DERECHOS FUNDAMENTALES E INTERNET: NUEVOS PROBLEMAS, NUEVOS RETOS

RAMÓN M. ORZA LINARES [*]

SUMARIO:

1. INTRODUCCIÓN

Aunque el debate sobre la necesidad de incorporar al orden jurídico nuevos derechos fundamentales no es nuevo en la teoría jurídica, es cierto que en la actualidad estamos asistiendo a unos cambios tecnológicos tan acelerados que muchas de las categorías jurídicas que se han utilizado hasta ahora están dejando de ser útiles o muestran graves carencias a la hora de resolver los problemas generados por las nuevas tecnologías de la comunicación y de la información.

Ello nos obliga a los juristas a que redoblemos los esfuerzos para que la utilización de estos nuevos instrumentos tecnológicos no supongan nuevas amenazas a la libertad y la igualdad de las personas. De hecho, es evidente que la intensidad con la que internet está modificando numerosos hábitos sociales puede llevar a la obligación de modular y de cambiar muchas

[*] Profesor Contratado Doctor. Universidad de Granada.

ReDCE. Año 9. Núm. 18. Julio-diciembre/2012. Págs. 275-336.

de las categorías jurídicas que se han ido construyendo como protección de las derechos fundamentales de las personas.

En efecto, aunque la aparición de internet es relativamente reciente [1], los cambios que ha introducido en nuestras sociedades son de tal envergadura que todavía son difíciles de prever las consecuencias de todo orden que pueden implicar.

Así, aunque la protección de datos personales ha avanzado de modo significativo desde los años ochenta del pasado siglo, lo cierto es que los derechos consolidados alrededor de esa protección —derechos de acceso, rectificación, cancelación y oposición— no pueden ser simplemente trasladados a las nuevas realidades de la «sociedad del conocimiento». Y ello a pesar del esfuerzo que las distintas agencias reguladoras, entre ellas la Agencia Española de Protección de Datos, están realizando en orden a intentar resolver los nuevos problemas que plantea internet con los instrumentos, ya más consolidados, que se han venido utilizando para la protección de datos.

Recientemente, sin embargo, esta vía de solución ha llegado a cierto bloqueo, como lo demuestran los recursos presentados por «Google» contra los acuerdos de la Agencia Española de Protección de Datos y la cuestión prejudicial presentada por la Audiencia Nacional ante el Tribunal de Justicia de la Unión Europea [2].

Desde el ámbito jurídico constitucional resulta obligado, por lo tanto, que no ocupemos de esta «nueva frontera» de los derechos fundamentales, dónde se están construyendo las bases de la sociedad futura y en los que están presentes nuevos retos como la superación de las fronteras físicas entre los Estados, las diversas concepciones de la libertad de expresión y el de-

[1] La definición del protocolo TCP/IP y de la palabra «internet» hay que situarla alrededor de 1982, todavía hay que esperar a 1991 para que aparezca la World Wide Web y a 1993 para que aparezca el primer navegador web el «NCSA Mosaic» (Cfr. *http://es.wikipedia.org/wiki/Mosaic* [Consulta: 6 de diciembre de 2012]. Información adicional sobre este navegador se puede obtener en *ftp://ftp.ncsa.uiuc.edu/Web/Mosaic/* [Consulta 6 de diciembre de 2012]).

[2] El texto del Auto en formato pdf, se puede obtener en *http://goo.gl/ASVo0* [Consulta 25 de octubre de 2012].

recho a la información, las dificultades procesales para la persecución de las infracciones administrativas y los delitos cometidos a través de la red o, en fin, la dificultad de perseguir los sitios de internet situados extraterritorialmente

En relación con el limitado objetivo de este artículo, pretendemos exponer sólo algunos de los nuevos problemas que ahora aparecen en relación con internet y la «sociedad del conocimiento» y algunas de las soluciones que, siquiera provisionalmente, se están adoptando internacionalmente. En este artículo nos vamos a referir, por lo tanto, al derecho al acceso, al derecho al anonimato y al derecho al olvido. Pero con ellos no se recogen todos los posibles problemas que puede plantear internet: dejamos de lado todo lo referente a la protección de datos personales, a la protección de copyright, a la censura o, entre otras, a la neutralidad de la red [3].

2. **EL DERECHO DE ACCESO**

Podríamos señalar que éste es el primero de los derechos vinculados a las nuevas tecnologías, ya que si no hay posibilidad de acceso a internet, poco más podemos decir. De hecho, así lo entendió la Comisión Especial sobre Redes Informáticas, creada por el Senado Español, ya en 1998, cuándo en sus conclusiones lo mencionaba dentro de su primera propuesta: «Todas las personas tienen el derecho fundamental de acceder libremente a la Red, sin discriminación de sexo, condición, características físico-psíquicas,

[3] Unas primeras aproximaciones al estudio de estos nuevos retos puede encontrarse EN R. M. ORZA LINARES, «¿Es posible la creación de nuevos derechos fundamentales asociados a las nuevas tecnologías de la información y de la comunicación?». Comunicación presentada al *IV Congreso de la Cibersociedad* 2009. En línea. Se puede consultar en *http://www.cibersociedad.net/congres2009/es/coms/es-posible-la-creacion-de-nuevos-derechos-fundamentales-asociados-a-las-nuevas-tecnologias-de-la-informacion-y-de-la-comunicacion/991/* [Consulta: 10 de noviembre de 2012]. *Vid.* también, del mismo autor, «Las nuevas tecnologías de la información y comunicación y nuevos derechos fundamentales». En VV.AA. *Realidades y tendencias del Derecho en el siglo XXI* . Tomo VI. Ed. Universidad Javierana y Ed. Themis, Bogotá, 2010, pp. 251-285.

edad o lugar de residencia» [4]. De hecho, para esta Comisión del Senado, «es una responsabilidad de los legisladores y del Gobierno Central y de los de las Comunidades Autónomas garantizar la igualdad de oportunidades a los ciudadanos y a los territorios del Estado». De tal modo que «la cesión de la configuración de redes únicamente al operador y al mercado inspirados en razones de carácter mercantil impide que se cumpla el principio de universalidad y de servicio público», ya que «todos los individuos y grupos sociales tienen derecho a disponer de instrumentos para su desarrollo y es aplicable el principio de subsidiaridad, cuando no pueden acceder a tales instrumentos por motivos ajenos a su voluntad de desarrollo humano como la distancia, la diferencia de renta, discapacidades físicas, densidad de población, predominio del sector agrícola, o los modos de vida rural, entre otros». Por ello, «no es posible dejar a los agentes del mercado las decisiones sobre el tendido y extensión de las redes cuya planificación y ordenamiento deben corresponder a la Administraciones Públicas» [5].

Las características técnicas de la Red exigen que, para poder acceder a la misma, se den unas condiciones técnicas previas. Es necesario tener un ordenador, u otro dispositivo que pueda conectarse (teléfono, tableta y, en los últimos años, televisiones, fotocopiadoras, impresoras, etc.), y una infraestructura de red que permita el acceso de los ciudadanos a la misma.

Las preocupaciones en este ámbito, van, pues, en esa doble dirección. Por un lado, de cara a los ordenadores u otros dispositivos y, por otro, en el desarrollo de los puntos de acceso y la red que los interconectan.

Por lo que se refiere a la primera cuestión, es de destacar la aparición de algunas iniciativas privadas para la construcción de ordenadores portátiles con pocas exigencias técnicas, que incluyan la conexión a internet y

[4] *Boletín Oficial de las Cortes Generales. Senado*. Serie I. Núm. 812, 27 de diciembre de 1999, pp. 1 y ss. En especial las pp. 46-48. Este Boletín, como el resto de las publicaciones oficiales del Senado español, puede consultarse en la página web del Senado. Concretamente, el citado en esta nota puede consultarse, en formato pdf, en: *http://www.senado.es/legis6/publicaciones/pdf/senado/bocg/I0812.PDF* [Consulta: 5 de diciembre de 2012].

[5] Ibídem, p. 46.

que tengan un coste reducido [6]. Y en relación con el desarrollo de la red de conexión tanto diversas entidades internacionales como algunos Gobiernos han impulsado distintas iniciativas al respecto. En este apartado, deberíamos destacar también los enormes desequilibrios que existen en la actualidad a la hora de poder acceder a la Red. De hecho, según datos del «Internet World Stats», referidos a junio de 2012, sólo un 34,3% de la población mundial tendría acceso a internet, destacando por encima de la media, Norteamérica, con un 78,6%, Australia/Oceanía con el 67,6% o Europa con un 63,2%. Mientras que bastante por debajo de la media se encontrarían África, con sólo el 15,6% de penetración o Asia con el 27,5%. En Oriente Medio la penetración sería de un 40,2% y en América Central y del Sur y en el Caribe el porcentaje se situaría en el 42,2% [7].

No obstante también existen algunas opiniones en contra de considerar el acceso a internet como un derecho humano. Así, Vinton G. Cerf, cocreador del protocolo TCP/IP y que es considerado como uno de los creadores de internet, en un artículo publicado en el *New York Times*, el pasado día 4 de enero de 2012 señalaba que «la tecnología es un facilitador de derechos, no un derecho en sí mismo» y habría que restringir la consideración de derecho humano a consideraciones como la libertad de expresión o la libertar de acceso a la información, pero éstos no deben estar ligados a ninguna tecnología en particular en un momento determinado [8].

[6] Destaca, por su importancia, la iniciativa que impulsó Nicholas Negroponte —director del «MIT Media Lab»— para que se construyan ordenadores de bajo coste que permitieran disminuir la «brecha digital» en los países más pobres. Este proyecto se presentó en el año 2005 en el Foro económico mundial de Davos. La iniciativa se engloba bajo la sigla en inglés OLPC (Un Ordenador Por Niño) y su página web es la siguiente: *http://olpc.com/* [Consulta: 4 de diciembre de 2012].

[7] También existen muchas diferencias dentro de cada una de las regiones entre unos países y otros. Cfr. *http://www.internetworldstats.com/stats.htm* [Consulta: 4 de diciembre de 2012].

[8] VINTON G. CERF: «Internet Access Is Not a Human Right». New York Times, 4 de enero de 2012. En línea: *http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?_r=2&* [Consulta: 4 de diciembre de 2012]. En el mismo sentido, A. THIERER expone que cualquiera que apoye el acceso a internet como

2.1. **Iniciativas internacionales**

En todo caso, la APC «Association for Progressive Communications», que desde 1995 es organismo consultivo de la ONU, y que agrupa a más de cincuenta redes de miembros y socios en todo mundo, en el año 2006 elaboró una carta sobre Derechos en Internet cuyo primer apartado se refiere al «impacto del acceso sobre el desarrollo y la justicia social» indicando que «Un acceso asequible, rápido y fácil a internet puede ayudar a generar sociedades más igualitarias». Asimismo, «puede servir para fortalecer los servicios de educación y salud, el desarrollo económico local, la participación pública, el acceso a la información, la buena gobernanza y la erradicación de la pobreza». En su apartado segundo «el derecho a acceder a la infraestructura sin importar dónde se viva» hace mención a que «Internet funciona como una estructura pública global» y que dicha infraestructura «debe estar ampliamente distribuida y ser soporte del ancho de banda suficiente para permitir a las personas de todas partes del mundo utilizar ese potencial para hacerse oír, mejorar su vida y expresar su creatividad». Así «la gente tiene derecho a contar con una columna vertebral de la red (conocida como "back-bone") bien distribuida y conectada a la red internacional». Junto a ello también es obligación de los gobiernos «locales y nacionales» y las organizaciones internacionales y comunitarias y las entidades del sector privado «apoyar y promover oportunidades gratuitas o de bajo costo en las áreas de capacitación, metodologías y materiales relativos al uso de internet para el desarrollo social» [9]. Más concretamente, la APC procla-

---

un derecho debería preguntarse quién paga los costes de ese derecho y cuáles serían las posibles desventajas para la competencia y la innovación, en «Vint Cerf on Why Internet Access Is Not a Human Right (+ A Few More Reasons)». En línea, *http://techliberation.com/2012/01/05/vint-cerf-on-why-internet-access-is-not-a-human-right-a-few-more-reasons/* [Consulta: 4 de noviembre de 2012]. Para un análisis de este debate, Cfr. JACINTO LAJAS, «El acceso a internet como derecho fundamental». En línea, *http://www.periodismociudadano.com/2012/01/21/el-acceso-a-internet-como-derecho-fundamental/* [Consulta: 4 de diciembre de 2012].

[9] «Carta de la APC sobre derechos en internet». En línea, *http://www.apc.org/en/node/5677/* [Consulta: 4 de diciembre de 2012].

ma «derecho a interfaces, contenido y aplicaciones accesibles para todos (incluido el diseño)», de tal modo que interfaces, contenidos y aplicaciones deben diseñarse para garantizar el acceso de todos, incluso las personas con discapacidades físicas, sensoriales o cognitivas, las personas analfabetas y las que hablan lenguas minoritarias» [10]. También «el derecho igualitario para hombres y mujeres» [11], el «derecho a un acceso asequible» [12], el derecho «al acceso en el lugar de trabajo» [13], el «derecho al acceso público» [14] y el «derecho a acceder y crear contenidos cultural y lingüísticamente diversos» [15]. En definitiva, la APC también vincula Internet a la educación y al derecho a participar libremente en la vida cultural de la comunidad.

[10] Ibídem. Apartado 1.4.

[11] «En varios lugares, las mujeres y los hombres no tienen acceso igualitario a informarse, acceder, usar y adaptar internet a sus necesidades. Los esfuerzos en pos de incrementar el acceso deben reconocer y eliminar las desigualdades de género existentes. Debe haber plena participación de la mujer en todas las áreas relativas al desarrollo de internet para garantizar la igualdad de género». Ibídem, Apartado 1.5.

[12] «Los responsables de la formulación de políticas y regulaciones deben garantizar que cada persona tenga un acceso asequible a internet. El desarrollo de la infraestructura de telecomunicaciones y el establecimiento de normas, precios, impuestos y aranceles debería hacer posible el acceso a personas de cualquier nivel de ingresos» Ibídem. Apartado 1.6.

[13] «Para muchas personas el lugar de trabajo es el principal o único punto de acceso a internet. Los trabajadores y empleados deben poder acceder a la red en los lugares de trabajo, incluso con fines educativos y para la protección de los derechos laborales». Ibídem, Apartado 1.7.

[14] «Muchas personas no gozarán nunca de acceso privado a computadoras o a internet. Debe haber puntos de acceso público disponibles, como telecentros, bibliotecas, centros comunitarios, clínicas y escuelas, para que todas las personas pueden tener acceso a una distancia razonable de su lugar de residencia o trabajo. Esto es especialmente importante para la gente joven de los países donde el acceso a internet aún no está suficientemente extendido o no es asequible». Ibídem, Apartado 1.8.

[15] «En los sitios web, las herramientas en línea y el software predominan las lenguas latinas. Ello afecta el desarrollo de contenidos locales en lenguas no latinas e impide el intercambio de contenidos entre las culturas. El desarrollo técnico debe alentar la diversidad lingüística en internet y simplificar el intercambio de información entre las lenguas». Ibídem, Apartado 1.9.

En esta misma línea, el día 1 de junio de 2011, el Relator especial de las Naciones Unidas para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa, la Relatora especial de la Organización de Estados Americanos para la Libertad de Expresión y la Relatora especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos adoptaron conjuntamente una Declaración sobre «Libertad de Expresión e Internet» en la que señalaban, entre otros extremos, que «los Estados tienen la obligación de promover el acceso universal a Internet para garantizar el disfrute efectivo del derecho a la libertad de expresión. El acceso a Internet también es necesario para asegurar el respeto de otros derechos, como el derecho a la educación, la atención de la salud y el trabajo, el derecho de reunión y asociación, y el derecho a elecciones libres» [16]. Asimismo, indican que «la interrupción del acceso a Internet, o a parte de este, aplicada a poblaciones enteras o a determinados segmentos del público (cancelación de Internet) no puede estar justificada en ningún caso, ni siquiera por razones de orden público o seguridad nacional. Lo mismo se aplica a las medidas de reducción de la velocidad de navegación de Internet o de partes de este». Y que «la negación del derecho de acceso a Internet, a modo de sanción, constituye una medida extrema que solo podría estar justificada cuando no existan otras medidas menos restrictivas y siempre que haya sido ordenada por la justicia, teniendo en cuenta su impacto para el ejercicio de los derechos humanos». Además, «otras medidas que limitan el acceso a Internet, como la imposición de obligaciones de registro u otros requisitos a proveedores de servicios, no son legítimas a menos que superen la prueba establecida por el derecho internacional para las restricciones a la libertad de expresión» [17].

