de servirse de la técnica para ser feliz y está destinado a cumplir la voluntad de la técnica, que se aprovecha, para mayor gloria de su propia fuerza, de la vida y de la felicidad humana"[134]. En este escenario, las relaciones entre derecho y técnica se traducen en el hecho de que el primero se convierte en "medio de la técnica". "No será ya la voluntad jurídica la que se sirva de la técnica para elaborar un cierto ordenamiento jurídico, sino que será la técnica la que se sirva del afán de lucro y de la voluntad jurídica para poder incrementar hasta el infinito su fuerza… La técnica está destinada a convertirse en la regla y todo el resto en lo regulado"[135]. ¿Qué podemos hacer los juristas ante tan espectacular como inevitable reto? No hay más alternativa que reivindicar de nuevo el valor de los derechos fundamentales, y muy en particular de la dignidad y libertad del ser humano. En el diálogo, además, hay que dar entrada a un interlocutor más, la ética. Pero sin perder de vista que los avances tecnológicos son imparables y que tienen a su alcance obviar (torear, en términos taurinos y más gráficos aunque menos eruditos) las herramientas de que hoy dispone el derecho para luchar contra la invasión de nuestra privacidad. Pensemos solo, por ejemplo, que la lucha contra el *spam* es prácticamente imposible dado que la gran mayoría de los correos basura que recibimos provienen de países en los que no hay legislación garantizadora de la protección de datos, y eso cuando se acierta a identificar la fuente originaria del *spam*, algo casi siempre imposible[136]. Por ello es imprescindible establecer mecanismo internacionales eficaces contra los ataque a la privacidad; ataques que, como ya he dicho, no saben de fronteras. La era de la información, la era digital, insisto, ha superado hace ya mucho la división territorial de los viejos Estados.

También es imprescindible que todos estemos concienciados sobre los riesgos a que nuestra privacidad está sometida. Concienciados no es agobiados, desde luego, pero tampoco debemos resignarnos a carecer de privacidad o asumirlo como algo inevitable en la sociedad moderna.

Imaginemos que estamos tranquilamente en nuestras casas. Alguien entra y tras decirnos que no nos preocupemos y que sigamos con lo que estamos haciendo, van tomando nota del programa de televisión que estamos viendo, de la página web que estamos visitando y de las que hemos visitado, de la llamada telefónica que estamos haciendo y de las que hemos hecho y recibido en el último año. Por encima de nuestro hombro cotillean el texto del correo electrónico que estamos escribiendo y a quién se lo enviamos. Abren nuestra cartera y toman nota de los números de nuestras tarjetas de crédito, de nuestro DNI. Con parsimonia escrutan todos los movimientos de nuestras cuentas corrientes, las revistas a las que estamos suscritos, las estancias en hoteles que hemos efectuado, los viajes realizados. Van al cajón donde tenemos nuestros papeles de los médicos, nuestras radiografías, análisis de sangre; escanean todo y lo guardan. Salimos de

casa y nos siguen, a nuestro lado, sin dejarnos. Recibimos una llamada en nuestro móvil y colocan un dispositivo para escuchar y grabar la conversación. Decimos a nuestro vigilante que nos deje en paz, que nos deje sólo, y nos contesta que lo siente, que no está en nuestras manos consentir o no su presencia. Que él siempre estará.

No es ciencia ficción. No es una pesadilla. Es una realidad. Virtual, de vigilancia invisible, pero real. Nuestra vida, queramos o no, es o puede ser así.

Marlon BRANDO reclamaba la privacidad no como un mero derecho, sino como una absoluta necesidad[137]. De Greta GARBO son estas palabras: "nunca he dicho que quiero estar sola. Sólo he dicho que quiero poder estar sola. Esta es la diferencia"[138].

Quizá todavía estemos a tiempo de preservar nuestra privacidad. La solución no está ni sólo ni siempre en nuestras manos. Agudicemos el ingenio jurídico para, de la mano de la técnica pero no bajo su dictadura, encontrar soluciones ingeniosas y eficaces que nos permitan seguir siendo libres con dignidad.

Notas

1 El presente trabajo tiene su origen en la Lección Magistral que fui invitado a impartir con motivo de la Apertura Solemne del Curso Académico en la Universidad San Pablo-CEU de Madrid en septiembre de 2008. Lo he revisado y actualizado para esta ocasión.

2 Planeta de Agostini, Barcelona, 2005. Pág. 187.

3 Ver Daniel J. SOLOVE, The Digital Person. Technology and Privacy in the Information Age, New York University Press, 2004, pág. 224. Se ha señalado que la fuente original de tal cita se desconoce dadas las fuertes críticas que por ella recibió McNealy: vid. Colin J. BENNETT y Charles D. RAAB, The Governance of Privacy. Policy Instruments in Global Perspective, The MIT Press, Cambridge-Londres, 2006, págs. 8 y 298.

4 Frase tomada de la Conferencia pronunciada en el marco de la IAPP Privacy Summit, 2007, Washington, 7 de marzo de 2007.

5 Ver José Antonio DIAZ ROJO, "Privacidad, ¿Neologismo o barbarismo?", en Espéculo. Revista de Estudios Literarios, nº 21, 2002. También en http://www.ucm.es/info/especulo/numero21/privaci.html.

6 Ver por ejemplo la STS, Sala 3ª, de 28 de mayo de 2008, donde el término privacidad se utiliza como sinónimo de carácter privado de una actividad en contraposición a su carácter público.

7 Véase la importante obra en cinco volúmenes dirigida por Philippe ARIÈS y George DUBY, Historia de la vida privada, Taurus, Madrid, 1987 a 1989.

8 "Does privacy Law work?", en Philip E. AGREE y Marc ROTENBERG (Eds.), Technology and Privacy: The new Landscape, The MIT Press, 1998, pág. 193.

9 "Perhaps the most striking thing about the right to privacy is that nobody seems to have any clear idea what it is", en "The Right to Privacy", recogido en Ferdinand David SCHOEMAN, Philosophical Dimensions of Privacy: An Anthology, Cambridge University Press, 1984 (reedición de 2007), pág. 272. Citado

también por James Q. WHITMAN, "The two Western Cultures of Privacy: Dignity versus Liberty", en Yale Law Journal, Vol. 113, Abril 2004, pags. 1151 y ss. También puede consultarse en http://papers.ssrn.com/abstract=476041.

10 Sentencia del TEDH de 28 de enero de 2003, asunto Peck contra Reino Unido, epígrafe 57. El Tribunal añade: "The Court has already held that elements such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8. That Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life" (see P.G. and J.H. v. the United Kingdom, no. 44787/98, § 56, ECHR 2001-IX...)".

11 Un buen resumen de las diferentes definiciones de privacidad en la doctina norteamericana puede verse en Markku LAUKKA, Criteria for Privacy Supporing System, http://www.tml.hut.fi/Research/TeSSA/Papers/Laukka/Laukka_nordsec2000.pdf.

12 Irwin ALTMAN, The Environment and Social Behavior. Privacy, Personal Space, Territory, Crowding, Brooks/Cole, Monterey, CA,1975.

13 Darhl M. PEDERSEN, "Psychological Functions of Privacy", en Journal of Environmental Psychology, nº 17, 1997, págs. 147-156.

14 Patricia Brierley NEWELL, "A Cross-Cultural Comparison of Privacy Definitions and Functions: a System Approach", en Journal of Environemntal Psychology, Volumen 18, nº 4, Diciembre 1998, páginas 351-371.

