PRIVACIDAD EN LA SOCIEDAD DE LA INFORMACIÓN

José Justo Megías

Abstract: *The Information Society has had a profound effect on the protection of privacy. The Universal Declaration of Human Rights reflects the need to protect the individual's private life and correspondence from arbitrary incursions, but at the time it was impossible to foresee how the New Technologies would affect this subject. Over the years, legislators and the courts have had to broaden these concepts to provide –not without certain difficulties– the required protection. Of particular note is the recognizing of the right to informative self-determination, the basis of which is found in German jurisprudence of the 1980s. Similarly, the double dimension attributed to privacy; the first being the exclusion of third parties from what belongs to and is retained within the sphere of what is intimate (intimacy); the second –dynamic– being the control of personal data by the interested party. In these pages we consider the vulnerability of privacy in the face of technological innovation and the response, generally by the courts, to safeguard the human rights related to it.*

Palabras clave: privacidad, intimidad, secreto de comunicaciones, protección de datos, Sociedad de la Información.

1. Marco general

El desarrollo de las Nuevas Tecnologías ha puesto a nuestro alcance, en el campo de las comunicaciones, posibilidades difíciles de imaginar hace sesenta años, cuando vio la luz la Declaración Universal de Derechos Humanos. Es cierto que muchas de ellas suponen mejoras de la calidad de

vida tanto personal como social, reportando incluso nuevas vías de promoción de la dignidad, pero también han abierto las puertas a nuevas formas de ataque a los derechos personales y a los intereses sociales por quienes se sirven de esos medios para fines ilícitos, ataques difíciles de neutralizar y perseguir dadas las innovadoras características tecnológicas. Uno de los campos más afectados en este sentido es el de la privacidad[1].

Resulta palmaria la distancia entre lo que nos promete el Derecho positivo como garantías y protección de nuestra privacidad –como elemento esencial de nuestro desarrollo personal– y lo que realmente se puede conseguir en la práctica, y es que no sólo las actividades de *hackers* y *crackers* llevan la delantera a cualquier diseño de seguridad por parte de las autoridades o del sector privado, sino que también han crecido las sospechas de atentados "oficiales" contra la vida privada con cierto amparo legal.

La psicosis social desencadenada tras los actos terroristas de Nueva York, Madrid y Londres sirvió a los legisladores de justificación para aprobar ciertas normas cuestionables. En el caso norteamericano, pocas horas después de los atentados de 2001, el FBI comenzó a solicitar a los proveedores de acceso a Internet, servicios web y mensajería electrónica que instalasen el sistema *Carnivore* de espionaje de la Red, llamado también DCS1000, idóneo para intervenir las líneas de comunicación que fluían a

1. He tratado estas cuestiones anteriormente en "Vida privada y nuevas tecnologías", en *RCE*, 17 (2001), pp. 3-27 y "Privacidad e Internet: intimidad, comunicaciones y datos personales", en *Anuario de Derechos Humanos*, 3 (2002), pp. 515-560. La bibliografía sobre este tema es abundantísima, por ello sólo destaco algunas de las obras utilizadas en las que se puede encontrar referencia de numerosos artículos y libros: GARCÍA SAN MIGUEL, L. (ed.), *Estudios sobre el derecho a la intimidad*, Tecnos, Madrid, 1992; PÉREZ LUÑO, A.E., *Manual de Informática y Derecho*, Ariel, Barcelona, 1996; ID., *La tercera generación de derechos humanos*, Thomson-Aranzadi, Cizur Menor, 2006; OLLERO, A., "La ponderación delimitadora de los derechos humanos. Libertad informativa e intimidad personal", en *La Ley*, 4691 (1998), pp. 1-4; FERNÁNDEZ, Mª L., *Nuevas tecnologías, Internet y Derechos Fundamentales*, McGraw-Hill, Madrid, 1998; HERRÁN, A. I., *La violación de la intimidad en la protección de datos personales*, Dykinson, Madrid, 1998; RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones: tecnología e intimidad*, McGraw-Hill, Madrid, 1998; HERRERO TEJEDOR, F., *La intimidad como derecho fundamental*, Colex, Madrid, 1998; ÁLVAREZ-CIENFUEGOS, J. Mª, *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, Pamplona, 1999; REBOLLO DELGADO, L., *El derecho fundamental a la intimidad*, Dykinson, Madrid, 2000; CAMPUZANO TOMÉ, H., *Vida privada y datos personales*, Tecnos, Madrid, 2000; SERRANO, Mª M., *El derecho fundamental a la protección de datos. Derecho español y derecho comparado*, Thomson-Civitas, Madrid, 2003; FERNÁNDEZ RODRÍGUEZ, J. J., *Secreto e intervención de las comunicaciones en Internet*, Thomson-Civitas, Madrid, 2004; MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica a la autodeterminación informativa*, Thomson-Civitas, Madrid, 2005.