Por todo ello, «los Estado tienen la obligación positiva de facilitar el acceso universal a Internet», y, como mínimo, deberían: «establecer meca-

[16] «Declaración conjunta sobre libertad de expresión e internet», 1 de junio de 2011. p. 4. En línea. Documento pdf: *http://www.osce.org/es/fom/78325* [Consulta: 4 de diciembre de 2012].

[17] Ibídem.

nismos regulatorios —que contemplen regímenes de precios, requisitos de servicio universal y acuerdos de licencia— para fomentar un acceso más amplio a Internet, incluso de los sectores más pobres y las zonas rurales más alejadas». También «Brindar apoyo directo para facilitar el acceso, incluida la creación de centros comunitarios de tecnologías de la información y la comunicación (TIC) y otros puntos de acceso público», y «Generar conciencia sobre el uso adecuado de Internet y los beneficios que puede reportar, especialmente entre sectores pobres, niños y ancianos, y en las poblaciones rurales aisladas». Finalmente, deberían «Adoptar medidas especiales que aseguren el acceso equitativo a internet para personas con discapacidad y los sectores menos favorecidos» [18].

Por su parte el Comité de Derechos Humanos de la ONU, reunido en Ginebra en julio de 2011 adoptó una *Observación General* en la que mencionaba que «Los Estados partes deberían tener en cuenta la medida en que la evolución de las tecnologías de la información y la comunicación, como Internet y los sistemas de difusión electrónica de la información en tecnología móvil, han cambiado sustancialmente las prácticas de la comunicación en todo el mundo». Y que «ahora existe una red mundial en la que intercambiar ideas y opiniones, que no se basa necesariamente en la intermediación de los medios de comunicación de masas». Por lo que «los Estados partes deberían tomar todas las medidas necesarias para fomentar la independencia de esos nuevos medios y asegurar el acceso a los mismos de los particulares» [19].

Y, en fin, el 10 de agosto de 2011 el Secretario General de la ONU trasmitió a la Asamblea General el informe del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión en el que se señala que «aunque el acceso a internet aún no es un derecho humano como tal… los Estados tienen la obligación positiva de promover

[18] Ibídem.

[19] Comité de Derechos Humanos de la ONU: *Observación General núm. 34*. 11 a 29 de julio de 2011. párrafo 15. Sig. CCPR/C/GC/34. En línea, *http://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/453/34/doc/G1145334.DOC?OpenElement* [Consulta: 4 de diciembre de 2012].

o facilitar el disfrute del derecho a la libertad de expresión y los medios necesarios para ejercer este derecho, lo que incluye a Internet». Además, «El acceso a internet no sólo es esencial para gozar del derecho a la libertad de expresión, sino también otros derechos como el derecho a la educación, el derecho al a libertad de asociación y de reunión, el derecho a la plena participación en la vida social cultural y político y el derecho al desarrollo social y económico» [20]. En el debate que se produjo a propósito de este informe en la Tercera Comisión de la Asamblea General, celebrado el 21 de octubre de 2011, el Relator Especial el Sr. La Rue Lewy destacó que «el uso de internet continúa a la zaga en los países en desarrollo», por lo que es necesario que «los Estados desempeñen una función dinámica haciendo que Internet sea más asequible y facilitando el acceso», además, «alienta también a los Estados a prestar apoyo a la formación de aptitudes en tecnología de la información y de las comunicaciones», lo que, en su opinión, podría hacerse «integrando la alfabetización en internet en los programas de estudios escolares». No obstante, la Sra. Alsaleh de la República Árabe Siria manifestó que a su delegación le gustaría saber «de qué modo puede conciliarse [la responsabilidad del Estado de proporcionar acceso a internet a sus habitantes] con el hecho de que un gran número de países desarrollados rechaza esa posición creando obstáculos al acceso de los países en desarrollo a la tecnología de la información y las comunicaciones», así como «los efectos de las sanciones económicas que imponen unilateralmente los países desarrollados y que afectan al acceso libre e irrestricto de los países en desarrollo a la tecnología…» [21].

[20] Asamblea General de las Naciones Unidas: *Promoción y protección del derecho a la libertad de opinión y de expresión*. Sexagésimo sexto periodo de sesiones. Tema 69 b) del programa provisional. Sig. A/66/290. En linea, *http://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/449/81/doc/N1144981.DOC?OpenElement* p. 18 [Consulta: 4 de diciembre de 2012].

[21] Asamblea General de las Naciones Unidas, Tercera Comisión: «Acta resumida de la 28.ª sesión». Nueva York, 21 de octubre de 2011. Págs. 3 y 6. En línea, documento pdf: *http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/558/15/PDF/N1155815.pdf?OpenElement* [Consulta: 4 de diciembre de 2012].

2.2. **Iniciativas gubernamentales en Europa**

En Europa, en los últimos años, hemos podido asistir a una creciente garantía del derecho de acceso a internet. De hecho, en el periodo que va desde el 31 de diciembre de 2000 hasta el 30 de junio del 2012 se ha producido un incremento del al población con acceso a internet de un 393,4% [22].

Así, en Suiza, el Consejo Federal determinó, tras una consulta pública en relación a la modificación de la «Ordonnance sur les services de télécommunication (OST)» en 2006[23] que, a partir de 1 de enero de 2008, toda la población podría tener acceso de banda ancha. Se estableció un servicio universal con una velocidad de trasmisión mínima de 600 kbits por segundo de descarga y 100 kbit por segundo de subida. La conexión debía incluir también un canal de voz, un número de teléfono y una entrada en el directorio telefónico público [24].

En Francia, en la *Decisión* del Consejo Constitucional Francés sobre la Ley por la que se favorece la Difusión y la Protección de la Creación en Internet [25], se considera como un derecho básico el derecho de acceso a

[22] Según Internet World Stats, en Europa los usuarios de internet pasaron de 105.096.093 personas a 518.512.109 personas, en el periodo reseñado. Tales datos pueden consultarse en *http://www.internetworldstats.com/stats.htm* [Consulta: 4 de diciembre de 2012].

[23] Se puede consultar el Informe final, en formato pdf, en *http://www.bakom.admin.ch/dokumentation/gesetzgebung/00909/01543/index.html?lang=fr&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ae2IZn4Z2qZpnO2Yuq2Z6gpJCDdYR9gGym162epYbg2c_JjKbNoKSn6A*— [Consulta 4 de diciembre de 2012].

[24] Cfr. la página web de la Oficina Federal de Comunicaciones en el Departamento de Medio Ambiente, Transporte, Energía y Comunicaciones *http://www.bakom.admin.ch/dokumentation/medieninformationen/00471/index.html?lang=en&msg-id=7308*. Concretamente, el art. 16 párr. 3 de la Ley de Telecomunicaciones faculta al Consejo Federal para adaptar el servicio universal al estado de la técnica y las exigencias sociales y económicas, En línea, *http://www.admin.ch/ch/f/rs/784_10/a16.html* [Consulta: 4 de diciembre de 2012].

[25] CONSEIL CONSTITUTIONNEL, *Décision núm. 2009-580 DC du 10 juin 2009*, «Loi favorisant la diffusion et la protection de la création sur internet». Se puede lo-

internet, bien que deduciéndolo directamente del art. 11 de la Declaración de los Derechos del Hombre y del Ciudadano de 1789 [26], entendiendo que «en el estado actual de los medios de comunicación y con respecto al desarrollo generalizado de los servicios de comunicación pública en línea» este acceso es importante para «la participación en la vida democrática y la expresión de ideas y opiniones» [27].

En Finlandia, el 1 de julio de 2010 entró en vigor una ley por la que se obligaba a todas las compañías de telecomunicaciones a proporcionar una conexión mínima de 1 Mb a todos los usuarios [28], pero curiosamente quedan fuera de esta garantía las segundas residencias (Casas de veraneo «kesäasuntoja»). Además, para 2015 el gobierno prevé que todos los finlandeses dispondrán de una conexión de 100 Mb. Estonia también ha legislado de modo similar.

En el Reino Unido, el Gobierno preveía para 2012 garantizar una conexión de, al menos, 2 Mb para todos los hogares, pero no consideraba establecerlo como derecho. Tal compromiso lo adquirió en un Informe deno-

---

calizar en la siguiente dirección electrónica: *http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html* [Consulta: 4 de diciembre de 2012], passim. La documentación completa de su tramitación legislativa puede obtenerse en la siguiente dirección: *http://www.senat.fr/dossierleg/pjl07-405.html* [Consulta: 4 de diciembre de 2012].

[26] «La libre comunicación de pensamientos y opiniones es uno de los derechos más valiosos del hombre: cualquier ciudadano podrá, por consiguiente, hablar, escribir, imprimir libremente, siempre y cuando responda del abuso de esta libertad en los casos determinados por la ley».

[27] Parágrafo 12 de la *Décision núm. 2009-580 DC del 10 de junio de 2009*, ya citada.

[28] El establecimiento y definición del servicio universal está contemplado en el Capítulo 6 de la Ley. El texto de la misma puede consultarse en *http://www.finlex.fi/fi/laki/ajantasa/2003/20030393?search%5Btype%5D=pika&search%5Bpika%5D=Internet-yhteys* [Consulta: 4 de diciembre de 2012]. Las velocidades de conexión las supervisa la Autoridad Reguladora de las Comunicaciones («Viestintävirasto»). Su página web es la siguiente: *http://www.ficora.fi/* [Consulta: 4 de diciembre de 2012].

minado «Digital Britain Final Report» [29] elaborado en junio de 2009 y presentado al Parlamento. Fruto de ese informe fue la «Digital Economy Act» de 2010 [30], que entró en vigor el 8 de junio de 2010, aunque no contempla ninguna regulación sobre derecho de acceso a internet o garantías de acceso mínimo [31].

Pero el problema no se plantea sólo en la posibilidad de acceso a internet, sino que el acceso a la Red se haga en condiciones de calidad y de rapidez. De hecho, en un informe elaborado por la Comisión Europea, se señalaba que «los beneficios de la banda ancha son tales que la imposibilidad de acceder a ella constituye un problema que debe abordarse con urgencia» [32]. De tal modo que «la falta de acceso a las conexiones de banda ancha constituye un aspecto del problema más general que suele denominarse «brecha digital», a saber, la distancia que separa a personas, empresas y territorios en cuanto a oportunidades de acceder a las TIC y utilizarlas» [33]. Para ello, y teniendo en cuenta los derechos involucrados, la Comisión proponía la intervención pública en el desarrollo de la banda ancha, sobre todo para garantizar la conexión prioritaria de «centros escolares, administraciones públicas y centros sanitarios» [34].

[29] DEPARTAMENT FOR CULTURE, MEDIA AND SPORT AND DEPARTAMENT FOR BUSINESS, INNOVATION AND SKILLS: *Digital Britain Final Report*. En línea: *http://www.official-documents.gov.uk/document/cm76/7650/7650.pdf* [Consulta: 4 de diciembre de 2012].

[30] Se puede consultar en *http://www.legislation.gov.uk/ukpga/2010/24/contents* En especial, su p. 82. [Consulta: 4 de diciembre de 2012].

[31] De hecho, su objetivo principal es la protección de los derechos de autor y combatir las infracciones de copyright y otras regulaciones sobre la televisión y la radio.

[32] COMISIÓN EUROPEA, *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones. Superar los desequilibrios de la banda ancha*. Bruselas, 20 de marzo de 2006. Pág. 3. Localizable en el servidor jurídico de la Unión: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0129:FIN:ES:HTML* [Consulta: 4 de diciembre de 2012].

[33] Ibidem.

[34] Ibidem, pp. 8 y 11.

En otro informe posterior, y partiendo de la base de que «Los Estados miembros deben garantizar, … que todos los usuarios finales tengan acceso desde ubicaciones fijas a servicios de transmisión de voz y datos, incluido el «acceso funcional a Internet», causando la menor distorsión posible en el mercado», la Comisión considera que, por ahora, no es necesario «modificar el concepto y los principios básicos del servicio universal en cuanto instrumento para evitar la exclusión social», de tal modo que deben ser los propios Estados, de acuerdo con el principio de subsidiaridad, los que determinen «la velocidad adecuada de trasmisión de datos en las conexiones de red que ofrezcan "un acceso funcional a internet"», aunque para evitar distorsiones, la Comisión «iniciará conversaciones con los Estados miembros, el Parlamento europeo y otras partes interesadas» sobre estas materias. Asimismo, «la Comisión presentará propuestas en el primer trimestre de 2012 para garantizar que los usuarios con discapacidad puedan acceder sin restricciones antes de 2015 a los sitios web del sector público y a los que ofrecen servicios básicos a los ciudadanos» [35].

Por último debemos también reseñar que el Parlamento Europeo adoptó el 5 de julio de 2011 una Resolución en la que afirmaba que «Destaca la importancia de las obligaciones de servicio universal (OSU) como red de seguridad para la integración social cuando las fuerzas del mercado no han sabido proporcionar por sí solas servicios básicos a los ciudadanos y a las empresas» y «Respalda los objetivos de «Acceso de banda ancha para todos» de la Agenda Digital y tiene el convencimiento de que el acceso a la banda ancha ayuda a los ciudadanos y a las empresas a sacar el máximo provecho del mercado único digital, en especial al mejorar la integración social, crear nuevas oportunidades para las empresas innovadoras desde los

[35] COMISIÓN EUROPEA, *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones. El servicio universal en el ámbito de las comunicaciones electrónicas: informe sobre el resultado de la consulta pública y de la tercera revisión periódica del alcance de ese servicio conforme al art. 15 de la Directiva 2002/22/CE*. Bruselas, 23 de noviembre de 2011. En línea, se puede obtener, en formato pdf, en la siguiente dirección: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0795:FIN:ES:PDF* [Consulta: 4 de diciembre de 2012].

puntos de vista ambiental y social, impulsando el empleo y el crecimiento y aumentando las oportunidades de comercio transfronterizo; aboga, a tal fin, por el fomento de la formación digital» por lo que pide a la Comisión que «ofrezca mayor apoyo financiero a los proyectos locales que proporcionan acceso digital y a todas las comunidades que ayudan a grupos con discapacidad a acceder a instrumentos tecnológicos, proporcionando conexiones en edificios públicos con acceso a Internet gratuito», por cuanto «una combinación de políticas y tecnologías (redes alámbricas, por cable, fibra, móvil y satélite) puede fomentar el desarrollo de nuevos servicios y aplicaciones en línea por parte de las empresas y los organismos públicos, como la e-educación, la e-sanidad y la e-administración, impulsando la demanda de conexiones de Internet más rápidas, haciendo más rentables las inversiones en redes abiertas de banda ancha, alentando así las asociaciones entre los sectores público y privado y desarrollando el mercado único digital, al tiempo que se mejora la inclusión de los ciudadanos marginados» [36].

2.3. **Regulación en España**

En España no han existido hasta el momento pronunciamientos sobre el carácter de derecho fundamental del acceso a internet. No obstante, sí podemos encontrar alguna regulación al respecto en relación a la posibilidad de que todos puedan conectarse a internet con independencia de su lugar de residencia, desde hace relativamente pocos años.