15 Una interesante exposición de algunos intentos de definir la privacidad puede consultarse en Daniel J. SOLOVE, Marc ROTEMBERG y Paul M. SCHWARTZ, Information Privacy Law, Aspen, New York, 2ª ed., 2006, págs. 40 y ss.

16 A Treatise on the Law of Torts or the Wrongs which arise independent of contract, Callaghan 2ª ed., Chicago, 1888, p. 29.

17 Harvard Law Review, Vol IV, 15 de diciembre de 1890, nº 5. El título completo del artículo es "The Right to Privacy (The implicit made explicit)". También se recoge en Ferdinand D. SCHOEMAN, Philosophical dimensions…, op. cit., págs. 75 y ss.. Hay edición bilingüe, italiano e inglés, editada por el Garante per la Protezione dei Dati Personali: Il Diritto alla Privacy. The Right to Privacy, Roma, 2005. Contiene una muy interesante "Introduzione". A tan importante artículo volvía a referirse no hace mucho Stefano RODOTA: Intervista su Privacy e Libertà, a cargo de Paolo CONTI, Editori Laterza, Roma-Bari, 2005, pp. 7 y ss.

18 Véase Stefano RODOTA, La vita e le regole. Tra diritto e non diritto, Feltrinelli, Milán, 2006, pág. 100.

19 Alan F. WESTIN, Privacy and Freedom, Atheneum, New York, 1967. Hay edición de 1970.

20 Como ha recordado Jan HOLVAST, "History of privacy", en Karl DE LEEUW y Jan BERGSTRA (eds.), The History of Information Security. A Comprehensive Handbook, Elsevier, Amsterdam, 2007, págs. 737 y ss.

21 Sobre el concepto, vid., por todos, Pablo LUCAS MURILLO DE LA CUEVA, El derecho a la autodeterminación informativa, Tecnos, Madrid, 1990 y, más recientemente, "La Constitución y el derecho a la autodeterminación informativa", en Cuadernos de Derecho Público, nº 19-20 (2003), monográfico sobre

Protección de Datos, págs. 27 y ss. También Ricard MARTINEZ, Una aproximación crítica a la autodeterminación informativa, Civitas, Madrid, 2004.

22 Lo íntimo, lo privado, lo público, Cuadernos de Transparencia, nº 6, IFAI, México D.F., 5ª ed., octubre 2008. También publicado en la Revista Claves de Razón Práctica, número 137, Madrid, noviembre 2003.

23 Privacy and Freedom, op. cit.

24 Hal ABELSON, Ken LEDDEN y Harry LEWIS, Blown to Bits. Your Life, Liberty and Happines after the Digital Explosion, Addison-Wesley, 2008, pág. 68.

25 Vid. M. LAUKKA, "Criteria for Privacy….", op. cit. Se basa en estudios de FUSILIER y HOYER, en TOLCHINSKY y otros, "Employee perception of invasion of Privacy", Journal of Applied Psychology, nº 66 (1981), págs. 308 y ss.

26 En el momento de escribir estas líneas no he podido comprobar la fecha exacta de la sentencia. Tomo la información del Diario EL PAIS, 3 de septiembre de 2008, pág. 27.

27 En particular, en su relación con la libertad de expresión e información. Sobre la diferencia entre libertad de expresión y libertad de información es sumamente clara la STS de 25 de febrero de 2008, cuyo fundamento jurídico cuarto merece la pena transcribir:

"CUARTO. - El derecho al honor y la libertad de expresión e información.

El art. 20.1 d) CE , en relación con el artículo 53.2 CE, reconoce como derecho fundamental especialmente protegido mediante los recursos de amparo constitucional y judicial el derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión y el art. 18.1 CE reconoce con igual grado de protección el derecho al honor.

Cuando se produce una colisión entre ambos derechos debe prevalecer la protección del derecho a la información siempre que su objeto tenga interés general, es decir, verse sobre asunto de relevancia pública por la materia y por las personas y la información sea veraz (SSTS, entre otras, de 19 de julio de 2006, rec. 2448/2002, y 18 de julio de 2007, rec. 5623/2000, y SSTC 54/2004, de 15 de abril, ciento 58/2003, de 15 de septiembre y 61/2004, de 19 de abril).

La libertad de expresión, igualmente reconocida en el art. 20 CE, tiene un campo de acción más amplio que la libertad de información (SSTC 104/1986, de 17 de julio y 139/2007, de 4 de junio), porque en tanto ésta se refiere a la narración de hechos, la de expresión alude a la emisión de juicios personales y subjetivos, creencias, pensamientos y opiniones. Comprende la crítica de la conducta de otro, aun cuando sea desabrida y pueda molestar, inquietar o disgustar a aquel contra quien se dirige (SSTC 6/2000, de 17 de enero, F. 5; 49/2001, de 26 de febrero, F. 4; y 204/2001, de 15 de octubre, F. 4), pues así lo requieren el pluralismo, la tolerancia y el espíritu de apertura, sin los cuales no existe «sociedad democrática» (SSTEDH de 23 de abril de 1992, Castells c. España, § 42, y de 29 de febrero de 2000, Fuentes Bobo c. España, § 43). Fuera del ámbito de protección de dicho derecho se sitúan las frases y expresiones ultrajantes u ofensivas, sin relación con las ideas u opiniones que se expongan, y por tanto, innecesarias a este propósito, dado que el art. 20.1 a) CE no reconoce un pretendido derecho al insulto, que sería, por lo demás, incompatible con la norma fundamental (SSTC 204/1997, de 25 de noviembre, F. 2; 134/1999, de 15 de julio, F. 3; 6/2000, de 17 de enero, F. 5; 11/2000, de 17 de enero, F. 7; 110/2000, de 5 de mayo, F. 8; 297/2000, de 11 de diciembre, F. 7; 49/2001, de 26 de febrero, F. 5; y 148/2001, de 15 de octubre, F. 4, SSTC 127/2004, de 19 de julio, 198/2004, de 15 de noviembre, y 39/2005, de 28 de febrero).

Con carácter general, los requisitos que debe reunir la información para que la libertad inherente a ella deba ser considerada prevalente respecto al derecho al honor son, en suma, los de interés general, veracidad y exposición no injuriosa o insultante".

28 S.M. JOURARD, "Some Psychological aspects of Privacy", Law and Contemporary Problems, nº 31 (1966), págs. 307 y ss. P. B. NEWELL, "A Systems Model of Privacy", Journal of Environmental Psichology, nº 14 (1994), págs. 65 y ss. A ellos se refiere LAUKKA, "Criteria....", op. cit.

29 "On Privacy (The American Dream: what happened to it?)", edición bilingüe en ingles e italiano, editado por el Garante per la protezione dei dati personali, en el Volumen Privacy, Roma, 2001. Incluye tambíen un interesante Ensayo de Piero BOITANI, "Il Paradiso perduto della Privacy", págs. 58 y ss.

30 LAUKKA, op. ult. cit, en base a las opiniones de PEDERSEN, NEWELL y KELVIN.

31 http://blog.wired.com/27bstroke6/surveillance/index.html

32 Vid sobre todo "La defensa frente al ruido ante el Tribunal Constitucional", en Revista de Administración Pública, nº 115, págs. 214 y ss., y "Medio ambiente sonoro", en ESTEVE PARDO (Coord.), Derecho del medio ambiente y Administración Local, Civitas-Diputación de Barcelona, 1996, págs. 227 y ss. Véanse asimismo Alberto DIAZ-ROMERAL, "La protección del medio ambiente urbano: la contaminación por el ruido en las ciudades y la sostenibilidad en el desarrollo urbano"; Patrica VALCARCEL, "Contaminación acústica y desarrollo sostenible en el marco de la actividad aeroportuaria. Algunas soluciones. En particular: ¿Servidumbres acústicas en la lucah contra el ruido?", ambos trabajos en PIÑAR MAÑAS (Dir.) Desarrollo Sostenible y Protección del Medio Ambiente, Civitas-Universidad San Pablo CEU, Madrid, 2002, págs. 255 y ss., y 207 y ss., respectivamente.