través de las redes de los ISPs. La *Foreing Intelligence Surveillance Act* (FISA) limitaba la facultad de intervención de comunicaciones, pero no en el supuesto de acciones criminales[2].

Días más tarde, el Senado aprobaba el proyecto de la *Anti-Terrorism Act*. Concedía al Gobierno un margen mayor en la utilización de la tecnología de vigilancia (intervención de las conexiones a Internet, sistemas de vigilancia de las comunicaciones globales, videocámaras *online*, dispositivos de reconocimiento del rostro y escaneo de las huellas digitales) para combatir el terrorismo. Revisado durante la última semana de septiembre, culminó con su aprobación por el Senado a mediados de octubre como *Provide Appropiate Tools Required to Intercept and Obstruct Terrorism* (PATRIOT) *Act*. Incluía una nueva definición de terrorismo y contemplaba la limitación de algunos derechos fundamentales: posibilidad de intervenir las líneas de teléfono o cualquier otro dispositivo electrónico de comunicación utilizado por persona sospechosa de terrorismo, identificación de remitentes y receptores de mensajes, conducción del tráfico de los usuarios hacia servidores centrales para su control, etc. De poco sirvieron las críticas de la Unión de Libertades Civiles de América sobre la inconstitucionalidad de algunas de sus cláusulas. La norma ampliaba definitivamente el estatuto *pen register* –dispositivo de seguimiento electrónico que se conecta a una línea de teléfono y registra los números marcados– a las comunicaciones electrónicas y a la navegación por Internet, de modo que para los investigadores sería más fácil obtener los datos sobre la actividad en Internet y el registro de información privada sobre direcciones IP. También contemplaba la obligación para los proveedores de servicios de Internet de contribuir en esta intervención, permitiendo a las autoridades capturar información o facilitándola[3]. En febrero de 2002 era enviada al Congreso una nueva propuesta de ley, la *Cyber Security and Enhancement Act*, que contenía el endurecimiento de las penas para los hackers y crackers y obligaba a los ISPs a comunicar a las autoridades la existencia de "riesgos razonables" en el tráfico de comunicaciones, y no sólo los "riesgos graves" recogidos en la *Patriot Act*.

2. Ello permitió a America Online y EarthLink la colaboración con el FBI en la consecución de información privada para esclarecer determinados hechos, aunque se negaron a instalar *Carnivore* por considerarlo innecesario.

3. La Asociación de Internautas (AI) y la Asociación de Usuarios de Internet (AUI) calificaron de *"demencial"* la *USA Patriot Act*, en especial por permitir la reconducción del tráfico de Internet hacia servidores centrales, donde retendrían los mensajes de correo electrónico para su revisión.