Así, la primera mención a la conexión de internet como derecho se encuentra en la inicial redacción del Real Decreto 425/2005 [37] que indicaba

[36] PARLAMENTO EUROPEO: *Resolución de 5 de julio de 2011, sobre el servicio universal y el número de urgencia 112*. Disponible en *http://www.europarl. europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0306+0+DOC +XML+V0//ES* [Consulta: 4 de diciembre de 2012].

[37] Real Decreto 425/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (Boletín Oficial del Estado, núm.

las condiciones por las que se establecía la conexión a internet como servicio universal. El que fuera considerado servicio universal implicaba, de acuerdo con el art. 27, «el conjunto definido de servicios cuya prestación se garantiza para todos los usuarios finales con independencia de su localización geográfica, con una calidad determinada y a un precio asequible» [38]. Y, dentro del conjunto definido de servicios, el art. 28 d) recoge: «Establecer comunicaciones de datos a velocidad suficiente para acceder de forma funcional a Internet, con arreglo a las recomendaciones pertinentes de la serie V de la UIT-T, sin perjuicio de que se puedan utilizar otros interfaces, previa autorización del Ministerio de Industria, Turismo y Comercio, en casos concretos y debidamente justificados. A estos efectos, se considerará velocidad suficiente la utilizada de manera generalizada para acceder a Internet por los abonados al servicio telefónico fijo disponible al público con conexión a la red mediante pares de cobre y módem para banda vocal». En definitiva, lo único que se garantizaba era la conexión a internet a baja velocidad.

Un par de años más tarde, la Ley 57/2007, de Medidas de Impulso de la Sociedad de la Información, en su Disposición Adicional Segunda señalaba que: «El Gobierno, en colaboración con las Comunidades Autónomas, impulsará la extensión de la banda ancha con el fin de conseguir, antes del 31 de diciembre de 2008, una cobertura de servicio universal de conexión a banda ancha, para todos los ciudadanos, independientemente del tipo de tecnología utilizada en cada caso y de su ubicación geográfica» [39]. No obs-

---

102, 29 de abril de 2005). El texto de este Real Decreto y del resto de las leyes recogidas en este artículo se pueden consultar en la página web del *Boletín Oficial del Estado*: *http://www.boe.es/*

[38] Esta definición viene recogida del art. 22 de la Ley 32/2003, General de Telecomunicaciones, que indica que «Se entiende por servicio universal el conjunto definido de servicios cuya prestación se garantiza para todos los usuarios finales con independencia de su localización geográfica, con una calidad determinada y a un precio asequible» (*Boletín Oficial del Estado* núm. 264, de 4 de noviembre de 2003).

[39] Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información (*Boletín Oficial del Estado* núm. 312, 29 de diciembre de 2007).

tante esta Ley no caracterizaba el acceso a internet como un derecho de manera distinta a como lo hacía el Decreto anterior, ni introducía nuevas especificaciones.

Finalmente, en la Ley 2/2011, de Economía Sostenible [40], se introdujo, en su art. 52, como elemento integrante del servicio universal de telecomunicaciones la conexión a banda ancha a una velocidad de 1 Mb, a través de cualquier tecnología. En el mismo artículo se habilitaba al Gobierno para que, en el plazo de cuatro meses, mediante Real Decreto estableciera las condiciones de acceso a banda ancha dentro de este servicio universal. Ese Real Decreto se publicó, finalmente, el 24 de mayo de 2011 [41].

En su texto se modifica el art. 27 del anterior Real Decreto 424/2005, ya citado, en el sentido de establecer que el servicio universal es «el conjunto definido de servicios cuya prestación se garantiza para todos los usuarios finales con independencia de su localización geográfica, con una calidad determinada y a un precio razonable». De tal modo que, en base al mismo, «todos los usuarios finales puedan obtener una conexión a la red pública de comunicaciones electrónicas desde una ubicación fija». Y, en el nuevo art. 28.1 b) se establece que, por lo que se refiere a internet, este servicio debe garantizar «comunicaciones de datos en banda ancha a una velocidad en sentido descendente de 1Mbit por segundo».

En todo caso, en el informe realizado por la Comisión del Mercado de las Telecomunicaciones en junio de 2010, se señalaba que en España la banda ancha en sus tramos de velocidad más alta, no sólo tenía una escasa penetración, sino que resultaba significativamente más cara que en el resto de los países de la Unión Europea.

Así, en junio de 2010 el tramo de líneas a velocidad alta (igual o superior a 10 Mb), sólo alcanzaba al 31,5% de las líneas y su coste era supe-

[40] El texto oficial de la ley se puede consultar en *http://www.boe.es/buscar/act.php?id= BOE-A-2011-4117* [Consulta: 4 de diciembre de 2012].

[41] Real Decreto 726/2011, de 20 de mayo, por el que se modifica el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril. Se puede consultar en formato pdf en *http://www.boe.es/boe/dias/2011/05/24/pdfs/BOE-A-2011-9012.pdf* [Consulta: 4 de diciembre de 2011].

rior, en el mejor de los casos, en un 18,1% a la media de la Unión Europea. Además, el 60% de las líneas se situaban en el tramo de velocidad media (entre 2 Mb y 10 M, no incluido), con un coste superior, también de la mejor oferta, en un 11,5% a la media de la UE. Y, por último, todavía subsistía un 8,5% a baja velocidad (desde 144 KB hasta 2 Mb, no incluido) cuyo costo, éste sí, se encontraba por debajo de la media de la UE en un 4,8% [42]. Y, en todo caso, el número de viviendas con acceso a internet en España, con datos de 2012, sólo llegaba al 67,9% del total de hogares [43].

Finalmente, es posible encontrar en las últimas redacciones de algunos Estatutos de Autonomía un reconocimiento al derecho de acceso a internet por parte de los ciudadanos.

Concretamente, el art. 34 de Estatuto de Autonomía de Andalucía señala que «Se reconoce el derecho a acceder y usar las nuevas tecnologías y a participar activamente en la sociedad del conocimiento, la información y la comunicación, mediante los medios y recursos que la ley establezca» [44]. También el art. 53.1 del Estatuto de Autonomía de Cataluña recoge que «Los poderes públicos deben facilitar el conocimiento de la sociedad de la información y deben impulsar el acceso a la comunicación y a las tecnologías de la información, en condiciones de igualdad, en todos los ámbitos de la vida social, incluido el laboral; deben fomentar que estas tecnologías se pongan al servicio de las personas y no afecten negativamente a sus derechos, y deben garantizar la prestación de servicios mediante dichas tec-

[42] COMISIÓN DEL MERCADO DE LAS TELECOMUNICACIONES: *Comparativa internacional de ofertas comerciales de banda ancha en la Unión Europea y España a junio de 2010*. p. 7 En línea, documento pdf: *http://www.cmt.es/c/document_library/get_file?uuid=0c8aa925-a102-410f-b13f-e546c7f680f2&groupId=10138* [Consulta: 4 de diciembre de 2012].

[43] INSTITUTO NACIONAL DE ESTADÍSTICA: *Encuesta sobre equipamiento y uso de tecnologías de la información y comunicación en los hogares en 2012*. En línea, *http://www.ine.es/jaxi/tabla.do?path=/t25/p450/a2012/l0/&file=01001.px&type=pcaxis&L=0* [Consulta: 4 de diciembre de 2012].

[44] Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía. Los textos oficiales, de ésta y de las siguientes leyes citadas, como se ha indicado, se pueden obtener en *http://www.boe.es/*

nologías, de acuerdo con los principios de universalidad, continuidad y actualización» [45] o, entre otros, el art. 7.6 del Estatuto de Autonomía de Extremadura que indica que los poderes públicos «Estimularán la investigación científica y técnica, la incorporación de procesos innovadores por los actores económicos, el acceso a las nuevas tecnologías por parte de empresas y ciudadanos y los mecanismos legales y técnicos que faciliten el libre acceso de todos al conocimiento y la cultura» [46] y el art. 19.2 del Estatuto de Autonomía de la Comunidad Valenciana indica que «Queda garantizado el derecho de acceso de los valencianos a las nuevas tecnologías y a que la Generalitat desarrolle políticas activas que impulsen la formación, las infraestructuras y su utilización» [47]. No obstante, las iniciativas de las Comunidades Autónomas en este sentido han sido escasas, aunque se han hecho importantes esfuerzos en relación con la dotación de equipamientos de uso público para numerosos pueblos [48].

[45] Ley Orgánica 6/2006, de 19 de julio, de reforma del Estatuto de Autonomía de Cataluña.

[46] Ley Orgánica 1/2011, de 28 de enero, de reforma del Estatuto de Autonomía de la Comunidad Autónoma de Extremadura.

[47] Ley Orgánica 1/2006, de 10 de abril, de Reforma de Ley Orgánica 5/1982, de 1 de julio, de Estatuto de Autonomía de la Comunidad Valenciana. También la Ley Orgánica 5/2007, de 20 de abril, de reforma del Estatuto de Autonomía de Aragón, en su art. 28.2 señala que [los poderes públicos de Aragón] «Del mismo modo, promoverán las condiciones para garantizar en el territorio de Aragón el acceso sin discriminaciones a los servicios audiovisuales y a las tecnologías de la información y la comunicación». También el art. 16.21 de la Ley Orgánica 14/2007, de 30 de noviembre, de reforma del Estatuto de Autonomía de Castilla y León indica que «La plena incorporación de Castilla y León a la sociedad del conocimiento, velando por el desarrollo equilibrado de las infraestructuras tecnológicas en todo su territorio y garantizando la igualdad de oportunidades de todas las personas en el acceso a la formación y al uso de las tecnologías de la información y la comunicación». En la misma línea, el art, 29 de la Ley Orgánica 1/2007, de 28 de febrero, de reforma del Estatuto de las Illes Balears establece que «En el ámbito de sus competencias, los poderes públicos de las Illes Balears impulsarán el acceso a las nuevas tecnologías, a la plena integración en la sociedad de la información y a la incorporación de los procesos de innovación».

[48] Por ejemplo, las Aulas Guadalinfo en Andalucía, utilizando software Linux. Cfr. *http://www.guadalinfo.es* [Consulta: 17 de diciembre de 2012].

3. EL DERECHO AL ANONIMATO

Pero una vez que hemos accedido a internet, otros problemas se plantean. Por ejemplo, la salvaguardia de un cierto anonimato en la navegación por internet puede suponer una importante protección de la libertad de la persona. La participación política, la configuración de la opinión pública e, incluso, las compras o las transacciones económicas a través de la red, pueden exigir, en ocasiones, una importante salvaguarda de la identidad propia.

3.1. Regulación legal del control de los datos

Así, en la *Declaración de Derechos del Ciberespacio* que Robert B. Gelman redactó el 12 de noviembre de 1997, en su art. 3 se establecía que «Toda persona tiene derecho a la privacidad, anonimicidad y seguridad en las transacciones en línea» [49]. Quizá fuera ésta una de las primeras ocasiones en las que se remarcaba este aspecto en relación con internet [50].

Entre nosotros, el Tribunal Constitucional Español, en la Sentencia 144/1999 [51], señalaba que «el art. 18.1 garantiza… un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, ve-

[49] Puede consultarse el texto de la Declaración y un breve análisis de la misma, realizada por L.G. Peñarrieta Bedoya, «Derecho al acceso a las tecnologías de comunicación e información», disponible en *http://www.monografias.com/trabajos37/derechos-ciberespacio/derechos-ciberespacio2.shtml* [Consulta: 25 de octubre de 2012].

[50] Un análisis más exhaustivo del derecho al anonimato se puede encontrar en R. M.ª Orza Linares, «El derecho al anonimato en la Red» *Revista Telos*, Núm. 89: Redes Sociales y democracia, octubre-diciembre, 2011, pp. 24-33.

[51] Sentencia del Tribunal Constitucional (STC) 144/1999, de 22 de julio (Sala 2ª) Fundamento Jurídico 8. Se trataba de un complejo Recurso de Amparo en el que el recurrente, candidato a unas elecciones, había observado que su hoja de antecedentes penales había sido utilizada sin su consentimiento por la Junta Electoral competente en esas elecciones y, a través de ellas y de otras actuaciones judiciales, acordar su inelegibilidad. El recurrente pretendía que el Tribunal Constitucional anulara esa declaración de inelegibilidad por, entre otras consideraciones, su vulneración del

dando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio». Y, además, el art. 18,3 garantiza también el secreto de las comunicaciones [52].

Por ello, no es extraño que la *Directiva* de la Unión Europea 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas) fuera muy cuidadosa a la hora de garantizar el anonimato en llamadas telefónicas ante la posibilidad de que los operadores de telefonía pudieran comunicar el numero desde el que se llama a la hora de establecer una conexión telefónica. Así, en su parágrafo 34, la *Directiva* señalaba que «Es necesario, por lo que respecta a la identificación de la línea de origen, proteger el derecho del interlocutor que efectúa la llamada a reservarse la identificación de la línea desde la que realiza dicha llamada y el derecho del interlocutor llamado a rechazar llamadas procedentes de líneas no identificadas», lo que se justifica por el hecho de que «Determinados abonados, en particular las líneas de ayuda y otras organizaciones similares, tienen interés en garantizar el anonimato de sus interlocutores» [53].

Y, de hecho, el art. 8 de esta *Directiva* establece que «1. Cuando se ofrezca la posibilidad de visualizar la identificación de la línea de origen, el proveedor del servicio deberá ofrecer al usuario que efectúe la llamada

---

derecho a la intimidad. El Tribunal consideró que, en efecto, su derecho a la intimidad había sido vulnerado, pero no aceptó la anulación de las decisiones de la Junta Electoral en cuanto a la inelegibilidad.

[52] El art. 18,1 de la Constitución Española establece que: «Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen».

Y su párrafo 3 señala que «Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».

[53] PARLAMENTO EUROPEO Y CONSEJO *Directiva 2002/58/CE* de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Disponible *en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:ES:PDF* [Consulta: 25 de septiembre de 2012].

la posibilidad de impedir en cada llamada, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen. El abonado que origine la llamada deberá tener esta posibilidad para cada línea. 2. Cuando se ofrezca la posibilidad de visualizar la identificación de la línea de origen, el proveedor del servicio deberá ofrecer al abonado que reciba la llamada la posibilidad, mediante un procedimiento sencillo y gratuito, siempre que haga un uso razonable de esta función, de impedir la presentación de la identificación de la línea de origen en las llamadas entrantes», bien que con la posibilidad de eliminar esta opción en determinados casos (art. 10 de la *Directiva*) [54].

Esta *Directiva* fue trasladada al derecho interno español en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones que, en su art. 38,3 indica que: «En particular, los abonados a los servicios de comunicaciones electrónicas tendrán los siguientes derechos: … f) A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere o la presentación de la identificación de su línea al usuario que le realice una llamada. g) A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada» [55].

Si la mera ocultación del número de los teléfonos que realizan llamadas ha merecido tal atención dentro de la Unión Europea, como una indudable garantía para el ejercicio de diversos derechos fundamentales, mucho

[54] Art. 10: «…el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público podrá anular: … 2. la supresión de la presentación de la identificación de la línea de origen y el rechazo temporal o la ausencia de consentimiento de un abonado o un usuario para el tratamiento de los datos de localización, de manera selectiva por línea, para las entidades reconocidas por un Estado miembro para atender llamadas de urgencia, incluidos los cuerpos de policía, los servicios de ambulancias y los cuerpos de bomberos, para que puedan responder a tales llamadas».

[55] Es significativo que, si bien, la *Directiva* se refiere a las llamadas telefónicas, en la legislación española se extiende este derecho a las «comunicaciones electrónicas», concepto que parece más amplio que las meras llamadas telefónicas.

más interés debería tener la protección del anonimato a la hora de navegar por internet. Como es imaginable, el estudio de una mera relación de páginas visitadas por una persona concreta, sobre todo si el rastreo se refiere a un periodo de tiempo más o menos prolongado, puede ofrecer una enorme información sobre la personalidad, la economía, los gustos, las aficiones, las preocupaciones de ese ciudadano en concreto. El perfil obtenido puede ser utilizado con diversos fines y puede entrañar serias amenazas para su libertad o seguridad.