33 "Il corpo e il post-umano", texto original amablemente cedido por el autor, pág. 5.

34 The Republic of Choice. Law, Authority and Culture, Harvard University Press, Cambridge, Mass., 1990, pág. 184.

35 La protection de la vie privée et des autres biens de la personnalité, Bruylant, Bruselas-Paris, 1990, pág. 167.

36 LAUKKA, "Criteria…", op. cit.

37 A la íntima relación entre dignidad y privacidad se ha referido ESCALANTE GONZALBO, El derecho a la privacidad, Cuadernos de Transparencia, nº 2, IFAI, México D.F., 6ª ed., octubre 2008.

38 "The two Western Cultures of Privacy: Dignity versus Liberty", en Yale Law Journal, Vol. 113, Abril 2004, pags. 1151 y ss. También puede consultarse en http://papers.ssrn.com/abstract=476041.

39 "The two Western Cultures of Privacy....", op cit., págs. 10 a 13 del texto disponible en http://papers.ssrn.com/abstract=476041.

40 Entre la doctrina norteamericana ha resaltado la estrecha relación entre privacidad y dignidad Edgard J. BLOUSTEIN: "Privacy as an aspect of human dignity. An Answer to Dean Prosser", *New York University Law Review*, nº 39 (1964), págs. 962 y ss., también recogido en SCHOEMAN, *Philosophical Dimensions*…., op. cit., págs. 156 y ss.

41 Recientemente en *La vita e le regole*…., op. cit., págs. 103 y ss.

42 Me he referido a tales tensiones en relación con la protección de datos, recientemente en "El derecho fundamental a la protección de datos. Contenido esencial y retos actuales. En torno al nuevo Reglamento de Protección de Datos", en PIÑAR MAÑAS y CANALES GIL, *Legislación de Protección de Datos*, Iustel, Madrid, 2008, págs. 91 y ss.

43 RODOTA se ha referido hace poco también a los riesgos que para la privacidad supone el mercado y la lucha por la seguridad: "Innovación, nuevas tecnologías, participación política y protección de datos. Un equilibrio para mejorar la democracia", conferencia impartida en los Cursos de Verano de la Universidad

del País Vasco, en el marco del Seminario *El acceso a la Información Parlamentaria*, impartida el 28 de julio de 2008. Utilizo el texto original que amablemente me ha facilitado el autor.

[44] Recientemente en "Consideraciones introductorias sobre el derecho fundamental a la protección de datos de carácter personal", *Boletín del Ilustre Colegio de Abogados de Madrid*, monográfico sobre *La Protección de Datos (I)*, núm. 36, 3ª época, abril 2007, págs. 13 y ss.

[45] Sobre ello vid. N. IRTI y E. SEVERINO *Dialogo su Diritto e Tecnica*, Editori Laterza, Roma-Bari, 2001; S. RODOTA *Tecnologie e diritti*, Il Mulino, Bari, 1995; *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Editori Laterza, Roma-Bari, 1997. Hay traducción al español: *Tecnopolítica. La democracia y las nuevas tecnologías de la información,* Losada, Buenos Aires, 2000; J.L. PIÑAR MAÑAS, "Revolución tecnológica, Derecho Administrativo y Administración Pública. Notas provisionales para una Reflexión", en T.R. FERNANDEZ y otros, *La Autorización administrativa. La Administración Electrónica. La Enseñanza del Derecho Administrativo*, Aranzadi, 2007.

[46] Los llamados RFID, "identificadores por radiofrecuencia"

[47] El coste económico de los avances tecnológicos y de nuevos dispositivos es cada vez menor, lo que facilita aún más su uso e implantación. Gordon MOORE expuso su visión del futuro de las tecnologías en un breve artículo, de apenas cuatro páginas, publicado en 1965, en términos que más adelante se conocerían (y así se conocen hoy) como la "Ley de Moore". Avanzó entonces que "The complexity for minimum component costs has increased at a rate of roughly a factor of two per year ..... Certainly over the short term this rate can be expected to continue, if not to increase. Over the longer term, the rate of increase is a bit more uncertain, although there is no reason to believe it will not remain nearly constant for at least 10 years": "Cramming more components onto integrated circuits", *Electronics*, Volumen 38, Número 8, 19 de Abril de 1965.

[48] Vid. CASTELLS, Manuel, *La era de la información. Vol. 1, La sociedad red*, Alianza Editorial, Madrid, 3ª ed., 2005, pág. 70.

[49] El incremento de las cámaras de vigilancia en las calles es ya tan alarmante como algo desgraciadamente normal. Plantea problemas de gran importancia sobre la privacidad y la protección de datos. Vid. el *Dictamen de la Comisión de Venecia sobre la videovigilancia en lugares públicos por parte de las autoridades públicas y la protección de los derechos humanos*, en *Revista Española de Protección de Datos*, nº 3 (julio-diciembre 2007), págs. 427 y ss. La Agencia Española de Protección de Datos ha dictado la Instrucción 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o de videocámaras (*BOE* de 12 de diciembre de 2006). La Conferencia Internacional de Autoridades de Protección de Datos celebrada en Londres durante los días 1 a 3 de noviembre de 2006 tuvo por tema precisamente la necesidad de adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos.

[50] Las siguientes reflexiones están tomadas de mi trabajo "Seguridad, Transparencia y Protección de Datos: el futuro de un necesario e incierto equilibrio", 2008.

51 Isaac ASIMOV, Los Límites de la Fundación, pág. 64 de la edición disponible en www.eBooket.com.

52 Así nos lo ha recordado RODOTA, "Il corpo…", op. cit., pág. 10.

53 Sobre ello recientemente vid. S. RODOTA La vita e le regole..... op. cit., págs. 174 y ss. Ellen ALDERMAN y Caroline KENNEDY consideraban ya hace más de diez años que la protección de la información genética era sin duda el tema más importante en el futuro de la protección de datos: The Right to

Privacy, Vintage Books, New York, 1997, pág. 336.

54 Véase Michael KINSLEY, "Inherited Properties. The U.S. Congress voted to ban genetic discrimination. But how much equality do Americans Really want?", en Time, 19 de mayo de 2008, pág. 60.

55 Sobre ello vid. Andrea KRIZSÁN (Ed.), Ethnic Monitoring and Data Protection. The European Context, CPS Books, Budapest, 2001. Es esclarecedor el trabajo en este libro de James A. GOLDSTON, "Race and Ethnic Data: a Missing Resource in the Fight against Discrimination", págs. 19 y ss.

56 http://technology.timesonline.co.uk/tol/news/tech_and_web/article3193223.ece. The Times, 16 de enero de 2008.

57 Ver por ejemplo K.W. BOWYER, "Face recognition technology: security versus privacy", Technology and Society Magazine, IEEE, Primavera de 2004, Volumen 23, páginas 9 y ss. Jay STANLEY y Barry STEINHARDT. "Face-Recognition Technology Threatens Individual Privacy." Opposing Viewpoints: Civil Liberties. Ed. Tamara L. Roleff. San Diego: Greenhaven Press, 2004. Ver http://www.enotes.com/civil-liberties-article/41394. Ver un ejemplo de tal sistema en HOLTZMAN, Privacy lost. How Technology is endangering your Privacy, Jossey-Bass, San Francisco, 2006, pág. 6.