La última controversia sobre el respeto de la privacidad en EE.UU. ha derivado de la modificación de la FISA en julio de 2008. Los cambios introducidos, que tienen efectos retroactivos, permiten la interceptación de comunicaciones sin previa autorización judicial. Con esta nueva regulación se impide que puedan prosperar las demandas multimillonarias interpuestas contra las empresas de telecomunicaciones que pusieron sus medios al servicio de las Fuerzas de Seguridad norteamericanas. De poco ha servido la oposición de la Unión Americana de Libertades Civiles (ACLU), que ha considerado dichas modificaciones contrarias a la Constitución[4].

El Reino Unido se sumó desde un principio a este tipo de regulación, con la consiguiente aprobación de normas ciertamente cuestionables[5]. Y poco tiempo después lo haría Alemania. En el año 2006 el Estado de Renania del Norte-Wesfalia había aprobado una ley que autorizaba a la policía a introducirse, a través de Internet, en los ordenadores personales de los internautas sospechosos de terrorismo y analizar el contenido de su disco duro. El 27 de febrero de 2008 se pronunciaba el Tribunal Constitucional sobre su inconstitucionalidad, dejando entrever que sólo sería constitucional tal registro si la ley lo autorizase en casos de "peligro para la vida de las personas o riesgo para el Estado", y previa autorización judicial. En su lectura pública, el Presidente del Alto Tribunal recalcaba que con esta sentencia se impulsaba la eficacia de un "derecho básico de garantía de confidencialidad e integridad de los sistemas técnicos de información". En España se encuentra sometida a la consideración del Tribunal Constitucional la Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*, que permite ciertos controles y seguimientos previos a la autorización judicial.

El interés por evitar posibles abusos siempre ha existido, pero en ocasiones parece que se trata más bien de un interés no muy firme. En el marco comunitario ya se había apreciado con la propuesta a principios de diciembre de 2000 de la *Carta Europea de Derechos Fundamentales* en la Cum-

4. Las modificaciones fueron aprobadas, tras un año de discusión, por el Senado norteamericano a principios de julio de 2008 por 69 representantes, y con tan sólo 28 votos en contra. Con ellas se legitimaban las interceptaciones llevadas a cabo desde el año 2005 sin previa autorización judicial.

5. Ya había aprobado algunas normas para el ámbito laboral provocando ciertas suspicacias, como la *Regulation of Investigatory Powers Act 2000*, que permitía –con ciertos límites– a las empresas controlar el uso del correo electrónico desde los puestos de trabajo.

bre de Niza; reforzaba el estatuto jurídico de los derechos que conforman la vida privada. A ella se uniría más tarde una Directiva del Parlamento Europeo y del Consejo, de 12 de julio de 2002, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas*[6]. Pero los acuerdos concretos adoptados en el seno del Consejo de Justicia y Asuntos de Interior restan efectividad.

Por lo que se refiere a la regulación jurídica en territorio español, el año 2000 fue especialmente significativo. Entró en vigor la Ley Orgánica 15/1999, de 13 de diciembre, de *Protección de Datos de Carácter Personal* (LOPD) y el Tribunal Constitucional dictó dos sentencias de gran trascendencia que afectaban a la citada ley y a la derogada LORTAD. Desde entonces también hemos podido contar con las primeras sentencias del Tribunal Supremo, de los Tribunales Superiores de Justicia y de la Audiencia Nacional relativas a la privacidad y nuevas tecnologías. Más tarde se han elaborado otras normas importantes, como las leyes que sectorialmente vinieron a regular la Sociedad de la Información (LSSICE y LISI), o se han modificado otras, como la *Ley General de Telecomunicaciones* –y el Reglamento que la desarrolla–, que han arrojado luz y claridad sobre las innovaciones aportadas por las Nuevas Tecnologías. Es de destacar, fundamentalmente, la importancia de la LOPD para el reconocimiento y protección del derecho a la "autodeterminación informativa", cumpliendo así con el mandato contenido en el art. 18.4 CE. Este derecho fundamental aporta –a la vertiente negativa, de exclusión, de la intimidad– una vertiente positiva que lo diferencia notablemente de la intimidad (art. 18.1 CE), aunque ambos derechos quedan bajo el paraguas de lo que nuestro Tribunal Constitucional entiende como vida privada. Por su parte, las SSTC 290/2000 y 292/2000, ambas de 30 de noviembre, resolvieron las dudas en torno a ciertas competencias legislativas sobre la cuestión y sobre el contenido esencial de los citados derechos respectivamente. A la intimidad y la autodeterminación informativa habría que añadir el derecho al secreto de las comunicaciones (art. 18.3 CE) y la inviolabilidad del domicilio (art. 18.2 CE)[7] para completar el contenido de la privacidad.