De hecho, la jurisprudencia internacional ha tenido ya la oportunidad de pronunciarse sobre estos extremos. Así, el Tribunal Europeo de Derechos Humanos, en su Sentencia de 3 de abril de 2007, «Caso Copland» [56], analizó si el seguimiento de las llamadas telefónicas, del uso del correo electrónico y de la navegación por internet realizada por los responsables de un «College» universitario de Gales (Reino Unido) sobre una trabajadora del mismo, suponía una violación de los derechos reconocidos en el Convenio Europeo de Derechos Humanos. En sus alegaciones, el Gobierno británico acepto que, en este caso, «si bien se efectuó cierto seguimiento de las llamadas, el correo electrónico y la navegación por Internet de la demandante con anterioridad a noviembre de 1999, no se llegó a interceptar las llamadas telefónicas ni a analizar el contenido de las páginas web visitadas por ella». Para el Gobierno inglés, «el seguimiento no consistió pues en nada más que un análisis de la información generada automáticamente para determinar si las instalaciones del College se habían usado con fines personales» [57]. Se trataba no de interceptar el contenido de las llamadas, o de los correos electrónico, sino de simplemente conocer a qué números se llamaba, a quién se enviaba los correos electrónico y el nombre o la dirección de las páginas web que se consultaba. Es más, según sus alegaciones, «En el supuesto de que el análisis de la relación de llamadas telefónicas, el correo

[56] Sentencia del TRIBUNAL EUROPEO DE DERECHOS HUMANOS (STEDH) 23/2007, de 3 de abril. La jurisprudencia del Tribunal, usualmente en francés o inglés, puede consultarse en la página web *http://www.echr.coe.int/*. La página web del Consejo de Europa es *http://www.coe.int/*

[57] Parágrafo 32.

electrónico e Internet se considerase una injerencia en el respeto de la vida privada o la correspondencia, el Gobierno señala que la injerencia estaba justificada» [58], Ya que, «En primer lugar, perseguía el fin legítimo de proteger los derechos y libertades de los demás al asegurar que no se abusase de unas instalaciones con cargo a los fondos públicos» y, en segundo lugar, «la injerencia tenía un fundamento en derecho interno en la medida en que el College, como organismo estatutario, cuyos poderes le facultan para ofrecer formación superior y hacer lo necesario y oportuno con tal propósito, tenía el poder de controlar razonablemente sus instalaciones para asegurar su capacidad de llevar a cabo sus funciones estatutarias». Concluía que «era razonablemente previsible que las instalaciones con las que cuenta un organismo estatutario con cargo a los fondos públicos no podían ser utilizadas en exceso con fines personales» [59].

A pesar de estas alegaciones, el Tribunal consideró que tales injerencias no estaban justificadas, ya que «según la reiterada jurisprudencia del Tribunal, las llamadas telefónicas que proceden de locales profesionales pueden incluirse en los conceptos de «vida privada» y de «correspondencia» a efectos del art. 8.1 (Sentencias Halford [TEDH 1997, 37], previamente citada, ap. 44 y Amann contra Suiza [TEDH 2000, 87] [GC], núm. 27798/1995, ap. 43, TEDH 2000-II). Es lógico pues que los correos electrónicos enviados desde el lugar de trabajo estén protegidos en virtud del art. 8, como debe estarlo la información derivada del seguimiento del uso personal de Internet» [60].

[58] Parágrafo 33.

[59] Parágrafo 34.

[60] Parágrafo 41. El Convenio Europeo de Derechos Humanos (4 de noviembre de 1950) señala que: «Art. 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».

Asimismo, el Tribunal recuerda que «la utilización de información relativa a la fecha y duración de las conversaciones telefónicas y en particular los números marcados, puede plantear un problema en relación con el art. 8 (RCL 1999, 1190 y 1572), ya que dicha información es «parte de las comunicaciones telefónicas» (Sentencia Malone contra el Reino Unido de 2 agosto 1984 [TEDH 1984, 1], serie A núm. 82, ap. 84)» y el hecho de que el College obtuviese esos datos legítimamente, «en forma de facturas telefónicas», no es impedimento para «constatar una injerencia en los derechos garantizados por el art. 8 (ibidem)» Y, lo que resulta más relevante, «el almacenamiento de datos personales relativos a la vida privada de una persona se halla también en el ámbito de aplicación del art. 8.1 (Sentencia Amann [TEDH 2000, 87], previamente citada, ap. 65)» [61]. Además el Tribunal considera que tal injerencia no estaba justificada ni por el derecho interno, ni por las normas internacionales [62].

Por todo ello, «el Tribunal considera que la recogida y almacenamiento de información personal relativa a las llamadas telefónicas, correo electrónico y navegación por Internet de la demandante, sin su conocimiento, constituye una injerencia en su derecho al respeto de su vida privada y su correspondencia, en el sentido del art. 8 del Convenio» [63], concediéndole a la recurrente una indemnización por daño moral y obligando al Gobierno británico a correr también con los gastos del proceso [64].

[61] Parágrafo 43.

[62] Parágrafos 45-48.

[63] Parágrafo 44.

[64] No obstante, la jurisprudencia mayoritaria del Tribunal Supremo considera que la obtención del número telefónico, por sí sólo no supone una injerencia en el ámbito protegido de la intimidad personal. Así, por ejemplo, la Sentencia del TRIBUNAL SUPREMO (STS) 921/2009 de 20 de octubre, considera, haciendo suyos unos votos particulares emitidos en la STS de 19 de febrero de 2007, que «Los números identificativos con los que operan los terminales no pueden constituir, por sí mismos, materia amparada por el secreto de las comunicaciones, pues afirmar lo contrario supondría, a nuestro juicio, confundir los medios que posibilitan la comunicación con la comunicación misma», y ello porque «Sostener semejante criterio no supone contradicción alguna, en nuestra opinión, con la doctrina del Tribunal Europeo de Derechos Humanos, significativamente la contenida en la Sentencia del denominado «caso

Así, hay que tener en cuenta que, en este mismo sentido de proteger la intimidad y el anonimato a la hora de navegar por internet, tanto la legislación de muchos países, como la actuación de las agencias gubernamentales de protección de datos, consideran a la dirección IP [65], un dato de carácter personal.

Malone», ni con la del Tribunal Constitucional ni, mucho menos aún, con la de esta misma Sala, pues esa doctrina se refiere a la extensión del ámbito protegido de la «comunicación» no tanto a los números telefónicos sino al hecho de que, a través de la averiguación de esos números, se conozcan extremos como el momento, la duración y, lo que es aún más importante, la identidad de las personas que establecen el contacto. Y eso sí que puede sostenerse que forma parte, auténticamente, de la «comunicación»».

[65] Según la WIKIPEDIA, una dirección IP es «una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del Modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se denomina también se ocupa para encontrar domicilios y toda la información necesariadirección IP dinámica (normalmente abreviado como IP dinámica). Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados generalmente tienen una dirección IP fija (comúnmente, IP fija o IP estática). Esta no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red. Los ordenadores se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS, que a su vez facilita el trabajo en caso de cambio de dirección IP, ya que basta con actualizar la información en el servidor DNS y el resto de las personas no se enterarán, ya que seguirán accediendo por el nombre de dominio..». COLABORADORES DE WIKIPEDIA. *Dirección IP* [en línea]. Wikipedia, La enciclopedia libre, 2012 [Consulta: 28 de octubre de 2012]. Disponible en *http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP*.

Así, el Grupo de Trabajo sobre el art. 29 [66], en su Dictamen 4/2007, sobre el concepto de datos personales, indicó que «si bien la identificación a través del nombre y apellidos es en la práctica lo más habitual, esa información puede no ser necesaria en todos los casos para identificar a una persona». Así puede suceder cuando se utilizan otros «identificadores» para singularizar a alguien. Efectivamente, los ficheros informatizados de datos personales suelen asignar un identificador único a las personas registradas para evitar toda confusión entre dos personas incluidas en el fichero. Y por lo que se refiere a internet «las herramientas de control de tráfico permiten identificar con facilidad el comportamiento de una máquina y, por tanto, la del usuario que se encuentra detrás. Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones. Sin ni siquiera solicitar el nombre y la dirección de la persona es posible incluirla en una categoría, sobre la base de criterios socioeconómicos, psicológicos, filosóficos o de otro tipo, y atribuirle determinadas decisiones puesto que el punto de contacto del individuo (un ordenador) hace innecesario conocer su identidad en sentido estricto». En otras palabras, «la posibilidad de identificar a una persona ya no equivale necesariamente a la capacidad de poder llegar a conocer su nombre y apellidos» [67].

Y, en particular, respecto de las direcciones IP el Dictamen señala que «el Grupo de trabajo considera a las direcciones IP como datos sobre una persona identificable», ya que como se indicó ya en el año 2000, «los pro-

[66] Este Grupo se creó en virtud del art. 29 de la *Directiva 95/46/CE*. Se trata de un organismo de la Unión Europea, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Este Grupo está compuesto por representantes de las autoridades nacionales de control de datos de los Estados miembros, de un representante del Controlador Europeo para la Protección de Datos (CEPD) y de un representante de la Comisión europea. Como ya hemos indicado, la dirección de internet en la que se puede consultar toda la legislación europea es *http://eur-lex.europa.eu/*.

[67] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Dictamen 4/2007 sobre el concepto de datos personales* (20 de junio de 2007), Disponible: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_es.pdf* [Consulta: 28 de octubre de 2012], p. 15.

veedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del art. 2 de la Directiva» [68]. Así, es posible que «en muchos casos exista la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como "cookies" con un identificador único o sistemas modernos de minería de datos unidos a bases de datos con información sobre usuarios de Internet que permite su identificación» [69]. Y ello sobre todo, si «el tratamiento de direcciones IP se lleva a cabo con objeto de identificar a los usuarios de un ordenador (por ejemplo, el realizado por los titulares de los derechos de autor para demandar a los usuarios por violación de los derechos de propiedad intelectual), el responsable del tratamiento prevé que los «medios que pueden ser razonablemente utilizados» para identificar a las personas pueden obtenerse, por ejemplo, a través de los tribunales competentes (de otro modo la recopilación de información no tiene ningún sentido), y por lo tanto la información debe considerarse como datos personales» [70].

Ya con anterioridad, la legislación española sobre protección de datos iba por el mismo camino. Así, el art. 3.a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se refiere a «dato de carácter personal» como «cualquier información concerniente a personas físicas identificadas o identificables». Y, en desarrollo de la mis-

[68] *Documento de trabajo WP 37: Privacidad en Internet*: - Enfoque comunitario integrado de la protección de datos en línea adoptado el 21.11.2000. Disponible en español en la siguiente dirección: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37es.pdf* [Consulta: 28 de octubre de 2012], p. 23.

[69] Ibidem.

[70] GRUPO DE TRABAJO … cit, pp. 18-19.

ma, su Reglamento, aprobado por Real Decreto 1720/2007, de 21 de diciembre, define en su art. 5.f) los datos de carácter personal como «cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a una personas físicas identificadas o identificables». El apartado o) del citado art. 5 recoge la definición de «persona identificable» y considera como tal «toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social».

Esta definición de dato personal se realiza en términos tan amplios que permite incluir sin ningún problema, como dato personal, todo aquel que permite vincular una información personal a una persona, condición que sin muchas complejidades, puede predicarse de las direcciones IP y en cumplimiento de ello han existido algunas resoluciones de la Agencia de Protección de Datos [71].

Desde otro punto de vista, grandes empresas de internet como Google han cuestionado que la dirección IP sea considerada un dato personal. Así, en un Encuentro que tuvo lugar en mayo de 2008, defendían que la dirección IP no podía ser un dato personal. Los argumentos más importantes eran que, en el caso de ordenadores compartidos —bibliotecas, cybercafés, etc.—

[71] *Resolución* de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS de fecha 5 de marzo de 2009. Se trata de una resolución dictada en un procedimiento abierto por una denuncia presentada por el Director de la Oficina de Defensa de los Derechos del Menor de las Islas Baleares en la que se ponía de manifiesto que una página web en que existía una red social denominada «Tcuento», publicaba las direcciones IP de las personas que participaban en la misma, muchos de ellos menores de edad. Este procedimiento no pudo concluir con sanción por no encontrar a la persona responsable de la citada página web. Ya hace algunos años esta Agencia ya defendía que la dirección IP era un dato de carácter personal, obligando al registro en la propia Agencia de las bases de datos que recogieran esos datos, en su *Informe 327/2003 «Carácter de dato personal de la dirección IP»*. El texto de esta Resolución y de las otras dictadas por esta Agencia, puede encontrarse en su página web: *http://www.agpd.es/*. Para una descripción somera de las características de esta Agencia, cfr, el extenso estudio realizado, ya hace algunos años, por M.M. SERRANO PÉREZ, *El derecho fundamental a la protección de datos*. Madrid, Civitas, 2003, pp. 471 y ss.

la asignación de direcciones IP podía ser compartida también por muchas personas diferentes, que muchos proveedores de internet asignaban direcciones IP dinámicas, por lo que varias cuentas diferentes podían usar la misma dirección IP durante el curso de una semana. Asimismo, que, en ambientes corporativos, cientos de usuarios podías estar conectados a una única dirección IP de salida [72], que una dirección IP por sí sola no puede asociarse a un individuo ni lo identifica, sino que sólo identifica a un equipo informático conectado a una red (de hecho, una variedad de equipos como impresoras, fax, escáneres, pueden poseer direcciones IP) o que, en fin, las direcciones IP pueden ser falsificadas o disfrazadas [73]. En este sentido señalaban la dificultad que se le plantean a empresas como Google, que recolectan direcciones IP «para garantizar la seguridad y la calidad de servicios», la caracterización de estos datos como «datos personales», tanto a la hora del impacto negativo que tendrían en sus operaciones técnicas, como a la hora de cumplir con los requisitos establecidos por las legislaciones nacionales para tratar los datos personales. Esto último, especialmente centrado en dos aspectos: requerir el consentimiento para el tratamiento de estos datos en el caso de usuarios no autenticados, incluyendo la prueba de que el consentimiento ha sido otorgado, y el ejercicio de los derechos de acceso, rectificación y cancelación.

[72] En este sentido, es significativo que en la *Resolución* de fecha 19 de julio de 2006 de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, se decidiera el archivo de una denuncia por publicación de datos personales por cuanto la dirección IP de la que provenía la información correspondía a un servidor *proxi* de la Universidad de Alicante, sin que constara que persona concreta podría haberla utilizado. El texto completo de la *Resolución* se puede consultar en la siguiente dirección electrónica: *https://www.agpd.es/portalweb/resoluciones/archivo_actuaciones/archivo_actuaciones_2006/common/pdfs/E-01055-2005_Resolucion-de-fecha-19-07-2006_Art-ii-culo-6-LOPD. pdf* [Consulta: 10 de noviembre de 2012].

[73] P. LESS ANDRADE, «Google, protegiendo la privacidad en Internet». En *VI Encuentro Iberoamericano de Protección de Datos*. Cartagena de Indias, mayo de 2009 (en línea). Localización: *https://www.agpd.es/portalweb/internacional/red_ iberoamericana/encuentros/VI_Encuentro/common/pla_privacidad_internet_vi_encuentro_iberoamerica.pdf* [Consulta: 10 de noviembre de 2012].

En cualquier caso, la desconfianza de las autoridades en el uso que por los ciudadanos se pueda estar haciendo de internet ha hecho que la Unión Europea haya aprobado la Directiva 2006/24/CE, que también modifica la anterior Directiva 2002/58/CE, en la que se establecía la obligación de los proveedores de acceso a internet de conservar los datos generados en las trasmisiones electrónicas.