58 Ver Tim KINDBERG y Timothy JONES "Merolyn the Phone":A Study of bluetooth Naming Practices, en http://www.cs.bath.ac.uk/pervasive/publications/ubicomp07.pdf.

59 El término se utilizó por primera vez en torno a 1988 por Mark WEISER. Ver su trabajo The Computer for the 21st Century, http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html. Ver Reijo AARNIO, "Data Protection and New Technologies: "Ubiquitous Computing"", en VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008, págs. 107 y ss. Asimismo Marc LANGHEINRICH, "Privacy by Design-Principles of Privacy-Aware Ubiquitous Systems", 2001, en http://www.vs.inf.ethz.ch/res/papers/privacy-principles.pdf

60 CLIPPINGER, *A Crowd of one. . The Future of Individual Identity*, Public Affaires, New York, 2007, págs. 28 y 32.

61 http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP. Información sobre los fallos de seguridad producidos en Estados Unidos puede también obtenerse en www.attrition.org/security/dataloss.html y en la web de la National Association of Information Destruction -- NAIDDirect, www.naidonline.org

62 El escándalo de la venta ilegal de datos en Alemana ha puesto en marcha una propuesta para reformar la ley de protección de datos para hacerla más exigente y garantista. Con la nueva ley, cuyo primer texto quiere tenerse para el próximo mes de noviembre, se exigiirá el consentimiento expreso de los interesados para la cesión de sus datos con fines comerciales. Hasta ahora, los datos personales de clientes pueden ser cedidos con tales fines si el afectado no se ha opuesto expresamente: http://www.dw-world.de/dw/article/0,2144,3576639,00.html

63 *Vigilar y castigar*, Ed. Siglo XXI, México, 1976. A ello se ha referido también Daniel J. SOLOVE, *The Digital Person. op. cit.*, págs. 30-31.

64 Vid. BENNETT y RAAB, *The Governance….*, op. cit., págs. 16 y ss.

65 Reg WHITAKER, *The End of Privacy: how Total Surveillance is Becoming a Reality*, New Press, New York, 1999. Cit. por BENNETT y RAAB, op. ult. cit, pág. 338. Existe traducción al español de la obra de WHITAKER: *El fin de la privacidad. Como la vigilancia total se está convirtiendo en realidad*, Paidos, 1999.

66 Vid. David. H. HOLTZMAN, *Privacy lost. ….. op. cit.,* págs. 265 y ss.

[67] J. ROSEN, *The Unwanted Gaze. The Destruction of Privacy in America*, Vintage Books, New York, 2000.

[68] Vid. R. SMITH, *War Stories: Accounts of Persons Victimized by Invasions of Privacy*, Privacy Journal, 1993. Cit. por BENNETT y RABB, *Governance of Privacy....*, op. cit., pág. 7.

[69] *Blown to Bits….. op. cit.* Se trata de un muy interesante libro con reveladoras reflexiones acerca del futuro que pueden depararnos las nuevas tecnologías.

[70] Simson GARFINKEL, *Database Nation: the Death of Privacy in 21st Century*, O'Reilly Media, Sebastopol, California, 2001.

[71] *The limits of Privacy*, Basic Books, New York, 1999. A lo largo de toda la obra se exponen los *detrimental effects* de un exceso de privacidad y se proponen soluciones alternativas que pasan, como digo en el texto, por una definición de la privacidad en términos "comunitarios", dando mayor importancia al interés general.

[72] Vid. David. H. HOLTZMAN, *Privacy lost. .....* Op. cit.

[73] *El miedo a la libertad*, utilizo la edición de Paidos, Buenos Aires, 4ª ed., 1978, pág. 308.

[74] Op. Ult. Cit., pág. 302.

[75] "Il corpo...", op. Cit., pág. 9.

[76] *La vita e le regole…*, op. cit., pág. 114. Y advierte RODOTA: "Se libertá e spontaneità si rifugeranno soltanto nei nostri spazi rigorosamente intimi e privati, saremo portati a considerare lontano e ostile tutto quello che stá nel mondo esterno. Qui può essere il germe di nuovi conflitti, e dunque di una permanente e pi`radicale insicurezza".

[77] LANGHEINRICH, "Privacy by Design….", op. cit., pág. 7.

[78] Al que sigue LAUKKA, op. ult. cit.

[79] El concepto de "information privacy" se acerca mucho, en su contenido, al de protección de datos. Véase por todos SOLOVE, ROTEMBERG y SCHWARTZ, *Information Privacy Law*, op. cit. Como señalan los autores, "Information Privacy concerns the collection, use, and disclosure of personal information" (pág. 1). Como señalan BENNETT y RAAB, los concpetos de "information privacy" y "protección de datos" surgieron casi al mismo tiempo en los años sesenta y setenta: *The Governance….*, op. cit., pág. 8.

[80] Así lo ha apuntado Markku LAUKKA "Criteria for privacy…", op. cit.

[81] *A Treatise on the Law of Torts ….."*, *op. cit.* p. 29.

[82] Vol IV, 15 de diciembre de 1890, nº 5, op. cit.

[83] Lo cual es importante, pues el artículo de WARREN y BRANDEIS llama la atención acerca de la necesidad de que el derecho reaccione frente a los ataques a la privacidad no sólo por parte del Gobierno, sino también desde sujetos privados. E. ALDERMAN y C. KENNEDY han llamado la atención acerca de ello, señalando que la Constitución americana sólo protege a los individuos frente a la acción del Gobierno, lo que refuerza el alcance novedoso de la aportación hecha por aquéllos: *The Right to Privacy,* op. cit., pág. 155.

[84] Ver Amitai ETZIONI, *The limits of Privacy*, op. cit, pág. 190.

[85] Ya incluso en 1890, es decir el mismo año en que se publicó el repetido artículo, como recuerda PROSSER en "Privacy (A legal Analysis)", *California Law Review*, nº 48 (1960), págs. 338 y ss., también recogido en Ferdinand D. SCHOEMAN, *Philosophical dimensions….*, op. cit., págs. 104 y ss, y en par-

ticular, pág. 105. Puede consultarse una amplia selección de casos a lo largo de toda la obra de SOLOVE, ROTENBERG y SCWARTZ, *Information Privacy Law,* op. cit., y en ALDERMAN y KENNEDY, *The Right to Privacy*, op. cit., *in toto*.

[86] William PROSSER, que es muy crítico con el artículo de WARREN y BRANDEIS, distingue hasta cuatro diferentes daños derivados del ataque a la privacidad: la intrusión en los asuntos privados del afectado; revelar información privada referente al mismo; la posibilidad de ofrecer al público una falsa imagen del afectado ("false light in the public eye"); y la apropiación de información de aquél: "Privacy (A legal Analysis)", op. cit. Vid. ALDERMAN y KENNEDY, *The Right to Privacy*, op. cit., págs. 155-156; BENNETT y RAAB, *The Governance...*, op. cit., pág. 126. HOLTZMAN analiza "the four torts" propuestos por PROSSER en *Privacy Lost*…., op. cit., págs. 94 y ss., así como SOLOVE en *The Digital Person*…., op. cit., págs. 57 y ss. Edgard J. BLOUSTEIN ha sido, por su parte, crítico con las posiciones de PROSSER: "Privacy as an aspect of human dignity ….", op. cit.

[87] "*Artículo 12.* Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

[88] "*Artículo 11.* Protección de la Honra y de la Dignidad 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

89 Artículo 17. 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la Ley contra esas injerencias o esos ataques.

90 "Artículo 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".

[91] *DOCE* C 364-1, de 18 de diciembre de 2000.