6. Complementa la regulación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.

7. Así viene a entenderlo el Tribunal Constitucional cuando expone que "el reconocimiento explícito en un texto constitucional del derecho a la intimidad es muy reciente y se encuentra en muy pocas Constituciones, entre ellas la española. Pero su idea originaria, que es el respeto

2. Qué debemos entender por vida privada

Una primera dificultad que debemos resolver se centra en la diferenciación entre *privacy* –en ocasiones traducida como privacidad– e intimidad, términos no coincidentes en cuanto a su significación. Fue en una sentencia de 1873 de un tribunal norteamericano cuando se utilizó por primera vez el término *privacy* con una pretensión jurídica. En ella se apoyaron años más tarde los abogados Warren y Brandeis para escribir su artículo *The Right to Privacy*[8], en el que defendieron la existencia de un derecho a preservar la "privacidad" de posibles injerencias no consentidas. Aunque la reivindicación tenía su fundamento, los tribunales pusieron objeciones para reconocer una protección jurídica inexistente hasta el momento del entorno personal. Tras una serie de sentencias titubeantes y contradictorias, la dictada en 1905 por la Corte Suprema de Georgia en el caso *Pavesick v. New England Life Insurance Company* sería decisiva. En ella se reconocía a cualquier persona unos derechos, entendidos como naturales, que debían ser respetados tanto por las autoridades como por los particulares y entre ellos se encontraba el de la "libertad personal", tanto en su vertiente de derecho a la vida pública como del derecho correlativo a la intimidad.

Años más, la Corte Suprema de EE.UU. –con Brandeis entre sus magistrados– consagró, al amparo de la Cuarta Enmienda, el reconocimiento del ámbito personal merecedor de protección jurídica. Aunque esta enmienda –referida a la propiedad privada– trataba de proteger el derecho del ciudadano a la seguridad en su persona, domicilio, documentos y efectos frente a registros, arrestos y embargos sin causa suficiente, también incluía la ilicitud de cualquier orden de registro o arresto que no contuviera una motivación fundada y la descripción del lugar que debía ser registrado o de

de la vida privada, aparece ya en algunas de las libertades tradicionales. La inviolabilidad del domicilio y de la correspondencia, que son algunas de esas libertades tradicionales, tienen como finalidad principal el respeto a un ámbito de vida privada, personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado" (STC 110/1984, de 26 de noviembre, Fundamento Jurídico 3°).

8. Warren, Ch. y Brandeis, L.D., "The Right to Privacy", en *Harvard Law Review*, 4 (1890), pp. 193-200. El origen de este artículo estuvo en el acoso al que fue sometida –por parte de la prensa– la familia Warren, objeto de críticas continuas por su forma de vida. Warren, con buena formación jurídica, acudió a su amigo Brandeis con la pretensión de iniciar un trabajo que justificara la necesidad de proteger jurídicamente aquello que veía atacado en su familia sin causa legítima y limitar así la intrusión en determinadas esferas que debían tener la consideración de privadas.

las personas o cosas sobre las que recaía la orden. La citada Enmienda se utilizó a partir de los años 30 para proteger la intimidad, pero no fue hasta 1965 cuando esta protección adquirió el rango de derecho constitucional, identificado su objeto con la "autonomía para tomar decisiones íntimas", y con la característica más propia de los derechos humanos de la primera generación: la exclusión de terceros de ámbitos que se entienden reservados al titular del derecho. Dado que en Estados Unidos se aprecia aún la preeminencia de la propiedad, no sólo de las cosas materiales, sino también de todo lo que concierne a la persona, no resulta difícil comprender que el ámbito de la intimidad fuera concebido como una esfera en la que sólo cada persona puede decidir si permite o no a los demás participar de su conocimiento, de modo que la facultad principal consiste en algo negativo –excluir–, no en llevar a cabo acciones concretas o en controlar determinados datos[9].