Así, en los que podíamos considerar como la exposición de motivos de esta Directiva, se señala que, si bien los arts. 5, 6 y 9 de la anterior Directiva 2002/58/CE establecían como obligaciones de los proveedores que los datos obtenidos en las transmisiones a través de internet deberían borrarse o hacerse anónimos cuándo no se necesiten para la transmisión, «salvo los datos necesarios para la facturación o los pagos por interconexión» [74], también se permitía que los Estados miembros limitasen esta obligación, siempre que tales restricciones constituyeran «medidas necesarias, apropiadas y proporcionadas en una sociedad democrática para fines específicos de orden público, como proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, detección y enjuiciamiento de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas» [75]. Como varios Estados, entre ellos España [76], hicieron uso de esa posibilidad, aunque con una gran diversidad en sus legislaciones, su corrección e igualación venía obligada, que es lo que pretendía la nueva Directiva del año 2006.

Así, aunque «de conformidad con el art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamenta-

[74] PARLAMENTO EUROPEO Y CONSEJO *Directiva 2006/24/CE,* de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, que modifica la anterior *Directiva 2002/58/CE*. Parágrafo 3. Se puede localizar el texto de esta Directiva en la siguiente dirección: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF* [Consulta: 210 de noviembre de 2012].

[75] Art. 15, apartado 1, de la *Directiva 2002/58/CE.*

[76] En la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico.

les (CEDH), toda persona tiene derecho al respeto de su vida privada y de su correspondencia» y ello obliga a que no pueda existir injerencia de la autoridad pública en el ejercicio de este derecho, lo cierto es que esta injerencia podrá realizarse cuándo «esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria, entre otras cosas, para la seguridad nacional o la seguridad pública, la prevención de desórdenes o delitos, o la protección de los derechos y las libertades de terceros».

Y para la Unión Europea, «dado que la conservación de datos se ha acreditado como una herramienta de investigación necesaria y eficaz para aplicar la ley en diferentes Estados miembros, en particular en asuntos de gravedad como la delincuencia organizada y el terrorismo, es necesario garantizar que los datos conservados se pongan a disposición de las fuerzas y cuerpos de seguridad durante un determinado período de tiempo, con arreglo a las condiciones establecidas en la presente Directiva». Por consiguiente, «la adopción de un instrumento de conservación de datos que cumpla los requisitos del art. 8 del CEDH es una medida necesaria» [77]. No obstante, los datos que se deben conservar son los «generados o tratados como consecuencia de una comunicación o de un servicio de comunicación y no los datos que constituyen el contenido de la información comunicada. Los datos deben conservarse de tal manera que se evite que se conserven más de una vez. Los datos generados o tratados, cuando se presten servicios de comunicaciones electrónicas, se refieren a los datos accesibles». En particular, en lo referente a la conservación de datos relativos a los correos electrónicos y la telefonía por Internet, «la obligación de conservar datos sólo puede aplicarse con respecto a los datos de los servicios propios de los proveedores o de los proveedores de redes» [78].

Para ello, el art. 1 de la Directiva establece, en su apartado 1, la obligación de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones de conservar determinados datos generados o tratados por los mismos, «para garantizar que los datos estén disponibles con fines de investigación, detección y enjuicia-

[77] *Directiva 2006/24/CE,* parágrafo 9.
[78] Ibidem, Parágrafo 13.

miento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro», y en su apartado 2, que los citados datos son concretamente «los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado», pero no «se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas» [79].

El periodo de conservación de tales datos se establece en una horquilla que va desde los seis meses, como mínimo, a los dos años como máximo (art. 6).

En la ley española que aplica esta directiva, la Ley 25/2007 [80] se establece una regulación prácticamente idéntica a la recogida en la Directiva comunitaria, estableciendo concretamente que la duración de la conservación de los datos sea de doce meses [81]. Indica la exclusión del deber de conservación al propio contenido de las comunicaciones electrónicas «incluida la información consultada utilizando una red de comunicaciones electrónicas» [82], aunque el rango de datos que se deben conservar es muy amplio.

Así, por sólo citar los datos que se refieren a las comunicaciones electrónicas, los operadores deben conservar los «Datos necesarios para rastrear e identificar el origen de una comunicación: …Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) La identificación de usuario asignada.
ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.

[79] Art. 1 de la *Directiva 2006/24/CE*. Concretamente, en el art. 5 se pormenorizan los datos que necesitan ser conservados. Además, en el apartado 2 de este art. 5 se enfatiza de nuevo que «De conformidad con la presente Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación».

[80] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (publicada en el *Boletín Oficial del Estado*, núm. 251 de fecha 19 de octubre de 2007).

[81] Art. 5 de la Ley 25/2007.

[82] Art. 1.3 de la Ley 25/2007.

iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono» [83].

Asimismo, los «Datos necesarios para identificar el destino de una comunicación: … Con respecto al correo electrónico por Internet y la telefonía por Internet:

i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.
ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación» [84].

Por lo que se refiere a los «Datos necesarios para determinar la fecha, hora y duración de una comunicación … Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.
ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario» [85].

Y también los «Datos necesarios para identificar el tipo de comunicación. … Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado» [86].

Finalmente los «Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación: … Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

[83] Art. 3 a) 2. de la Ley 25/2007.
[84] Art. 3 b) 2. de la Ley 25/2007.
[85] Art. 3 c) 2. de la Ley 25/2007.
[86] Art. 3 d) 2. de la Ley 25/2007.

i) El número de teléfono de origen en caso de acceso mediante marcado de números.
ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación» [87].

Y para todo tipo de comunicaciones móviles, los «Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.º La etiqueta de localización (identificador de celda) al inicio de la comunicación.
2.º Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones» [88].

Pero es que, además, tampoco se escapan de este control las llamadas infructuosas. Así el art. 4,2 de la Ley 25/2007 extiende la obligación de conservación «a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada».

También señala concretamente que los datos deben cederse, previo mandamiento judicial [89], a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado, a los funcionarios del Servicio de Vigilancia Aduanera y al personal del Centro Nacional de Inteligencia [90] y el plazo para esta cesión de datos «Si no se establece otro plazo distinto» será de setenta y dos horas «contadas a partir de las 8:00 horas del día laborable siguiente a aquél en que el sujeto obligado reciba la orden» [91].

[87] Art. 3 e) 2. de la Ley 25/2007.
[88] Art. 3 f) 2. de la Ley 25/2007.
[89] Esta necesidad de mandamiento judicial para la cesión de estos datos, también se extendió al Ministerio Fiscal por decisión de la Sala General no jurisdiccional del Tribunal Supremo, con fecha 23 de febrero de 2010. *Vid.* STS 247/2010, ya citada.
[90] Art. 6 de la Ley 25/2007.
[91] Art. 7 de la Ley 25/2007.

En otras latitudes, también nos encontramos intentos gubernamentales de establecer medidas adicionales para evitar el anonimato en la Red. Concretamente en Perú, se está discutiendo una propuesta de ley [92], que ya ha sido sometida a una primera discusión en el Parlamento y que, en Dictamen aprobado por la Comisión de Justicia y Derechos Humanos del Congreso, de fecha 26 de junio de 2012, señala en su art. 23 que «no se encuentran dentro del secreto de las comunicaciones» los datos correspondientes a la identidad de los titulares de «… los números de protocolo de internet», estableciendo además, la obligación de las empresas proveedoras de servicios de ceder los datos anteriores, junto con los datos de identificación a la Policía o al Ministerio Público, eso sí, «con la autorización del juez a cargo del proceso».

Y en Méjico se ha aprobado una denominada popularmente «ley de Geolocalización» [93] que permite solicitar datos de geolocalización para investigaciones policiales, sin necesidad de una orden judicial de por medio y bajo motivos de mera sospecha [94]. Los proveedores que se nieguen a entregar la información recibirán una cuantiosa multa por negarse a cooperar

[92] El texto oficial del Pre Dictamen y el texto original de Proyecto de ley 0034/2011-CR se puede consultar en la siguiente dirección web: *http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc01_2011.nsf/0/9acc347a13bfb859052578e9007c116f/$FILE/PL00034110811.pdf* [Consulta: 10 de octubre de 2012]. Asimismo, el estado actual del proyecto puede consultarse en *http://www2.congreso.gob.pe/Sicr/TraDocEstProc/CLProLey2011.nsf* [Consulta: 10 de octubre de 2012] y el texto actual del proyecto en *http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc01_2011.nsf/d99575da99ebfbe305256f2e006d1cf0/c577d32aa8f2602605257a420003de03/$FILE/00034DC15MAY200712.PDF* [Consulta: 10 de octubre de 2012].

[93] Denominada oficialmente «Decreto por el cual «SE REFORMAN, ADICIONAN Y DEROGAN DIVERSAS DISPOSICIONES DEL CÓDIGO FEDERAL DE PROCEDIMIENTOS PENALES, DEL CÓDIGO PENAL FEDERAL, DE LA LEY FEDERAL DE TELECOMUNICACIONES, DE LA LEY QUE ESTABLECE LAS NORMAS MÍNIMAS SOBRE READAPTACIÓN SOCIAL DE SENTENCIADOS Y DE LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA» publicado en el *Diario Oficial de la Federación* el 17 de abril de 2012. El texto de la citada norma se puede consultar en la siguiente dirección web *http://www.dof.gob.mx/nota_detalle.php?codigo=5243973&fecha=17/04/2012* [Consulta: 10 de octubre de 2012].

[94] Concretamente el nuevo art. 133 Quáter señala que: «Tratándose de investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro,

con las autoridades. No obstante esta ley ha sido recurrida por la Comisión Nacional de los Derechos Humanos, ante la Suprema Corte de Justicia de la Nación por inconstitucional [95]. Los argumento esgrimidos son fundamentalmente tres: Que no es necesario una orden del juez para acceder a estos datos, que existe imprecisión en cuanto a las personas que pueden ser investigadas (la norma señala «»equipos de comunicación móvil asociados a una línea, que se encuentren *relacionados* con investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas») y falta de precisión en cuanto al tiempo de la duración de la investigación. Por todo ello, los recurrentes consideran que las medidas acordadas «tienen un sumo potencial para la trasgresión de los derechos fundamentales», por cuanto la facultad discrecional otorgada a las Procuradurías General de la República y locales, en concreto: «a) carece de limitación temporal; b) no es clara respecto de las personas que pueden o no se ser sujetas a la vigilancia y, c) no contempla la participación de la autoridad judicial en la autorización, supervisión y revocación de la misma».

3.2. **Datos personales y páginas web privadas**

Por lo que se refiere a la utilización de páginas web propiedad de entidades privadas, es obvio que debe primar en todo caso el consentimiento de los interesados. Ese requisito debe ser una condición previa para el uso de todas las facilidades que se ofrecen libremente en el ámbito de la red. Sin embargo, ese consentimiento está condicionado por varios factores. En primer lugar, las condiciones de uso de los diferentes sitios o páginas web normalmente se refieren a legislación ajena a la del país en la que se encuen-

---

extorsión o amenazas, el Procurador General de la República o los servidores públicos en quienes delegue la facultad, solicitarán por simple oficio o medios electrónicos a los concesionarios o permisionarios del servicio de telecomunicaciones la localización geográfica, en tiempo real, de los equipos de comunicación móvil asociados a una línea, que se encuentren relacionados».

[95] El texto de la demanda se puede consultar en *http://cndh.org.mx/Acciones_Inconstitucionalidad* [Consulta: 10 de octubre de 2012].

tra el usuario y suelen estar redactadas en un lenguaje críptico difícil de entender por la generalidad de las personas. Además, las grandes corporaciones que explotan sitios como «Microsoft», «Apple», «Google» o «Facebook, por citar las más conocidas, suelen situar sus sedes en Estados Unidos, dónde las regulaciones estatales de protección de los usuarios suelen tener una menor intensidad que, por ejemplo, en la Unión Europea. Además las condiciones se ofrecen sin posibilidad de ser matizadas por sus usuarios que sólo tienen la opción de aceptarlas o rechazarlas en bloque —y ya son conocidos los problemas derivados de los contratos de adhesión, en el ámbito de los derechos de los consumidores—. Por último, y no es un problema menor, no existen controles fiables que impidan que los menores de edad no estén aceptando —y por lo tanto, contratando— condiciones y términos legales que ni entienden ni están autorizados a suscribir.

La cuestión del consentimiento también tiene una enorme importancia en relación a la persecución de los delitos cometidos por la divulgación de datos o imágenes de terceros. Concretamente, por lo que se refiere a la comisión de un delito contra la intimidad consistente, por ejemplo, en la difusión de imágenes en internet, es necesario que su previa captación haya sido también delictiva. Como apunta Puente Aba, la difusión de imágenes captadas con consentimiento de los interesados, o mediante técnicas lícitas de captación de imágenes (por ejemplo, cámaras de seguridad), no resultaría delictiva [96]. Sin embargo, si la propia captación de imágenes no es consentida y con la intención de descubrir sus secretos o vulnerar su intimidad, ya sí estaríamos dentro lo prohibido por el art. 197 [97] del Código penal y podría imponerse la pena prevista en el mismo.

[96] Aunque la autora se refiere a los tipos contemplado en el art. 197 del Código Penal. No obstante, sí pueden ser típicos de un delito o falta de injurias, o constituir infracciones de la legislación (no penal) relativa a la protección del honor, de la propia imagen o de los datos personales. L. M.ª Puente Aba, «Difusión de imágenes ajenas en Internet: ¿ante qué delitos nos encontramos?» En J.C. Carbonell Mateu, y otros (dir.) *Constitución, Derechos Fundamentales y sistema penal* tomo II. Ed. Tirant lo Blanc, Valencia, 2009, pp. 1541-1547.

[97] Art. 197 del Código Penal Español: «1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, car-

Por lo demás, y en relación a combatir el anonimato, se observa una tendencia creciente a buscar datos reales de las personas que utilizan las redes sociales. No es sólo que una persona ceda voluntariamente sus datos, sino que se establecen controles y cruces de información con otros usuarios para comprobar que los datos que se introducen son reales, pertenecen a personas físicas identificables a los que, además, se les incita de muy diversas maneras, a seguir incluyendo información de carácter personal (profesión, nombres de los cónyuges, edad, sexo, lugar de residencia, centros de enseñanzas, aficiones, gustos literarios y musicales, etc.). Y a todo ello se le suma la posibilidad de vincular fotografías y vídeos personales. En definitiva nos encontramos con una exposición absoluta de la intimidad personal. En este sentido es muy reveladora la denominada «política de nombres» de «Google+». Así, esta empresa no tiene ningún problema en señalar que «es importante que uses tu nombre para que las personas que quieran relacionarse contigo puedan encontrarte. Tu nombre es aquel por el que te conocen tus amigos, familiares y compañeros de trabajo». Y en caso de que exista alguna «incidencia de nombre», la empresa te pedirá que envíe una prueba de que ése es tu nombre verdadero, incluso enviando documentación oficial escaneada [98]. En fin, no sólo quieren que demos nuestros datos verdaderos, bajo pena de bloquear o borrar todo el contenido que hayamos incluido en todos los servicios de «Google» («Gmail», «Blogger»,

---

tas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses… 4. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior…».

98 *Vid. http://support.google.com/plus/bin/answer.py?hl=es&answer=1228271* [Consulta: 15 de octubre de 2012].

etc.) sino que, además, quieren que, para acreditarlo fehacientemente, le enviemos copia de nuestra documentación oficial.

De hecho, sólo a través de las protestas y críticas públicas se ha podido obligar de alguna manera a las redes sociales a establecer algún grado de protección de la privacidad «por defecto» o a introducir algunos controles para los menores de edad [99].

Significativamente, las recomendaciones de la Agencia Española de Protección de Datos van en una línea radicalmente diferente [100]. Así, por lo que se refiere a las peticiones de nombres, la Agencia recomienda que «No utilice su nombre real para configurar el ordenador, aplicaciones, móviles y otros servicios de internet para los que no sea realmente necesario». Es más, la Agencia recuerda que «en Internet no todo el mundo es quien dice ser». Por lo tanto «si cuando solicitan sus datos no dicen para qué los van a usar, o no entiende lo que le dicen, nunca dé sus datos».