[92] U.S. Department of Health , Education & Welfare, *Records, Computeres and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data System*. Vid. SOLOVE, ROTENBERG y SCHWARTZ, *Information Privacy Law*, op. cit., págs. 35-36 y 577-578.

[93] BENNETT y RAAB, *The Governance*…, op. cit., pág. 121.

[94] En la XXVII Conferencia Internacional de Autoridades de Protección de Datos celebrada en Montreux, Suiza, los días 13 a 15 de septiembre de 2005 se aprobó una Declaración Final sobre « *The protection of personal data and privacy in a globalised world : a universal right respecting diversities* », en la que se hace una referencia expresa a los principios del derecho a al protección de datos:

Recognising that the principles of data protection derive from international legal binding and non binding instruments such as the OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the United Nations Guidelines concerning Computerized Personal

Data Files, the European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data and the Asia Pacific Economic Cooperation Privacy Framework,

17. Recalling that these principles are in particular the following:
- Principle of lawful and fair data collection and processing,
- Principle of accuracy,
- Principle of purpose-specification and -limitation,
- Principle of proportionality,
- Principle of transparency,
- Principle of individual participation and in particular the guarantee of the right of access of the person concerned,
- Principle of non-discrimination,
- Principle of data security,
- Principle of responsibility,
- Principle of independent supervision and legal sanction,
- Principle of adequate level of protection in case of transborder flows of personal data.

95 Directiva 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

96 La bibliografía sobre la Directiva es abundantísima. Vid., recientemente, Christopher KUNNER, *European Data Protection Law: Corporate Compliance and Regulation*, Oxford University Press, 2ª ed., 2007.

97 Vid. PIÑAR MAÑAS "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas", *Cuadernos de Derecho Público*, nº 19-20, Monográfico sobre *Protección de Datos*, págs. 45 y ss. Ha sido traducido al inglés: "ECJ Case Law on the Right to Protection of Personal Data. Part. 1", *BNA International. World Data Protection Report*, Volumen 6, Nº 1, enero 2006. Págs. 3-11; La segunda parte, en la misma Revista, Volumen 6, Nº 2. Febrero, 2006. Págs. 23-32.

98 En la interpretación y desarrollo de la Directiva ha tenido y tiene un protagonismo esencial la labor del llamado Grupo del Artículo 29 de la Directiva, *"Art. 29 Working Party"*, así denominado por haber sido creado por el artículo 29 de la Directiva. Según el nº 1 de este precepto, "Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, …. que tendrá carácter consultivo e independiente". En el repetido artículo 29 y en el 30 se establece su naturaleza, régimen y funciones. Sobre el Grupo del Artrículo 29 vid. Peter SCHAAR, "The Work of the Article 29 Working Party", en VARIOS AUTORES, *Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006*, Fundación BBVA, Madrid, 2008, págs. 107 y ss. También desarrolla un importante cometido en lo que se refiere al tratamiento de datos por parte de las Instituciones europeas, el Supervisor Europeo de Protección de Datos. Sobre esta figura vid. Peter J. HUSTINX, "Data Protection in the European Institutions", en VARIOS AUTORES, *Proccedings of the First European Congress…., op. cit.,* págs. 113 y ss; HIJMANS, Hielke, "The European data protection supervisor: the institutions of the EC controlled by and independent authority", *Common Market Law Review*. Vol. 43 (2006), nº. 5, págs. 1313-1342.

99 De aquél año son las importantes sentencias dictadas en los asuntos Amann contra Suiza, de 16 de febrero de 2000 y Rotaru contra Rumania, de 4 de mayo de 2000.

100 "Artículo 7. Respeto de la vida privada y familiar

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".

[101] "Artículo 8. Protección de datos de carácter personal.

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

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

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

[102] A ello me he referido en "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", en *Asamblea. Revista Parlamentaria de la Asamblea de Madrid*, nº 13, dic. 2005, pág. 21 y ss.

[103] "Privacy and the Future: Some Opening Reflections", en VARIOS AUTORES, *Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006*, Fundación BBVA, Madrid, 2008, pág. 20.

[104] 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.

El artículo 2º es del siguiente tenor: "Artículo 2. Carta de los Derechos Fundamentales de la Unión Europea.

A tenor de lo dispuesto en el párrafo segundo del artículo 10 de la Constitución española y en el apartado 8 del artículo 1 del Tratado de Lisboa, las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán también de conformidad con lo dispuesto en la Carta de los Derechos Fundamentales publicada en el «Diario Oficial de la Unión Europea» de 14 de diciembre de 2007, cuyo texto íntegro se reproduce a continuación: (a continuación el texto íntegro de la Carta).

[105] La primera ratifica la constitucionalidad de la existencia de la Agencia Española de Protección de Datos, con competencias en todo el territorio nacional, en cuanto garante de un Derecho fundamental que debe tener un contenido homogéneo para todas las personas (físicas). La segunda consolida una evolución jurisprudencial constitucional que ha ido configurando el Derecho a la protección de datos, desde el reconocimiento del Derecho a la intimidad y privacidad, pasando por el llamado Derecho a la autodeterminación informática o informativa. Merece la pena recordar también las Sentencias constitucionales 110/84, 254/93, 143/94, 94/98, 11/98, 144/99 y 202/99 que resuelven básicamente recursos de Amparo, frente a tratamientos ilícitos, contrarios al principio de "autodeterminación informativa", que se traduce en el Derecho de control sobre los datos relativos a la propia persona o, lo que es lo mismo, el Derecho a controlar el uso de los mismos datos personales por parte de su titular. Así las sentencias 144/99 y 202/1999, dictadas frente a la utilización por RENFE de los datos de diversos trabajadores relativos a su afiliación sindical. Resoluciones anteriores relacionan el Derecho a la protección de datos de carácter personal con el Derecho a la intimidad (SSTC 143/1994, 254/1993 y 110/1984), proclamando con carácter general *"El reconocimiento global de un Derecho a la intimidad o a la vida privada que abarque su defensa frente las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida"*. En particular, la STC 254/1993 señala que la Constitución de 1978 ha incorporado el "Derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos". Añade que no es posible aceptar que "el Derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados.... son absolutamente necesarias para que los intereses protegidos por el artículo 18 de la Constitución, y que dan vida al Derecho fundamental a la intimidad, resulten real y

efectivamente protegidos". Para un análisis de la jurisprudencia del Tribunal Constitucional en la materia, vid. E. GUICHOT, *Datos personales y Administración Pública*, Thomson-Civitas, 2005, págs. 68 y ss.

[106] La doctrina del Tribunal Constitucional ha sido asumida totalmente por los Tribunales. Véase la magnífica obra coordinada por Carlos LESMES SERRANO, *La ley de Protección de Datos. Análisis y comentario de su jurisprudencia*, Lex Nova, Valladolid, 2008. Como ejemplo de tal asunción, he aquí un párrafo de la reciente Sentencia del Tribunal Supremo de 26 de junio de 2008, en el que además se distingue una vez más entre intimidad y protección de datos: "En nuestra Sentencia de 13 de Septiembre de 2.002 (Rec.92/1999) nos fijamos en que el *art. 18* de la Constitución garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen en su párrafo 1º y en su apartado 4º consagra lo que: "la jurisprudencia constitucional ha denominado el "derecho fundamental a la protección de datos personales", derecho fundamental estrechamente conectado con el reconocido en el apartado 1º del mismo precepto, aunque con un contenido propio y diferenciado, que –en palabras de la STC 292/2000, de 30 de noviembre - "impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información", habiéndose de tener en cuenta que, como dice esta misma sentencia constitucional, "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, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el *art. 18.1 CE* otorga, sino los datos de carácter personal. 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"; de forma que, en conclusión, "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, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso".