La mentalidad continental europea, por el contrario, no suele reducir los derechos a facultades negativas, de exclusión, sino que prima también su vertiente positiva[10]; en el caso que nos ocupa conllevaría la facultad de controlar los datos personales por parte de cada sujeto, incluso de aquellos que aparentemente no son datos íntimos, pero que podrían dar acceso a nuestra intimidad si fueran tratados siguiendo determinadas pautas. No sólo se pretende limitar su conocimiento, sino poder cambiar datos, anularlos, pedir información sobre aquellos que nos afecten y del uso que se hace de los mismos, etc. En esta dirección apuntó la *Carta Europea de Derechos Fundamentales,* cuyos arts. 7 y 8 tienen por objeto esta cuestión. El primero establece que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y del secreto de sus comunicaciones", lo que representaría la vertiente negativa o de exclusión de la vida privada. En cambio el segundo –más en consonancia con los adelantos tecnológicos– reconoce que "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan", que deben ser tratados "de modo leal,

9. Una de las consecuencias inmediatas de esta mentalidad es el juego de la *exclusionary rule* –también con fundamento en la Cuarta Enmienda– cuando se obtiene una prueba incriminatoria sirviéndose de un atentado a la vida privada, regla que deja al juez cierta discrecionalidad para decidir si es más valiosa la intimidad o el bien jurídico atacado y conocido mediante la acción ilegal.

10. Vid. CARPINTERO, F., *Libertad y Derecho*, Escuela Libre del Derecho, México, 1999, pp. 12-105. No siempre fue así. Mientras que dominó la concepción de la Escuela Kantiana el objetivo del Derecho fue salvaguardar las esferas de libertad de los individuos, quedando reducidas a ámbitos de los que se podía excluir lícitamente a los demás.

para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente"[11].

Lo cierto es que podemos distinguir claramente entre intimidad y vida privada (o privacidad), pues la primera tiene como objeto propiamente excluir a los extraños del conocimiento de nuestros datos íntimos, mientras que la segunda conlleva no sólo el respeto de éstos, sino también su control, así como el secreto de las comunicaciones y de las circunstancias en que se producen, el control de otros datos públicos que dan acceso a la intimidad[12], etc. Además, por su naturaleza, podríamos decir que el secreto de las comunicaciones, o la inviolabilidad del domicilio, o incluso en ocasiones el control de datos, son derechos que están al servicio de la intimidad, pues lo que se pretende con ellos es evitar que se llegue al conocimiento de ésta. El derecho a la intimidad, por tanto, tendría un carácter material, mientras que los otros tendrían un carácter más formal; es decir, para evitar el conocimiento de la intimidad, toda comunicación debe ser secreta, o todo domicilio debe ser inviolable, o todos los datos personales deben permanecer bajo el control de su titular[13], salvo que haya una causa justifi-

11. El contenido de estos dos artículos fue recogido también en el Tratado por el que se establecía una Constitución para Europa (por ejemplo, artículos I-51, II-68, etc.). El hecho de que no fuera aprobada por Francia y Holanda impidió su entrada en vigor y su sustitución por el Tratado de Lisboa, recientemente rechazado por Irlanda. Sobre la relevancia y tratamiento de esta materia en Europa, vid. PÉREZ LUÑO, A.-E., "Internet y derechos humanos", en *La tercera generación de derechos humanos*, cit., pp. 87-128, especialmente pp. 106-114 y ARENAS RAMIRO, M., "El principio del consentimiento en los Estados miembros de la Unión Europea", en *Revista Española de Protección de Datos*, 2 (2007), pp. 159-183.