Por lo que afecta a las redes sociales señala que «Las redes sociales son una importante fuente para la obtención de información sobre las personas. Debe garantizar la seguridad de su información mediante una configuración adecuada de su perfil y utilizando contraseñas adecuadas. Tenga presente que los buscadores pueden permitir a cualquier tercero obtener la información pública de los perfiles». En todo caso, «No publique en los perfiles de las redes sociales excesiva información personal».

Y, por último, en relación al correo electrónico la Agencia también indica que «Conviene utilizar una segunda cuenta, aparte de la personal, para acceder a servicios con interés temporal o comerciales».

[99] Precisamente, Facebook, Inc. y Facebook Ireland Ltd, .hasta el día 10 de diciembre de 2012 han abierto una votación de sus usuarios sobre una «Declaración de derechos y responsabilidades» y una «Política de uso de datos». En línea, *http://www.facebook.com/* [Consulta: 4 de diciembre de 2012].

[100] Se trata de unas *Recomendaciones para una navegación más privada* en las que recoge numerosos consejos para la utilización responsable de internet. Puede consultarse en *http://www.agpd.es/portalwebAGPD/jornadas/dia_internet_2012/recomendaciones-ides-idphp.php* [Consulta: 10 de noviembre de 2012].

3.3. **Reconocimiento facial**

Especial atención debe prestarse últimamente a los programas de reconocimiento facial. Aunque ya hace años que se ha venido trabajando en tecnologías biométricas, con la finalidad de identificar personas a través de una imagen de la misma, lo cierto es que ya se han producidos avances muy significativos en este campo. De hecho es sorprendente la fiabilidad que están teniendo en el reconocimiento facial, programas de uso generalizado como, por ejemplo, «Picasa» o «Find my face» de «Google» o en «Facebook». Ello permite obtener datos personales para la identificación, localización y acceso a otros datos personales, sin consentimiento del interesado, simplemente a través del análisis de una imagen que contenga el rostro de esa persona y obtenida, por ejemplo, de otras imágenes online o capturadas con un simple teléfono móvil.

De hecho, como señala la Agencia Española de Protección de Datos en su Memoria de 2011, «la popularización de estos servicios, su implantación en redes sociales como Facebook o en servicios de reconocimiento facial y etiquetado de fotografías como «Find my Face» de Google, conlleva una serie de desafíos para la privacidad, como puede ser el tratamiento de imágenes digitales de personas que no utilizan el servicio y no han dado su consentimiento para ello, o la utilización de las imágenes para otras finalidades distintas para las que fueron tomadas». Hasta tal punto que, en opinión de la Agencia, «cabe llegar la posibilidad de buscar personas mediante la introducción de su imagen en un buscador (sacada por ejemplo a través de un teléfono móvil) obteniendo como resultado imágenes coincidentes o el perfil de una red social» [101].

Fruto de esas preocupaciones, el Grupo de Trabajo del art. 29 [102] de la Unión Europea adoptó unas recomendaciones en marzo de 2012. En este

[101] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Memoria AEPD 2011*. En línea, en *http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2011/common/Memoria_2011.pdf* p. 47 [Consulta: 10 de noviembre de 2012].

[102] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Dictamen 2/2012 sobre reconocimiento facial en los servicios en línea y móviles*. El do-

documento se observa que, actualmente, los servicios en línea y móviles « pueden captar imágenes de una persona (con o sin su conocimiento) y transmitirlas a continuación a un servidor remoto para su tratamiento». De hecho, «los servicios en línea, muchos de los cuales pertenecen a entidades privadas que se encargan de explotarlos, han acumulado vastos archivos de imágenes cargadas por los propios individuos». Es más, «en algunos casos, esas imágenes pueden haber sido obtenidas ilícitamente, recuperándolas de otros sitios públicos como las memorias caché de los motores de búsqueda», u obteniéndolas a través de fotografías realizadas con dispositivos móviles (cámaras o teléfonos, por ejemplo) que permiten a los usuarios «obtener imágenes y conectarse en tiempo real a servicios en línea a través de conexiones permanentes». En consecuencia, «los usuarios pueden compartir esas imágenes con otras personas o llevar a cabo una identificación, autenticación/verificación o categorización para acceder a información adicional sobre la persona, conocida o desconocida, que se encuentra delante de ellos» [103].

Por ello, y teniendo en cuenta que la imagen de una persona es considerado un dato personal que puede considerarse incluso como de categoría especial, por cuanto puede incidir en aspectos tales como origen étnico, religión o salud de una persona en concreto, el Grupo de Trabajo elabora unas recomendaciones. Así, recomienda a los responsables del tratamiento de los datos, un especial cuidado en la obtención del consentimiento de las personas cuyos imágenes están siendo obtenidas o tratadas. Asimismo éstos «deben asegurarse de que las imágenes digitales y las plantillas únicamente se utilizan para el objetivo especificado para el que han sido facilitadas». Debiendo establecer «controles técnicos para reducir el riesgo de que las imágenes digitales sean sometidas a tratamientos posteriores por parte de terceros para fines a los que el usuario no ha dado su consentimiento», así como «incorporar herramientas para que los usuarios controlen la visi-

---

cumento, adoptado el 2 de marzo de 2012, se puede consultar en *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_es.pdf* [Consulta: 10 de noviembre de 2012].

[103] Ibídem, p. 1.

bilidad de las imágenes que hayan publicado cuando la configuración por defecto sea restringir el acceso por parte de terceros». Además, «los responsables del tratamiento de los datos deberán asegurarse de que las imágenes digitales de las personas que no sean usuarios registrados del servicio o no hayan dado su consentimiento en otra forma para tal tratamiento únicamente sean objeto de tratamiento en la medida en que el responsable de los datos tenga un interés legítimo en el mismo» [104].

En todo caso, «los responsables del tratamiento de los datos deberán garantizar que los datos extraídos de una imagen digital para elaborar una plantilla no sean excesivos y contengan solamente la información necesaria para el fin previsto, evitando así cualquier tratamiento posible en el futuro», además de asegurarse de que las plantillas no pudieran «ser transferibles de un sistema de reconocimiento facial a otro». Finalmente, «el responsable del tratamiento de los datos deberá facilitar a las personas afectadas los mecanismos adecuados para ejercer su derecho de acceso, cuando proceda, tanto a las imágenes originales como a las plantillas generadas en el contexto del reconocimiento facial» [105].

Pero, en la práctica, estas funcionalidades han supuesto una invasión tan importante en la privacidad que también algunas autoridades de protección de datos han adoptado medidas más enérgicas al respecto. Así, en Irlanda, el Comisionado para la Protección de Datos inició una investigación sobre «Facebook» [106] en la que concluyeron que la posibilidad de establecer eti-

[104] Ibídem, p. 8. En todo caso, para la correcta valoración del interés legítimo, puede consultarse la *Sentencia* del TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA de 24 de noviembre de 2011 en el que se resuelve una cuestión prejudicial presentada por el Tribunal Supremo en relación al concepto de «interés legítimo». La sentencia se puede obtenerse en *http://curia.europa.eu/juris/document/document.jsf?docid=115205&doclang=ES&mode=&part=1* [Consulta: 10 de noviembre de 2012]. También la STS de 8 de febrero de 2012. Puede consultarse en *http://www.elderecho.com/administrativo/Tribunal-Contencioso-Administrativo-Sentencia-Recurso-EDJ_EDEFIL20120215_0007.pdf* [Consulta: 10 de noviembre de 2012].

[105] Ibídem, pp. 9 y 10.

[106] El informe se puede consultar en *http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf* [Consulta: 10 de octubre

quetas de nombre en las imágenes, sin consentimiento de las personas interesadas no era admisible. «Facebook», posiblemente ante el temor de un endurecimiento de las políticas de privacidad en Europa, y antes de agotar el plazo de cuatro semanas que se le había otorgado (cuyo incumplimiento podría conllevar la imposición de una multa de 100.000 euros) actuó desactivando ese servicio. Asimismo se comprometió a eliminar antes del 15 de octubre de 2012 cualquier patrón o modelo de datos que se usara como base para reconocer las caras de los usuarios. No obstante es fácil augurar que estas tecnologías seguirán teniendo un uso intensivo en el futuro.

4. **DERECHO AL OLVIDO**

4.1. **Consideraciones generales**

La otra cara de la moneda para proteger la libertad de los ciudadanos, una vez que nuestra identidad ya haya aparecido claramente incorporada a la red, la protagoniza el «derecho al olvido». Este derecho debería entenderse como el derecho de las personas a impedir que datos personales propios circulen por internet sin su consentimiento. Las razones pueden ser muy variadas, pero en lo que se refiere a datos cuyo conocimiento pueda perjudicar a las personas, de lo que se trata, como ha señalado Pere Simón recientemente, es de tener la posibilidad de «equivocarse y volver a empezar» [107].

---

de 2012]. Otras autoridades de protección de datos, como las de Noruega, por ejemplo, también anunciaron a lo largo del verano de 2012 que iniciaban investigaciones sobre el reconocimiento facial en «Facebook» Cfr. *http://www.bloomberg.com/news/2012-08-02/facebook-faces-norway-probe-over-facial-recognition-photo-tags.html* [Consulta: 10 de octubre de 2012].

[107] P. SIMÓN CASTELLANO: «El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos» *Ponencia presentada en el Congreso Libertad, transparencia y política en Internet: ejercicio, amenazas y garantías*. Madrid, Centro de Estudios Políticos y Constitucionales, Madrid, 19

De hecho, como también ha apuntado este autor, este «derecho a equivocarse» está contemplado en nuestros ordenamientos de maneras muy diversas [108]. De hecho, en todos los países de nuestro entorno cultural existen normas sobre la prescripción de los delitos, sobre la cancelación de antecedentes penales que constan en los Registros Públicos o sobre la cancelación de informaciones sobre aspectos económicos que pudieran afectar a las personas (quiebras, insolvencias, etc.). Es más, es posible encontrar resoluciones jurisdiccionales que defienden y amparan en diversos países un cierto «derecho al olvido», sobre todo en lo atinente a cuestiones penales [109].

4.2. **El derecho al olvido en España**

Entre nosotros, la Agencia Española de Protección de Datos, principalmente desde el año 2007, ha realizado una importante labor en defensa de

---

y 20 de octubre de 2012. Pendiente de publicación. Su monografía El Régimen Constitucional del Derecho al Olvido Digital (Ed. Tirant Lo Blanc, Valencia, 2012) es imprescindible para el conocimiento actual de esta materia. También L. COTINO HUESO «Entre el derecho al olvido y el olvido de la libertad de información y la transparencia». *Ponencia presentada en el Congreso Libertad, transparencia y política en Internet: ejercicio, amenazas y garantías*. Madrid, Centro de Estudios Políticos y Constitucionales, Madrid, 19 y 20 de octubre de 2012. Pendiente de publicación. *Vid.* también, desde un punto de vista más general, L. COTINO HUESO (editor), *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*, PUV (Publicaciones de la Universidad de Valencia), Valencia, 2011.

[108] Y cita, entre otras, «la anonimización de los datos personales en la publicación de las sentencias, la cancelación de antecedentes penales, la regulación de la amnistía» entre otros. P. SIMÓN CASTELLANO «El carácter relativo del derecho al olvido…», *op. cit.*

[109] Cfr. A. PACE «El derecho a la propia imagen en la sociedad de los mass media» *Revista Española de Derecho Constitucional*, núm. 52, enero-abril de 1998, pags. 33-52. En especial, la p. 48 y la nota núm. 50. No obstante el autor se muestra bastante pesimista sobre la posibilidad de que un afectado pueda impedir que los medios de comunicación vuelvan a publicar noticias o informaciones de su vida pasada, si vuelve a ser relevante.

los derechos de los ciudadanos a que sus datos no circulen por internet sin su consentimiento, aunque ha centrado su objetivo en impedir no tanto que los datos no estén contemplados en la páginas de internet, sino en que los buscadores, en especial «Google» no indexara en sus búsquedas esos datos [110]. Esta solución, aunque pudiera satisfacer en parte los intereses de los particulares que recurrían, no deja de ser insatisfactoria, ya que no afecta a la propia existencia de los datos en la red, sino a dificultar que se encuentren.

En la actualidad esta vía de resolución de los conflictos está en una cierta vía muerta por cuanto «Google Spain S.L.» ha recurrido estas resoluciones ante la Audiencia Nacional al considera que la responsabilidad de mantener esos datos accesibles al público es de terceros ajenos. Así, en el curso del procedimiento ordinario 725/2010 que se sigue a su instancia contra la Agencia Española de Protección de Datos, se ha dictado un Auto de fecha 27 de febrero de 2012 en el que la Sala de lo Contencioso Administrativo (Secc. 1) de la Audiencia Nacional acuerda el planteamiento de una cuestión prejudicial de interpretación ante el Tribunal de Justicia de la Unión Europea para que este Tribunal declare, entre otras cuestiones «Si la actividad de GOOGLE, como buscador de contenidos de terceras personas, puede considerarse un tratamiento de datos» y, por lo tanto, debe garantizar los derechos de cancelación y oposición, «Si la AEPD … puede requerir a GOOGLE para que cancele o bloquee la información, aun cuando su mantenimiento en la página de origen sea lícita, pero el solicitante considere que su aparición en los resultados de búsqueda atenta a su privacidad, dignidad o al derecho al olvido « y, en definitiva, «si la AEPD … puede requerir directamente al buscador, sin dirigirse previa o simultáneamente al

[110] Un análisis exhaustivo de las resoluciones de la Agencia Española de Protección de Datos puede encontrarse en R.M. Orza Linares, y S. Ruíz Tarrías «El derecho al olvido en Internet» En A. Carrillo i Martínez, M. Peguera, I. Peña-López y M. Vilasau Sonala (coord.) *Neutralidad de la red y otros retos para el futuro de Internet. Actas del VII Congreso Internacional Internet, Derecho y Política*. Universitat Oberta de Catalunya, Barcelona, 11-12 de julio de 2011. Ed. Huygens, Barcelona, 2011. Pp. 371-389 (el texto, disponible en pdf, se puede obtener en *http://goo.gl/bs4kO*) [Consulta: 25 de septiembre de 2012].

webmaster para exigir la retirada de la información» [111]. En la actualidad este procedimiento todavía no ha concluido.

Recientemente, desde 2010, la Agencia también ha comenzado a interpretar más rigurosamente los requisitos que los recurrentes deben cumplir para atender sus reclamaciones. Así, deben concurrir las siguientes circunstancias para que el citado derecho de oposición regulado en el art. 34.a) del Reglamento de la Ley Orgánica de Protección de Datos aprobado por Real Decreto 1720/2007, pueda ser atendido: «a) Que exista un motivo legítimo y fundado. b) Que dicho motivo se refiera a su concreta situación personal y c) Y que el motivo alegado justifique el derecho de oposición solicitado» [112]. En el mismo sentido, una Resolución de fecha 12 de julio de 2012 señala que «desde ese análisis de los requisitos legales, no se parecía motivo legítimo y fundado que justifique el derecho de oposición en este caso, ya que se trata de un supuesto de relevancia pública, en el que no se han acreditado que los datos, y la información que éstos proporcionan, sean inexactos o hayan quedado obsoletos». Criterio que hasta el momento sólo se había aplicado a los medios de comunicación en sentido estricto [113].

Como novedad, en las últimas Resoluciones de la Agencia también aparecen los buscadores «Yahoo» o «Bing», aunque es de reseñar que tanto uno como otro se niegan a reconocerle autoridad a la Agencia para imponerle sus decisiones. En el caso de «Bing» suele alegar que tiene su sede operativa en Luxemburgo, y por lo tanto no le afecta la legislación española, y

[111] El texto del Auto, ya citado, en formato pdf, se puede obtener en *http://goo.gl/ASVo0* [Consulta 25 de octubre de 2012].