[107] Las siguientes consideraciones ya las he expuesto en "El derecho fundamental a la protección de dastos. Contenido esencial….", op. cit., págs. 26 y ss.

[108] Fundamentos Jurídicos segundos de ambas Sentencias.

[109] Sobre la importancia del artículo 18.4 en relación con el derecho a la protección de datos, vid recientemente el "Prólogo" de Tomás DE LA QUADRA SALCEDO, al libro coordinado por Juan ZABIA DE LA MATA, *Protección de datos. Comentarios al Reglamento*, Lex Nova, Valladolid, 2008, págs. 7 y ss.

[110] Ley Orgánica 3/1985, de 29 de mayo, Ley Orgánica 5/1992, de 29 de octubre, y Ley Orgánica 10/1995, de 23 de noviembre.

[111] Sobre el Reglamento vid Juan ZABIA DE LA MATA (Coord.), *Protección de Datos. Comentarios al Reglamento*, op. cit. PIÑAR MAÑAS y CANALES GIL, *Legislación de Protección de Datos*, op. cit. PIÑAR MAÑAS, "El porqué de un reglamento de desarrollo de la Ley Orgánica de Protección de Datos", en *Revista Española de Protección de Datos*, nº 3 (julio-diciembre 2007), págs. 9 y ss.; PIÑAR MAÑAS, "Strengthen-

ing Legal Certainty: New Regulations Developing the LOPD (Organic Data Protection Act)", en VARIOS AUTORES, *Proccedings of the First European Congress….,* págs. 33 y ss.; Antonio TRONCOSO, "Regulatory Development of the LOPD", en VARIOS AUTORES, *Proccedings….., op. cit,* págs. 51 y ss.; Belén VELEIRO, "Regulatory Development of the LOPD from a Business Perspective", en VARIOS AUTORES, *Proccedings ….op. cit.*, págs. 81 y ss. Juan Manuel FERNANDEZ LOPEZ, "Algunas reflexiones sobre los aspectos generales que regula el reglamento de desarrollo de la LOPD", en *Revista Española de Protección de Datos*, nº 3 (julio-diciembre 2007), págs. 35 y ss.

[112] Gran parte de ellas pueden consultarse en el *Código de Protección de Datos*, edición preparada por la Agencia Española de Protección de Datos, Ed. La Ley, Madrid, 2005. Deben tenerse especialmente en cuenta la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales; la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos; la Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos; la Ley Orgánica 10/2007, de 8 de octubre, reguladora de bases de datos policiales sobre identificadores obtenidos a partir del ADN; la Ley 30/2007, de contratos del sector público; la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, o la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

[113] *The Governance of Privacy….*, op. cit., pág. 19.

[114] "The good news is that there is legal protection for privacy. The bad news is that it doesn't work particularly well": *Privacy Lost…*, op. cit., pág. 119.

[115] James RULE y otros, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*, Elsevier, New York, 1980, págs. 68 y ss.

[116] Cit. por BENNETT y RAAB, *The Governance….*, op. cit., pág. 147.

[117] "Does Privacy Law work?", op. cit., págs. 193 y ss.

[118] A esta Sentencia se ha referido también recientemente RODOTA, "Innovación, nuevas tecnologías, ….", op. cit.

[119] Epígrafe 181 de la Sentencia.

[120] Epígrafe 203.

[121] Sobre los instrumentos de autorregulación, vid., entre otros, BENNETT y RAAB, *The Governance….*, op. cit., págs. 151 y ss.

[122] Vid los comentarios de María José BLANCO ANTON a los artículos citados en Juan ZABIA DE LA MATA (Coord.), *Protección de Datos. Comentarios al Reglamento*, op. cit., págs. 635 y ss.

[123] A ello me he referido con cierta extensión en "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", op. cit.

[124] A ello me he referido ya en "El derecho fundamental a la protección de datos. Contenido esencial…", op. cit., pág. 91.

[125] Sobre la "evaluation of impact" vid. BENNETT y RAAB, *Governance of Privacy….*", op. cit., págs. 235 y ss. A la evaluación del impacto se ha referido también RODOTA, en "Innovación, nuevas tecnologías, ….", op. cit.

[126] WHITE, "The use of Privacy Impacts Assessments in Canada", *Privacy Files*, nº 4, 2001, pág. 2.

127 Vid. Marc LANGHEINRICH, Privacy by Design -Principles of Privacy- Aware Ubiquitous Systems, op. cit. El Supervisor Europeo de Protección de Datos ha resaltado la necesidad de reforzar ese principio en su Documento de 28 de abril de 2008 "The EDPS and EU Research and Technological Development", que puede consultarse en la dirección http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf.

128 Marit HANSEN, Ari SCHWARTZAND y Alissa COOPER, "Privacy and Identity Management", *IEEE Security & Privacy*, Marzo-abril, 2008, pág. 39.

129 Sobre la necesidad de que los soportes y sistemas de información tengan en cuenta las medidas de seguridad necesarias para garantizar la protección de datos, véanse los artículos 5.2 y 79 y ss. del Reglamento de Desarrollo de la LOPD, aprobado por Real Decreto 1720/2007. Asimismo, la Disposición Adicional única del Reglamento, en virtud de la cual "los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto que permitan alcanzar de acuerdo con lo establecido en el título VIII de este Reglamento".

130 M. LANGHEINRICH, *Privacy by Design….*, op. cit., pág. 16. Y afirma: "Si ciertas previsiones legales no pueden imponerse , es necesario encontrar soluciones tecnológicas o procedimentales alternativas, o la ley deberá cambiarse"

131 IRTI, Natalino, y SEVERINO, Emanuele, *Dialogo su Diritto e Tecnica*, Editori Laterza, Roma-Bari, 2001

132 Op. cit., pág. 14.

133 "Si pone sempre come principio ordinatore rispetto alla materia regolata". Op. cit., pág. 15.

134 "L'uomo è destinato ad abbandonare l'illusione di servirsi della técnica per essere felice, ed è destinato a fare la volontà della técnica, che si serve, per la gloria della propria potenza, della vita e della felicità umane". Op. cit., pág. 39.

135 "Non sará più la volontà giuridica a servirsi della técnica per realizzare un certo ordinamento giuridico, ma sará la técnica a servirsi della volontà di profitto e della volontà giuridica per incrementare all'infinito la propria potenza... La técnica è destinata a diventare al regola e tutto il resto il regolato". Id. Pág. 80.

136 Para luchar contra el spam y otras amenazas internacionales para la privacidad se constituyó en Londres, el 11 de octubre de 2004 el llamado London Action Plan, integrado por representantes de más de 27 países. Vid. http://www.londonactionplan.org/

137 "Privacy is not something that I'm merely entitled to; it's an absolute prerequisite". Cit. Por David H. HOLTZMAN, Privacy lost: How Technology….., pág. 3.

138 "I never said, "I want to be alone". I only said "I want to be left alone". There is all the difference". Cit. Por David H. HOLTZMAN, *Privacy lost....*, pág. 211. La cita original está tomada de la película Gran Hotel. También citada por RODOTA, *La vita e le regole….*, op. cit., pág. 99.

Bibliografia utilizada y citada

AARNIO, "Data Protection and New Technologies: "Ubiquitous Computing"", en VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008, págs. 107 y ss.

ABELSON, LEDDEN y LEWIS, Blown to Bits. Your Life, Liberty and Happines after the Digital Explosion, Addison-Wesley, 2008.