12. La Exposición de Motivos de la LOPD se hizo eco de esta diferencia al manifestar que "la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado".

13. Ya en 1984 dejaba claro el Tribunal Constitucional que era necesario proteger determinados ámbitos para proteger la intimidad, manifestando que los avances tecnológicos obligaban "a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida" (STC 110/1984, Fundamento Jurídico 3º).

cada para permitir lo contrario. Habría que matizar que el simple hecho de intervenir una comunicación no implica forzosamente que podamos llegar a lo íntimo –dependerá de su contenido–, pero lo que no se puede negar es que constituye un medio idóneo para conseguirlo[14].

Como consecuencia de estas distinciones, también se reivindica una protección diferente, acorde a cada ámbito. La intimidad, donde se sitúa "el ámbito de los pensamientos de cada cual, de la formación de las decisiones, de las dudas que escapan a una clara formulación, de lo reprimido, de lo aún no expresado y que quizás nunca lo será...", debe estar protegida por un "velo de total opacidad que sólo podría ser levantado por el individuo mismo"[15]. En cambio, la privacidad sería un ámbito donde imperan exclusivamente los deseos y preferencias individuales, condición necesaria del ejercicio de la libertad individual, y que podría denominarse "esfera personal reconocida"; sus límites dependerían del contexto cultural y social, de modo que el velo que la cubre debería ser de una transparencia relativa. Estas precisiones nos permiten un análisis o estudio, por separado, de los derechos afectados por las Nuevas Tecnologías en este ámbito, esto es, la intimidad, el secreto de las comunicaciones y la autodeterminación informativa, aunque todos conformen al mismo tiempo lo que entendemos como vida privada[16].

3. El derecho a la intimidad

Al establecer Yepes Stork las notas que definen a la persona, afirmaba que la primera de ellas es la intimidad, como grado máximo de la inmanencia o *apertura hacia dentro* que corresponde a cualquier ser humano[17].

14. Así lo ha vuelto a declarar la STC 70/2002, en el Fundamento Jurídico 9º al estimar que "El concepto de lo secreto tiene carácter formal: 'El concepto de secreto en el art. 18.3 tiene un carácter formal, en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado'".

15. Garzón Valdés, E., "Privacidad y publicidad", en *Doxa*, 21-1 (1998), p. 226.

16. Cfr. Pérez Luño, A.-E., "Biotecnologías e intimidad", en *La tercera generación de derechos humanos*, cit., pp. 129-161, especialmente pp. 129-136.

17. "La intimidad es el grado máximo de la inmanencia, porque no es sólo un lugar donde las cosas quedan guardadas para uno mismo sin que nadie las vea, sino que además es, por así decir, un dentro que crece, del cual brotan realidades inéditas, que no estaban antes: son las cosas que se nos ocurren, planes que ponemos en práctica, invenciones, etc. La intimidad tiene capacidad creativa. Por eso la persona es una intimidad de la que brotan novedades, una

Es la nota que nos permite a cada uno ser nosotros mismos y de ahí su importancia y necesidad de protección, pues en ella entronca el rumbo que le demos a nuestras actuaciones y, en definitiva, a nuestra vida. No se trata solamente de proteger algo interno de las miradas extrañas, sino de permitir que ese algo "interno" guíe sin intromisiones ilegítimas el pleno desarrollo de cada persona de acuerdo con su dignidad. "La característica más importante de la intimidad es que no es estática, sino algo vivo, fuente de cosas nuevas, creadora: siempre está como en ebullición, es un núcleo del que brota el mundo interior. Por ahí se puede ver que ninguna intimidad es igual a otra, porque cada una es algo irrepetible, incomunicable: nadie puede ser el yo que yo soy. La persona es única e irrepetible, porque es un *alguien*; no es sólo un *qué*, sino un *quién*. La persona es la contestación a la pregunta ¿quién eres? Persona significa inmediatamente quién, y quién significa un ser que tiene nombre, que es alguien ante los demás"[18]. Si arrebatáramos la intimidad a una persona, estaríamos atacando directamente su dignidad, lo más vulnerable del ser.