[112] *Resolución* de 17 de febrero de 2010, en base a una queja presentada por un particular. Disponible en *http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-01435-2009_Resolucion-de-fecha-17-02-2010_Art-ii-culo-6.4-LOPD_Recurrida.pdf* [Consulta: 25 de septiembre de 2012].

[113] *Resolución* de 12 de julio de 2011, en base a una queja presentada por un particular contra una información publicada que lo relacionaba con un caso de narcotráfico. Disponible en *http://www.agpd.es/portalwebAGPD/resoluciones/tutela_ derechos/tutela_derechos_2011/common/pdfs/TD-00249-2011_Resolucion-de-fecha-12-07-2011_Art-ii-culo-16-LOPD-34-RD-1720-b-2007.pdf* [Consulta 25 de septiembre de 2012].

«Yahoo» se remite a un acuerdo que posee con Microsoft Corp. por lo que toda reclamación presentada contra ella debe entenderse contra Microsoft Corp., en su sede de Redmond, Washington, Estados Unidos.

A pesar de todo ello, según datos de la propia Agencia, las reclamaciones sobre «derecho al olvido» han aumentado en 2011 un ochenta por ciento en relación con las reclamaciones presentadas en el año 2010. Concretamente, la Agencia señala que se han presentado, en 2011, un total de 160 reclamaciones para solicitar la cancelación de datos personales en internet, que contrasta con las tres reclamaciones que se presentaron en 2007 [114]. En todo caso, como señala la propia Agencia en su Memoria de 2011, esta demanda creciente de los ciudadanos sólo se puede atender desde su conexión con los tradicionales derechos de cancelación y oposición [115].

En esta misma línea de incidir sobre los buscadores y no sobre la fuente de los datos, también la Agencia ha emitido distintas resoluciones y recomendaciones en relación con los instrumentos técnicos apropiados para evitar la indexación de las páginas web por los buscadores.

Concretamente, en relación con los datos publicados por el Boletín Oficial del Estado (B.O.E.), la Agencia, en una significativa Resolución, la dictada el 28 de agosto de 2012 en el que se analiza una reclamación de un ciudadano contra la publicación en el B.O.E. de sus datos a propósito de la concesión de un indulto. Aunque la Agencia rechaza la reclamación, es muy interesante el razonamiento que recoge en su Resolución. Así, tras concluir que el BOE «al publicar en su página web los datos personales de ciudadanos, está realizando un tratamiento de datos total o parcialmente automatizado; y ello aunque exista una obligación legal de publicar determinados actos administrativos y de que sea considerado una fuente de acceso público», ello no le exime —según la legislación vigente en materia de protección de datos de carácter personal— «de adoptar las medidas necesarias, y adecuadas según el estado actual de la tecnología, para evitar la indexación

[114] Datos recogidos en la *Memoria* de sus actividades correspondientes al año 2011. Se puede consultar en *http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2011/common/Memoria_2011.pdf* [Consulta 10 de noviembre de 2012]. P. 44.

[115] Ibídem, p. 45.

de los datos personales del reclamante en sus páginas, con objeto de que en el futuro los motores de búsqueda de internet no puedan asociarlas a él y con ello se impida la divulgación de manera indiscriminada de sus datos personales».

Por ello, la Agencia considera que «si bien el ciudadano no puede oponerse al mantenimiento en el Boletín Oficial de sus datos de carácter personal, al resultar éste perfectamente legítimo por encontrarse amparado en la Ley que ordena la publicación de los Reales Decretos de indulto, sí puede sin embargo el ciudadano oponerse —en los casos en que exista un motivo legítimo y fundado en el sentido previsto en el art. 6.4 de la LOPD— a que sus datos personales sean objeto de tratamiento previniendo su posible captación por los buscadores de Internet o dicho de otra forma, obstaculizando una cesión para el tratamiento por los mismos por los responsables de dichos motores de búsqueda» [116].

Y el estado actual de la tecnología a la que se refiere la Agencia, consiste en la utilización de un archivo denominado *robots.txt* que se inserta en el fichero que se sube a internet y que recoge los datos que los buscadores no deben indexar a la hora de rastrear las páginas webs.

Pero la utilización de esos ficheros por el BOE tampoco es pacífica. De hecho, el Boletín los vino utilizando hasta 2010, pero luego dejo de hacerlo, por lo que todo lo que aparecía en el Boletín era indexado y clasificado por los buscadores. La Agencia se ocupó de ello y, en una Resolución de fecha 23 de noviembre de 2011 indicó que «La AEPD entiende que, en el actual estado de la tecnología —al margen de las mejoras técnicas que quepa introducir sobrevenidamente (sic.)— la adopción del protocolo de la industria denominado «robots.txt» es un método válido para atender las solicitudes de los ciudadanos que, de acuerdo con lo previsto en el Capítulo IV del Título III del Reglamento de desarrollo de la LOPD han ejercitado su derecho de cancelación o de oposición ante un boletín o diario oficial, al

[116] *Resolución* de 29 de agosto de 2012. Disponible en: *http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-01018-2012_Resolucion-de-fecha-29-08-2012_Art-ii-culo-34-RD-1720-b-2007.pdf* [Consulta 10 de noviembre de 2012].

considerar que existen motivos que justifican la cesación del tratamiento consistente en permitir la indexación de sus datos publicados en una determinada edición» [117]. De hecho, el BOE comunicó a la Agencia que volvía a utilizar esos ficheros para que los buscadores no indexaran los datos que aparecían allí [118].

En cualquier caso, esto es una solución parcial, ya que en nuestro país existen numerosos Boletines Oficiales (uno por cada Comunidad Autónoma, uno por cada provincia, etc.) que están faltos de una regulación común y donde cada uno ofrece soluciones distintas y, además, en la actualidad los buscadores han empezado a ofrecer en sus resultados de búsquedas algunos de los datos que, en teoría no hubieran podido obtener, de acuerdo con el contenidos en esos ficheros *robots.txt* [119].

4.3. **El estado de la cuestión en la Unión Europea**

Por lo que se refiere a los intentos de regulación legal, en estos momentos, está en discusión, en la Comisión del Parlamento Europeo encargada de Libertades Públicas, Justicia y Asuntos de Interior, la Propuesta de Reglamento de la Comisión Europea sobre la «Protección de los individuos con respecto al procesamiento de datos personales y el libre flujo de dichos datos» de fecha 25 de enero de 2012 [120]. Esta Propuesta, en su art. 17 (*Derecho al olvido y a la supresión*), dispone que:

[117] *Resolución* de fecha 23 de noviembre de 2011. Disponible en: *http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-00950-2011_Resolucion-de-fecha-23-11-2011_Art-ii-culo-34-RD-1720-b-2007.pdf* [Consulta: 10 de septiembre de 2012].

[118] En la siguiente página web puede consultarse su fichero *robots.txt*: *http://www.boe.es/robots.txt* [Consulta: 10 de noviembre de 2012].

[119] No obstante, en las últimas semanas el buscador «Google» está ofreciendo páginas no indexables por el archivo *robots.txt*, pero acompañándolos de la siguiente información: «No hay disponible una descripción de este resultado debido al archivo *robots.txt* de este sitio».

[120] Se puede consultar en: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF* [Consulta: 25 de septiembre de 2012].

«1. El interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión, especialmente en lo que respecta a los datos personales proporcionados por el interesado siendo niño, cuando concurra alguna de las circunstancias siguientes:

a) los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados;

b) el interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el art. 6, apartado 1, letra a), o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos;

c) el interesado se opone al tratamiento de datos personales con arreglo a lo dispuesto en el art. 19;

d) el tratamiento de datos no es conforme con el presente Reglamento por otros motivos.

2. Cuando el responsable del tratamiento contemplado en el apartado 1 haya hecho públicos los datos personales, adoptará todas las medidas razonables, incluidas medidas técnicas, en lo que respecta a los datos de cuya publicación sea responsable, con miras a informar a los terceros que estén tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. Cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales, será considerado responsable de esa publicación.

3. El responsable del tratamiento procederá a la supresión sin demora, salvo en la medida en que la conservación de los datos personales sea necesaria:

a) para el ejercicio del derecho a la libertad de expresión de conformidad con lo dispuesto en el art. 80;

b) por motivos de interés público en el ámbito de la salud pública de conformidad con lo dispuesto en el art. 81;

c) con fines de investigación histórica, estadística y científica de conformidad con lo dispuesto en el art. 83;

d) para el cumplimiento de una obligación legal de conservar los datos personales impuesta por el Derecho de la Unión o por la legislación de un Estado miembro a la que esté sujeto el responsable del tratamiento; las legislaciones de los Estados miembros deberán perseguir un objetivo de interés público, respetar la esencia del derecho a la protección de datos personales y ser proporcionales a la finalidad legítima perseguida;

e) en los casos contemplados en el apartado 4.

4. En lugar de proceder a la supresión, el responsable del tratamiento limitará el tratamiento de datos personales cuando:

a) el interesado impugne su exactitud, durante un plazo que permita al responsable del tratamiento verificar la exactitud de los datos;

b) el responsable del tratamiento ya no necesite los datos personales para la realización de su misión, pero estos deban conservarse a efectos probatorios; c) el tratamiento sea ilícito y el interesado se oponga a su supresión y solicite en su lugar la limitación de su uso;

c) el interesado solicite la transmisión de los datos personales a otro sistema de tratamiento automatizado de conformidad con lo dispuesto en el art. 18, apartado 2.

5. Con excepción de su conservación, los datos personales contemplados en el apartado 4 solo podrán ser objeto de tratamiento a efectos probatorios, o con el consentimiento del interesado, o con miras a la protección de los derechos de otra persona física o jurídica o en pos de un objetivo de interés público.

6. Cuando el tratamiento de datos personales esté limitado de conformidad con lo dispuesto en el apartado 4, el responsable del tratamiento informará al interesado antes de levantar la limitación al tratamiento.

7. El responsable del tratamiento implementará mecanismos para garantizar que se respetan los plazos fijados para la supresión de datos personales y/o para el examen periódico de la necesidad de conservar los datos.

8. Cuando se hayan suprimido datos, el responsable del tratamiento no someterá dichos datos personales a ninguna otra forma de tratamiento.

9. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el art. 86, a fin de especificar:

a) los criterios y requisitos relativos a la aplicación del apartado 1 en sectores y situaciones específicos de tratamiento de datos;

b) las condiciones para la supresión de enlaces, copias o réplicas de datos personales procedentes de servicios de comunicación accesibles al público a que se refiere el apartado 2;

c) los criterios y condiciones para limitar el tratamiento de datos personales contemplados en el apartado 4».

Aunque aún es pronto para ver cuál puede ser la redacción definitiva de este Reglamento, lo cierto es que se siguen observando muchas similitudes con el derecho de cancelación ya conocido y estudiado. La novedad,

por lo tanto, puede estribar en la posibilidad de armonizar las legislaciones internas en esta materia y en la capacidad que pueda tener la Unión Europea para obligar a los grandes portales y buscadores de internet en el cumplimiento de esta regulación. A pesar de estas limitaciones, esta armonización es una posibilidad esperanzadora.

Por lo que respecta a intentos de regulación en otros países, en la mayoría de las ocasiones lo que ocultan son intentos más o menos elaborados de control de lo que se publica en internet o, incluso, de censura [121].

Así, en Italia está en estos momentos en discusión parlamentaria un Proyecto de Ley sobre difamación [122] con una serie de enmiendas que, si se aprobaran, podría permitiría a cualquier persona que considere que una entrada en Wikipedia es ofensiva a su imagen, la posibilidad de ordenar la corrección o la eliminación de dicho contenido. Ante la gravedad de esta regulación, la propia página de Wikipedia en italiano publicó un comunicado señalando que la aprobación de esa futura ley en esos términos posiblemente supondría la desaparición de Wikipedia en italiano [123]. Concretamente, la enmienda 3400 [124] permitiría que «l'interessato, anche senza esperire la procedura di cui al comma 2, può chiedere al prestatore di servizi della società dell'informazione l'eliminazione dei contenuti diffamatori o dei dati personali trattati in violazione della presente legge». En caso de negativa a la eliminación el responsable de la página pudiera ser condenado con multas. A la fecha de la redacción de este trabajo el Senado italiano todavía no ha terminado la discusión de este proyecto de ley.

[121] Cfr. R. ORZA LINARES «El derecho al olvido en internet: Algunos intentos para su regulación legal» *Comunicación presentada en el Congreso Libertad, transparencia y política en Internet: ejercicio, amenazas y garantías*. Centro de Estudios Políticos y Constitucionales, Madrid, 19 y 20 de octubre de 2012.

[122] El texto original de la propuesta puede consultarse en *http://www.senato.it/japp/bgt/showdoc/16/DDLPRES/679457/index.html* [Consulta:10 de noviembre de 2012].

[123] El comunicado se puede leer en *http://it.wikipedia.org/wiki/Wikipedia:Comunicato_24_ottobre_2012/es* [Consulta: 10 de noviembre de 2012].

[124] El texto de la Enmienda completa puede consultase en: *http://www.senato.it/japp/bgt/showdoc/frame.jsp?tipodoc=Emend&leg=16&id=681524&idoggetto=709641* [Consulta: 10 de noviembre de 2012].

5. CONCLUSIONES

Aunque en estos temas la elaboración de las conclusiones no puede tener sino una finalidad esencialmente provisional, sí me gustaría poner algunos aspectos de manifiesto.

El primero de ellos es la vigencia del debate sobre la necesidad de incorporar al orden jurídico nuevos derechos de carácter fundamental. De hecho desde la aparición de las primeras Declaraciones de Derecho, y especialmente la Declaración de Derechos del Hombre y del Ciudadano de 1789, la necesidad de completar y aumentar los derechos allí recogidos ha sido una necesidad social, analizada doctrinal y jurisprudencial de manera constante.

Así, como es conocido, a la «primera generación» de derechos de carácter estrictamente liberal, que pretendían garantizar a la persona simplemente una esfera de libertad y autonomía (libertad, igualdad, propiedad, etc.), le siguió una «segunda generación» de derechos vinculados a la creación constitucional del Estado social. La definitiva incorporación de este tipo de Estado a las Constituciones, llevó a sus textos nuevos derechos fundamentales como el derecho a la educación, al trabajo, a la seguridad social, a la huelga, que, además, exigían un intervencionismo estatal para garantizar su eficacia.

Y más posteriormente se ha planteado en el debate social y doctrinal la necesidad de ir incorporando a las Constituciones nuevos derechos constitucionales como el derecho a un medio ambiente adecuado, a la protección del patrimonio, a la salud o el acceso a la cultura. En esa línea, Constituciones como la española de 1978 ya realizaron una cierta incorporación de estos nuevos derechos a su articulado, aunque en este caso se hiciera a través de su consideración como «Principios», con una eficacia diferida a su posterior desarrollo legal [125].

[125] Una evolución muy ilustrativa del contenido de la Constitución, en lo que se refiere a los derechos, lo podemos encontrar en M. BONACHELA MESAS «Los Derechos y Deberes fundamentales» en M. BONACHELA; J. CAZORLA y J.J. RUIZ-RICO *Derechos, Instituciones y Poderes en la Constitución de 1978*. Granada, 1983, pp. 147 y ss.

Y cuando aún no se ha terminado de llegar a un consenso sobre qué derechos pueden ser incluidos en esta «tercera generación», ni acaban de encontrarse cauces idóneos para hacerlos realmente efectivos [126], se abre con enorme fuerza la necesidad de definir otro nuevo conjunto de derechos a incluir en los textos constitucionales, vinculados a lo que empieza a conocerse como la «sociedad del conocimiento» y que vayan más allá de la mera protección de los datos personales o de una adaptación más o menos forzada de los derechos tradicionales.