Agencia Española de Protección de Datos, Código de Protección de Datos, Ed. La Ley, Madrid, 2005.

ALDERMAN y KENNEDY, The Right to Privacy, Vintage Books, New York, 1997.

ALTMAN, The Environment and Social Behavior. Privacy, Personal Space, Territory, Crowding, Brooks/Cole, Monterrey, CA,1975.

ARIÈS y DUBY, Historia de la vida privada, Taurus, Madrid, 1987 a 1989.

ASIMOV, Los Límites de la Fundación, edición disponible en www.eBooket.com.

BENNETT y RAAB, The Governance of Privacy. Policy Instruments in Global Perspective, The MIT Press, Cambridge-Londres, 2006.

BLANCO ANTON, Comentarios a los artículos 71 a 78 en ZABIA DE LA MATA (Coord.), Protección de Datos. Comentarios al Reglamento, Lex Nova, Valladolid, 2008., págs. 635 y ss.

BLOUSTEIN: "Privacy as an aspect of human dignity. An Answer to Dean Prosser", New York University Law Review, nº 39 (1964), págs. 962 y ss. También recogido en SCHOEMAN, Philosophical Dimensions…., págs. 156 y ss.

BOITANI, "Il Paradiso perduto della Privacy", en Garante per la protezione dei dati personali, Privacy, Roma, 2001págs. 58 y ss.

BOWYER, "Face Recognition Technology: Security Versus Privacy", Technology and Society Magazine, IEEE, Primavera de 2004, Volumen 23, páginas 9 y ss.

CASTELLS, La era de la información. Vol. 1, La sociedad red, Alianza Editorial, Madrid, 3ª ed., 2005.

CLIPPINGER, A Crowd of one. The Future of Individual Identity, Public Affaires, New York, 2007

COOLEY, A Treatise on the Law of Torts or the Wrongs which arise independent of contract, Callaghan 2ª ed., Chicago, 1888.

DE LA QUADRA SALCEDO, "Prólogo" al libro coordinado ZABIA DE LA MATA, Protección de datos. Comentarios al Reglamento, Lex Nova, págs. 7 y ss.

DE LEEUW y BERGSTRA (eds.), *The History of Information Security. A Comprehensive Handbook*, Elsevier, Amsterdam, 2007

DIAZ ROJO, "Privacidad, ¿Neologismo o barbarismo?", en Espéculo. Revista de Estudios Literarios, nº 21, 2002. También en http://www.ucm.es/info/especulo/numero21/privaci.html.

DIAZ-ROMERAL, "La protección del medio ambiente urbano: la contaminación por el ruido en las ciudades y la sostenibilidad en el desarrollo urbano"; PIÑAR MAÑAS (Dir.) Desarrollo Sostenible y Protección del Medio Ambiente, Civitas-Universidad San Pablo CEU, Madrid, 2002, págs. 255 y ss.

ESCALANTE GONZALBO, El derecho a la privacidad, Cuadernos de Transparencia, nº 2, IFAI, México D.F., 6ª ed., octubre 2008.

ETZIONI, The limits of Privacy, Basic Books, New York, 1999.

FAULKNER, "On Privacy (The American Dream: what happened to it?)", edición bilingüe en ingles e italiano, editado por el Garante per la protezione dei dati personali, en el Volumen Privacy, Roma, 2001.

FERNANDEZ LOPEZ, "Algunas reflexiones sobre los aspectos generales que regula el reglamento de desarrollo de la LOPD", en Revista Española de Protección de Datos, nº 3 (julio-diciembre 2007), págs. 35 y ss.

Lecturas

FOUCAULT, Vigilar y castigar, Ed. Siglo XXI, México, 1976.

FRIEDMAN, The Republic of Choice. Law, Authority and Culture, Harvard University Press, Cambridge, Mass., 1990.

FROMM, El miedo a la libertad, he utilizado la edición de Paidos, Buenos Aires, 4ª ed., 1978

Garante per la Protezione dei Dati Personali: Privacy, Roma, 2001.

Il Diritto alla Privacy. The Right to Privacy, Roma, 2005.

GARFINKEL, Database Nation: the Death of Privacy in 21st Century, O'Reilly Media, Sebastopol, California, 2001.

GARZON VALDES, Lo íntimo, lo privado, lo público, Cuadernos de Transparencia, nº 6, IFAI, México D.F., 5ª ed., octubre 2008. También publicado en la Revista Claves de Razón Práctica, número 137, Madrid, noviembre 2003.

GELLMAN, "Does privacy Law work?", en Philip E. AGREE y Marc ROTENBERG (Eds.), Technology and Privacy: The new Landscape, The MIT Press, 1998, pág. 193.

GOLDSTON, "Race and Ethnic Data: a Missing Resource in the Fight against Discrimination", en Andrea KRIZSÁN (Ed.), Ethnic Monitoring and Data Protection. The European Context, CPS Books, Budapest, 2001págs. 19 y ss.

GUICHOT, Datos personales y Administración Pública, Thomson-Civitas, 2005.

HANSEN, SCHWARTZAND y COOPER, "Privacy and Identity Management", IEEE Security & Privacy, Marzo-abril, 2008, págs. 38 y ss.

HIJMANS, "The European data protection supervisor: the institutions of the EC controlled by and independent authority", Common market law review. Vol. 43 (2006), nº. 5, págs. 1313-1342.

HOLTZMAN, Privacy lost. How Technology is endangering your Privacy, Jossey-Bass, San Francisco, 2006.

HOLVAST, "History of privacy", en Karl DE LEEUW y Jan BERGSTRA (eds.), The History of Information Security. A Comprehensive Handbook, Elsevier, Amsterdam, 2007

HUSTINX, "Data Protection in the European Institutions", VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008, págs. 113 y ss

IRTI y SEVERINO Dialogo su Diritto e Tecnica, Editori Laterza, Roma-Bari, 2001.

JOURARD, "Some Psychological aspects of Privacy", Law and Contemporary Problems, nº 31 (1966), págs. 307 y ss.

KINDBERG y JONES "Merolyn the Phone":A Study of bluetooth Naming Practices, en http://www.cs.bath.ac.uk/pervasive/publications/ubicomp07.pdf

KINSLEY, "Inherited Properties. The U.S. Congress voted to ban genetic discrimination. But how much equality do Americans Really want?", en Time, 19 de mayo de 2008, pág. 60.

KRIZSÁN (Ed.), Ethnic Monitoring and Data Protection. The European Context, CPS Books, Budapest, 2001.

KUNNER, European Data Protection Law: Corporate Compliance and Regulation, Oxford University Press, 2ª ed., 2007.

LANGHEINRICH, "Privacy by Design-Principles of Privacy-Aware Ubiquitous Systems", 2001, en http://www.vs.inf.ethz.ch/res/papers/privacy-principles.pdf

LAUKKA, Criteria for Privacy Supporing System, http://www.tml.hut.fi/Research/TeSSA/Papers/Laukka/Laukka_nordsec2000.pdf

LUCAS MURILLO DE LA CUEVA:

El derecho a la autodeterminación informativa, Tecnos, Madrid, 1990

"La construcción del derecho a la autodeterminación informativa", *Revista de Estudios Políticos*, nº 104, 1999.

"La Constitución y el derecho a la autodeterminación informativa", en *Cuadernos de Derecho Público*, nº 19-20 (2003), monográfico sobre *Protección de Datos*, págs. 27 y ss.