Aunque la persona vive en sociedad, rodeado de otras muchas personas ante las que debe dar cuenta de innumerables actuaciones, sin embargo tiene también la necesidad de volverse hacia su interior y meterse dentro de sí. No solemos adoptar nuestras decisiones de un modo irreflexivo, instintivamente, sino que éstas suelen ser el resultado de un proceso racional interno en el que han intervenido sentimientos, formas de pensar, deseos, anhelos... que normalmente no deseamos revelar a los demás. Es más, en numerosas ocasiones nos comportaríamos de modo distinto si no pudiéramos mantener "retirado" de los demás ese proceso de toma de decisiones. Esta necesidad de la persona de retirarse a un lugar interior discreto es precisamente lo que viene a proteger el derecho a la intimidad y, en definitiva, lo que nos permite desarrollar la personalidad propia que quedará reflejada en nuestro comportamiento externo, porque la intimidad no se agota en la interioridad humana, sino que también condiciona la acción. La sobe-

intimidad creativa, capaz de crecer" y que cuando se muestra al exterior supone una "manifestación de la intimidad". YEPES STORK, R., *Fundamentos de Antropología,* Eunsa, Pamplona, 1996, pp. 76-77.

18. YEPES STORK, R., *Fundamentos de Antropología*, cit., p. 78. Afirma un poco antes que "lo íntimo es tan central al hombre que hay un sentimiento natural que lo protege: la vergüenza o pudor, que es, por así decir, la protección natural de la intimidad, el cubrir u ocultar espontáneamente lo íntimo frente a las miradas extrañas". Cfr. también SPAEMANN, R., *Personas. Acerca de la distinción entre "algo" y "alguien"*, Eunsa, Pamplona, 2000.

ranía del ser humano sobre sus acciones no puede consistir simplemente en no encontrar impedimentos para ejecutarlas, sino que excluye también la mirada ajena durante la decisión, puesto que esa mirada ajena puede condicionarnos en el modo de comportamiento. Como afirma L. García San Miguel, la intimidad sería "el derecho a no ser conocidos, en ciertos aspectos, por los demás. Es un derecho al secreto, a que los demás no sepan lo que somos o lo que hacemos"[19]. E. Garzón llega a dar por válido que el paso desde lo privado hacia lo público pueda estar caracterizado por la hipocresía y la reducción de la verdad, de modo que cuando no nos sea posible evitar la curiosidad ajena y "malsana" de nuestra intimidad se convertiría en lícito actuar de acuerdo con lo "políticamente correcto", aunque no responda exactamente a la verdad de lo que sentimos y pensamos[20]. En definitiva, es un derecho al servicio de la libertad, fundamentalmente, en el desarrollo de la propia personalidad y debe ser, por tanto, uno de los derechos perfectamente delimitados y protegidos por cualquier ordenamiento jurídico. Es tal su importancia que los límites a su protección sólo quedan justificados en la medida que se establecen para salvaguardar la sociedad.

Los textos internacionales no han hecho sino recoger esta necesidad humana, si bien se aprecia en ellos una visión más genérica y abstracta de la vida privada en contraposición a la mayor concreción de la intimidad que encontramos en los textos jurídicos de las legislaciones internas. El art. 12 de la *Declaración Universal de Derechos Humanos* establece que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"[21]. Dado que la *Declaración* era tan sólo eso, una declaración, se

19. García San Miguel, L., "El derecho a la intimidad", en AA.VV., *Diccionario crítico de derechos humanos*. Univ. Internacional de la Rábida, Huelva, 2000, p. 258.