Se trataría de un serio intento doctrinal de evitar la disociación de la sociedad en razón a su conocimiento o ignorancia de estas nuevas tecnologías de la información y de la comunicación. Por lo tanto, se habla de la necesidad de, en primer lugar, garantizar el derecho de acceso para todos los ciudadanos a estas nuevas tecnologías (para evitar lo que se conoce como la «brecha digital») [127], con independencia de su nivel cultural, social o económico. Pero también de hacer efectivos otros derechos como el de la autodeterminación informativa (lo que se ha venido denominando «habeas data») y el conocimiento de los mecanismos de control en la utilización de los datos personales por terceros [128], la extensión del secreto de las

[126] Piénsese en los problemas derivados del cumplimiento efectivo de derechos como los recogidos en el art. 45.1 de la Constitución española: «Todos tienen el derecho a disfrutar de un medio ambiente adecuado para el desarrollo de la persona, así como el deber de conservarlo», o en el art. 47 del mismo texto legal: «Todos los españoles tienen derecho a disfrutar de una vivienda digna y adecuada», que tantos debates está planteando en la sociedad española actual.

[127] No hay que olvidar que el hecho de que distintas partes de la sociedad cambien a distinta velocidad, que unas se muevan rápidamente y otras se retrasen es fuente de tensiones sociales. El llamado «*cultural lag*» es un fenómeno estudiado desde hace años y cuyas consecuencias se conocen detalladamente. Cfr, F. MURILLO FERROL *Estudios de sociología política*. Madrid, Tecnos, 1972, pp. 93 y ss.

[128] Incluyendo por supuesto, a los propios funcionarios de las administraciones públicas. De hecho, en 2009, la Secretaría General de la Administración de Justicia tuvo que emitir una Circular en la que acordaba «calificar de indebidas todas las consultas que, sin estar autorizadas por resolución judicial se realicen a través de las aplicaciones disponibles en el Punto Neutro Judicial», de tal modo que se obligaba a «poner en conocimiento de los Secretarios Judiciales la realización de cualquier consulta

comunicaciones a las comunicaciones electrónicas, la garantía de un cierto derecho al anonimato cuando se navegue por internet, se hagan transacciones económicas o se participe políticamente a través de la Red, o, entre otros, de la implantación de un derecho al olvido con la cancelación de datos privados incorporados a internet.

Además, también es necesario tener en cuenta la aparición de reguladores privados diferenciados de los aparatos tradicionales del Estado (administración pública, policía, tribunales), que poseen, y de modo creciente, un enorme poder. Por poner algunos ejemplos, la fuerza que pueden tener los proveedores de acceso o de contenido a la red o la posibilidad que tienen buscadores como Yahoo, Google o Bing (Microsoft), de establecer mecanismos de censura privados, incluso de manera opaca, sin conocimiento de su existencia por parte de los ciudadanos o de las administraciones públicas nacionales, pueden suponer una enorme amenaza para el ejercicio de las libertades ciudadanas.

Pero el camino para la incorporación a los textos constitucionales de estos nuevos derechos nunca es fácil ni rápido. De hecho, es común la resistencia de las Constituciones a las reformas (la idea de la «rigidez» constitucional), por lo que en la práctica se ha acudido con frecuencia, en ocasiones anteriores, a otras vías para atender estas nuevas necesidades puestas

---

indebida realizada por los funcionarios, por si consideraban conveniente proceder a su baja como usuarios de la aplicación de consulta». Es más, «Si las consultas indebidas fueron realizadas por los Secretarios Judiciales, se pondrá en conocimiento de los Secretarios de Gobierno a los efectos oportunos». Y además, se establecía que «respecto a la consultas no autorizadas por resolución judicial de las que pudiera derivarse la comisión de una falta grave o muy grave por perseguir la obtención de cualquier tipo de información relativa a ex cónyuges, familiares o terceras personas, físicas o jurídicas, que guarden cualquier relación con cónyuges o familiares de los usuarios, se remitirá copia a las Administraciones disciplinariamente competentes para que, en su caso, se instruyan los correspondientes expedientes, remitiéndose testimonio al Juzgado de Instrucción en funciones de Guardia territorialmente competente, cuando los hechos pudieran ser constitutivos de delito». El texto íntegro de esta sorprendente Circular 6/2009 se puede consultar en *http://www.samuelparra.com/wp-content/uploads/2009/04/circular-6-2009.pdf* [Consulta: 5 de diciembre de 2012].

normalmente de manifiesto por la doctrina o por la práctica. Así, dejando al margen las posibles «mutaciones» constitucionales a las que ya se refirió Jellinek [129], la vía de la interpretación jurisprudencial aparece como una de las más adecuadas para ello. De hecho, para De Vergottini la influencia ejercida por la jurisprudencia en este ámbito es «particularmente importante», especialmente «la de los tribunales cuyo fin principal consiste en comprobar la conformidad de la legislación ordinaria con la Constitución e interpretarla». En estos casos, «para saber cuál es el alcance efectivo de la Constitución es imposible prescindir del conocimiento de las sentencias de los Tribunales», ya que su actividad «ha llevado a continuas adecuaciones a la realidad contemporánea… a veces modificándolas sensiblemente como demuestra la experiencia de EE.UU., de Canadá y de Australia» [130].

A ello se refería concretamente el Magistrado del Tribunal Constitucional español, Jiménez de Parga, cuando en un Voto Particular a la Sentencia del Tribunal Constitucional español 290/2000, de 30 de noviembre, indicaba que «no ha de sorprendernos que en la Constitución Española de 1978 no se tutelase expresamente la libertad informática», ya que «veintidós años atrás la revolución de la técnica en este campo apenas comenzaba y apenas se percibía». Y ello supone un problema ya que «A diferencia de lo que ocurre en otros textos constitucionales (por ejemplo, en los de Portugal o Argentina, siguiendo la senda de la Constitución de Estados Unidos de América) nuestra Ley Fundamental de 1978 no incluye una cláusula abierta, después de haber consignado una amplia lista de derechos y libertades» [131].

[129] Para JELLINEK, la reforma de la Constitución es «la modificación de los textos constitucionales producida por acciones voluntarias e intencionadas», mientras que «por mutación de la Constitución entiendo la modificación que deja indemne su texto sin cambiarlo formalmente que se produce por hechos que no tienen que ir acompañados por la intención, o conciencia, de tal mutación». En G. JELLINEK *Reforma y Mutación de la Constitución*. Madrid, Centro de Estudios Constitucionales, 1991, p. 7.

[130] G. DE VERGOTTINI *Derecho Constitucional Comparado*. Madrid, Espasa-Calpe, 1985, pp. 177-178.

[131] Voto Particular del Magistrado Jiménez de Parga, al que se sumó también el Magistrado Mendizábal Allende, a la STC 290/2000, de 30 de noviembre (Pleno),

No obstante, para Jiménez de Parga, incluso con estas dificultades, es posible configurar un nuevo «derecho de libertad informática», con unos contenidos «mucho más amplios que los que proporciona el art. 18.4 de la Constitución» a través de la consideración que de la dignidad de la persona hace el art. 10.1 de la Constitución española. Así, «nos hallamos… ante unos principios constitucionales (la dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás)» que condicionan toda la interpretación del ordenamiento, a la vez que son directamente aplicables. Con ellos «y el apoyo de determinados derechos expresamente reconocidos en la Constitución de 1978, así como en Textos internacionales, es posible extender la tutela a ciertos derechos de singular relieve e importancia en el actual momento de la historia». Tal es «el derecho fundamental a la libertad informática». Y concluye señalando que «reitero que el reconocimiento y protección de nuevos derechos fundamentales es un cometido importante de la jurisdicción constitucional, la cual, con esta ampliación de su tutela, facilita la permanencia durante largo tiempo de la Constitución» [132].

Junto con la jurisprudencia, también sería posible que estos eventuales nuevos derechos tuvieran acogida en tratados y convenios internacionales que, dadas las características transnacionales de estas nuevas tecnologías de la comunicación y de la información, aparecen como un medio especialmente idóneo. De hecho, la regulación de los nombres de dominios e, incluso,

---

Ponente: González Campos, Recursos de Inconstitucionalidad contra la Ley Orgánica 5/1992 de regulación del tratamiento automatizado de los datos de carácter personal. Boletín Oficial del Estado, núm. 4 (4 de enero de 2001), Suplemento, pp. 70-93 El voto particular, a partir de la página 92. La jurisprudencia completa del Tribunal Constitucional Español, desde el año 1981 hasta la actualidad, también se puede consultar en su página web: http://www.tribunalconstitucional.es/

[132] Ibídem. Un análisis más exhaustivo de los mecanismos de interpretación constitucional en relación a los valores y principios que contempla la Constitución de 1978, puede encontrarse en R. M.ª Orza Linares *Fundamentos de la democracia constitucional: los valores superiores del ordenamiento jurídico*. Granada, Ed. Comares, 2003, en especial en el Cap. III.

la creación de un cierto «gobierno de internet» exige la colaboración internacional [133]. Un ejemplo constante de esta vía puede ser la labor legislativa —a través del derecho originario (los tratados) o del derecho derivado (elaborado por sus propios órganos)— de la Unión Europea.

De hecho, esta evolución la podemos observar en relación con el derecho de acceso a internet y la generalización del servicio universal. Sin embargo, parece claro que hemos observado un serio retroceso en lo que se refiere a la protección del anonimato en las comunicaciones electrónicas. De hecho, aunque la protección del secreto de las comunicaciones telefónicas avanzaba en la línea de proteger incluso los números telefónicos que eran objeto de utilización, lo cierto es que en estos últimos años el retroceso ha sido espectacular. Así, se ha pasado de una creciente garantía no sólo del contenido de la comunicación, sino también de los elementos que la facilitan, a obligar a las compañías prestadoras de servicios a que establezcan los medios técnicos necesarios para que registren, en España durante un año, los datos de todas las comunicaciones «incluso las infructuosas» que realizan todos los ciudadanos sin excepción. Algo esperanzadora es, en esta línea la labor que está desarrollando la Unión Europea en la línea que indica el documento de la Unión Europea conocido como el «Programa de Estocolmo. Una Europa abierta y segura que sirva y proteja al ciudadano» [134]: «Cuando se trata de evaluar la intimidad del individuo en el espacio de libertad, seguridad y justicia, prevalece el derecho a la libertad. El derecho al respeto de la vida privada y el derecho a la protección de los datos personales de los ciudadanos están inscritos en la Carta de los Derechos Fundamentales». Y así «Principios básicos como la limitación en función del objetivo, la proporcionalidad, la legitimidad del tratamiento de datos, los límites del período de almacenamiento, la seguridad y la confidencialidad,

[133] Como ejemplo la Cumbre Mundial de la Sociedad de la Información, celebrada en Ginebra (primera fase-2003) y Tunez (segunda fase-2005). Se puede obtener información sobre las mismas en *http://www.itu.int/wsis/geneva/index-es.html* y en *http://lac.derechos.apc.org/wsis/wsis.shtml* [Consulta: 7 de diciembre de 2012].

[134] Este documento se puede consultar en: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:es:PDF* [Consulta: 25 de septiembre de 2012].

así como el respeto a los derechos individuales, el control por unas autoridades de supervisión nacionales independientes y el acceso a recurso judicial efectivo deben quedar garantizados, y debe establecerse un sistema general de protección».

Al menos sí se ha garantizado legalmente en la mayoría de los países la obligación de mandamiento judicial para la cesión de estos datos a los agentes de los cuerpos y fuerzas de seguridad. Aunque lo cierto es que la mera custodia de esos datos durante prolongados lapsos de tiempo, amplía enormemente las posibilidades de una utilización ilegítima de los mismos.

No se trataría sólo de que la policía tenga acceso a ellos, mediante mandamiento judicial, sino que su existencia puede facilitar el uso —incluso ilegítimo— de tales datos, sobre todo teniendo en cuenta que la evolución acelerada de la tecnología facilita enormemente la gestión de tales datos y la posibilidad de encontrar los datos escogidos de una manera rápida y fácil y sin que los funcionarios con autorización de acceso posean especiales conocimientos informáticos.

Este es el típico caso en el que, con la excusa de la protección de la seguridad pública y la lucha contra el terrorismo, se han justificado la adopción de medidas que, de otra manera, parecerían desproporcionadas y carentes de justificación constitucional.

En todo caso es muy significativo que, como ya hemos citado, hasta la propia Agencia Española de Protección de Datos recomiende que no se utilice el nombre real para todo aquello en lo que no sea necesario o que no se publiquen en los perfiles de las redes sociales excesiva información personal [135]. Y es que, en efecto, podemos coincidir con la Agencia en la necesidad de que, en la medida de lo posible, seamos nosotros mismos los primero que procuremos proteger nuestra privacidad. Este aspecto nos lleva a la necesidad de aumentar la formación y la información de los ciudadanos en estos ámbitos. Y especialmente cuando se trate de menores.

[135] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Recomendaciones para una navegación más privada* , ya citada. Puede consultarse en *http://www.agpd.es/portalwebAGPD/jornadas/dia_internet_ 2012/recomendaciones-ides-idphp.php* [Consulta: 10 de noviembre de 2012].

En el caso de que deseemos borrar los datos propios que aparecen en internet, los problemas son también importantes.

En la práctica sólo podemos utilizar los derechos reconocidos ya hace algunos años en relación con la protección de datos. Esto es, los derechos de acceso, rectificación, cancelación y oposición. Y, en ese sentido, habría que alabar los esfuerzos de la Agencia Española de Protección de Datos para garantizar el «derecho al olvido» a través de una reinterpretación continuada de estos derechos.

Sin embargo, cabría concluir que en la actualidad la confluencia, por un lado, de una demanda creciente de datos personales reales en internet, la continua fuente de datos personales que las publicaciones oficiales se vuelcan en la red y el creciente volumen de información que suministran también a internet los medios de comunicación, hacen que los intentos de los ciudadanos por preservar su vida privada al margen de internet, utilizando estos recursos, resultan infructuosos.

Por ello habría que introducir en la legislación otros instrumentos legales, al margen de la reinterpretación de los derechos de acceso, rectificación, cancelación y oposición, que refuercen la posición del ciudadano que desea preservar su anonimato, incluso en internet. Quizá sea la STC 144/1999 al señalar que «el art. 18.1 [Constitución Española] garantiza… un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos», la que ofrezca un nuevo punto de apoyo para la creación de instrumentos legales que refuercen el control sobre nuestra propia vida y garanticen también en estos ámbitos, en definitiva, nuestra libertad.

Resumen:

En el texto se analizan las consecuencias que el impacto de las nuevas tecnologías de la información y de la comunicación (TIC's) puede suponer para la libertad y la igualdad de los ciudadanos. Así, vamos a estudiar el modo en el que el ordenamiento jurídico responde a esos nuevos retos y se propone, finalmente, la configuración de unos nuevos derechos vinculados a estas tecnologías: el derecho de acceso, que se predica universal y no discriminatorio, el derecho al anonimato, consagrado en el ámbito de las comunicaciones telefónicas, pero muy discutido en el ámbito de internet, y el derecho al olvido como medio para evitar que la divulgación, utilizando las nuevas tecnologías, de informaciones antiguas, erróneas o desactualizadas, puedan afectar a la vida y condicionar la libertad de las personas.

Palabras Clave: *Constitución, Derecho Constitucional, Unión Europea, Derechos fundamentales, Internet, nuevas tecnologías, privacidad, anonimato, derecho de acceso, derecho al olvido, TIC's.*

Abstract:

The following text analyzes the consequences that the impact of new technologies of information and communication technologies (ICT) can suppose for the liberties and equality of citizens. We are going to study the way in which the legal system responds to these new challenges and proposes finally setting some new rights associated with these technologies: the right of access, it should be universal and non-discriminatory, the right to anonymity, respected in the area of telephone communications, but much discussed in the area of internet, and the right to be forgotten as a means to prevent the disclosure, using new technology, old information, incorrect or outdated, may affect life and affect the liberties of the people.

Keywords*: Constitution, Constitutional Law, European Union, Fundamental Rights, Internet, new technologies, privacy, right to anonymity, right to internet access, right to be forgotten, ICT.*