MARTIN-RETORTILLO:

"La defensa frente al ruido ante el Tribunal Constitucional", en *Revista de Administración Pública*, nº 115, págs. 214 y ss.,

"Medio ambiente sonoro", en ESTEVE PARDO (Coord.), *Derecho del medio ambiente y Administración Local*, Civitas-Diputación de Barcelona, 1996, págs. 227 y ss

MARTINEZ, *Una aproximación crítica a la autodeterminación informativa*, Civitas, Madrid, 2004.

McNEALY, Conferencia pronunciada en el marco de la *IAPP Privacy Summit, 2007*, Washington, 7 de marzo de 2007.

MOORE "Cramming more components onto integrated circuits", *Electronics*, Volumen 38, Número 8, 19 de Abril de 1965.

NEWELL:

- "A Cross-Cultural Comparison of Privacy Definitions and Functions: a System Approach", en *Journal of Environemntal Psychology*, Volumen 18, nº 4, Diciembre 1998, páginas 351-371.

- "A Systems Model of Privacy", *Journal of Environmental Psichology*, nº 14 (1994), págs. 65 y ss.

PEDERSEN, "Psychological Functions of Privacy", en *Journal of Environmental Psychology*, nº 17, 1997, págs. 147-156.

PIÑAR MAÑAS:

(Dir.) *Desarrollo Sostenible y Protección del Medio Ambiente*, Civitas-Universidad San Pablo CEU, Madrid, 2001

"El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas", *Cuadernos de Derecho Público*, nº 19-20, Monográfico sobre *Protección de Datos*, págs. 45 y ss. Ha sido traducido al inglés: "ECJ Case Law on the Right to Protection of Personal Data. Part. 1", *BNA International. World Data Protection Report*, Volumen 6, Nº 1, enero 2006. Págs. 3-11; La segunda parte, en la misma Revista, Volumen 6, Nº 2. Febrero, 2006. Págs. 23-32.

"El porqué de un reglamento de desarrollo de la Ley Orgánica de Protección de Datos", en *Revista Española de Protección de Datos*, nº 3 (julio-diciembre 2007)

"Consideraciones introductorias sobre el derecho fundamental a la protección de datos de carácter personal", *Boletín del Ilustre Colegio de Abogados de Madrid*, monográfico sobre *La Protección de Datos (I)*, núm. 36, 3ª época, abril 2007, págs. 13 y ss.

"Revolución tecnológica, Derecho Administrativo y Administración Pública. Notas provisionales para una Reflexión", en T.R. FERNANDEZ y otros, *La Autorización administrativa. La Administración Electrónica. La Enseñanza del Derecho Administrativo*, Aranzadi, 2007.

"El derecho fundamental a la protección de datos. Contenido esencial y retos actuales. En torno al nuevo Reglamento de Protección de Datos", en PIÑA MAÑAS y CANALES GIL, *Legislación de Protección de Datos*, Iustel, Madrid, 2008.

"Seguridad, Transparencia y Protección de Datos: el futuro de un necesario e incierto equilibrio", 2008.

"Strengthening Legal Certainty: New Regulations Developing the LOPD (Organic Data Protection Act)", en VARIOS AUTORES, *Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006*, Fundación BBVA, Madrid, 2008, págs. 33 y ss

PIÑAR MAÑAS y CANALES GIL, *Legislación de Protección de Datos*, Iustel, 2008

PROSSER, "Privacy (A legal Analysis)", *California Law Review*, nº 48 (1960), págs. 338 y ss., también recogido en SCHOEMAN, *Philosophical dimensions….*, op. cit., págs. 104 y ss

RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Bruylant, Bruselas-Paris, 1990.

RODOTA:

Tecnologie e diritti, Il Mulino, Bari, 1995;

Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione, Editori Laterza, Roma-Bari, 1997. Hay traducción al español: *Tecnopolítica. La democracia y las nuevas tecnologías de la información,* Losada, Buenos Aires, 2000

Intervista su Privacy e Libertà, a cargo de Paolo CONTI, Editori Laterza, Roma-Bari, 2005.

La vita e le regole. Tra diritto e non diritto, Feltrinelli, Milán, 2006.

"Il corpo e il post-umano", texto original amablemente cedido por el autor, 2008.

"Privacy and the Future: Some Opening Reflections", en VARIOS AUTORES, *Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006*, Fundación BBVA, Madrid, 2008, págs. 19 y ss.

"Innovación, nuevas tecnologías, participación política y protección de datos. Un equilibrio para mejorar la democracia", conferencia impartida en los Cursos de Verano de la Universidad del País Vasco, en el marco del Seminario *El acceso a la Información Parlamentaria*, impartida el 28 de julio de 2008. He utilizado el texto original que amablemente me ha facilitado el autor

ROSEN, The Unwanted Gaze. The Destruction of Privacy in America, Vintage Books, New York, 2000.

RULE y otros, The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies, Elsevier, New York, 1980.

SCHAAR, "The Work of the Article 29 Working Party", en VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008, págs. 107 y ss.

SCHOEMAN, Philosophical Dimensions of Privacy: An Anthology, Cambridge University Press, 1984 (reedición de 2007),

SMITH, War Stories: Accounts of Persons Victimized by Invasions of Privacy, Privacy Journal, 1993.

SOLOVE, The Digital Person. Technology and Privacy in the Information Age, New York University Press, 2004

SOLOVE, ROTEMBERG y SCHWARTZ, *Information Privacy Law*, Aspen, New York, 2ª ed., 2006.

STANLEY y STEINHARDT. "Face-Recognition Technology Threatens Individual Privacy." Opposing Viewpoints: Civil Liberties. Ed. Tamara L. Roleff. San Diego: Greenhaven Press, 2004

THOMSON, "The Right to Privacy", recogido en Ferdinand David SCHOEMAN, Philosophical Dimensions of Privacy: An Anthology, Cambridge University Press, 1984 (reedición de 2007), pág. 272.

TOLCHINSKY y otros, "Employee perception of invasion of Privacy", Journal of Applied Psychology, nº

66 (1981), págs. 308 y ss.

TRONCOSO, "Regulatory Development of the LOPD", en VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008, págs. 51 y ss

U.S. Department of Health , Education & Welfare, Records, Computeres and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data System, Washington, 1973.

VALCARCEL, "Contaminación acústica y desarrollo sostenible en el marco de la actividad aeroportuaria. Algunas soluciones. En particular: ¿Servidumbres acústicas en la lucah contra el ruido?", en PIÑAR MAÑAS (Dir.) Desarrollo Sostenible y Protección del Medio Ambiente, Civitas-Universidad San Pablo CEU, Madrid, 2002, págs. 207 y ss.

VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008.

VELEIRO, Regulatory Development of the LOPD from a Business Perspective, en VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008, págs. 81 y ss.

WARREN y BRANDEIS, "The Right to Privacy (The implicit made explicit)". Harvard Law Review, Vol IV, 15 de diciembre de 1890, nº 5.

WEISER The Computer for the 21st Century, http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html

WESTIN, Privacy and Freedom, Atheneum, New York, 1967.

WHITAKER, The End of Privacy: how Total Surveillance is Becoming a Reality, New Press, New York, 1999. Existe traducción al español de la obra de WHITAKER: El fin de la privacidad. Como la vigilancia total se está convirtiendo en realidad, Paidos, 1999.

WHITE, "The use of Privacy Impacts Assessments in Canada", Privacy Files, nº 4, 2001, págs. 2 y ss.

WHITMAN, "The two Western Cultures of Privacy: Dignity versus Liberty", en Yale Law Journal, Vol. 113, Abril 2004, pags. 1151 y ss. También puede consultarse en http://papers.ssrn.com/abstract=476041.

ZABIA DE LA MATA (Coord.), Protección de datos. Comentarios al Reglamento, Lex Nova, Valladolid, 2008.