20. Cfr. Garzón Valdés, E., *Privacidad y publicidad*, cit., p. 231. Previamente ha sentado la base de que la revelación de lo íntimo es discrecional por parte de su titular, y "ello explica por qué la revelación voluntaria de nuestra intimidad solemos hacerla sólo en caso de relaciones excepcionales como las que crea el amor o un cierto tipo de amistad que justamente llamamos 'íntima'. En estos casos la revelación suele ser recíproca y es considerada como forma más auténtica de entrega al otro. Está también, desde luego, la transmisión de secretos al confesor, o su versión laica, el psicoanalista" (p. 229).

21. También de 1948, aunque un poco anterior, la *Declaración Americana de los Derechos y Deberes del Hombre*, en su art. 5, establecía que "toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar". Y el *Convenio Europeo para la Protección de los Derechos Humanos* establecía dos años más tarde en su art. 8 que "Toda persona tiene derecho al respeto de su vida privada y familiar, de

hacía preciso establecer mecanismos de garantía que pudieran ofrecer una protección real y efectiva tanto de la intimidad como del resto de derechos humanos que guardan relación con ella; para cumplir tal misión se aprobó en 1966 el *Pacto Internacional de Derechos Civiles y Políticos*, cuyo art. 17 establecía que nadie sería "objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación"; este instrumento contemplaba algunos mecanismos –insuficientes a todas luces– para la salvaguarda de los derechos o reparación por la vulneración de los mismos. La diferencia más destacable entre uno y otro artículo es que en el segundo texto se abren las puertas a las injerencias "legales", es decir, se pone de manifiesto que la intimidad no puede ser entendida como derecho absoluto, sino que es susceptible de límites; pero continúa siendo preceptiva la eliminación de cualquier injerencia arbitraria, haya sido o no objeto de una regulación legal.

Otros textos, de diversos ámbitos de aplicación, vinieron con posterioridad a incidir sobre la importancia –para el desarrollo de la persona– que tiene la protección de la intimidad, como fueron el *Pacto de San José de Costa Rica* de 1970, el Convenio 108 *Para la protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal* de 1981[22], la *Declaración del Parlamento Europeo sobre Derechos y Libertades Fundamentales* de 1989, la *Convención de los Derechos del Niño* de 1990, etc. El más reciente es la ya citada *Carta Europea de Derechos Fundamentales,* aprobada en Niza en diciembre de 2000, que reconoce el derecho al respeto de la vida privada y familiar, de su domicilio y del secreto de sus comunicaciones (art. 7) y el derecho a la protección de los datos de carácter personal (art. 8). La debilidad de estas exigencias proviene no del fundamento que las acompaña –sin duda cuentan con un fundamento fuerte–, sino del tipo de texto en el que se recogen, que se asemejan más a declaraciones de buena voluntad. Lo que sí aportan, sin embargo, es una mayor claridad en torno a la autonomía entre cada uno de estos derechos sin privarlos de una estrecha conexión.

su domicilio y de su correspondencia". Solamente razones de seguridad, bienestar económico, defensa del orden, prevención de infracciones penales, protección de la salud, de la moral o de los derechos y libertades de los demás podrían justificar injerencias en este ámbito de la intimidad.

22. Modificado en junio de 1999, fue uno de los textos internacionales más importantes. España se cuenta entre los primeros Estados que lo ratificaron –junto con Alemania, Noruega, Suecia y Francia–, entrando en vigor en noviembre de 1985.

El paso definitivo para distinguir de forma clara los diversos derechos que conforman la vida privada lo dieron los textos constitucionales, que abandonaban esta expresión para dar cabida de forma expresa a la "intimidad", con la advertencia del peligro que podría derivar de las Nuevas Tecnologías. Así, nuestra Constitución recogió en su art. 18.1 el derecho a la intimidad personal y familiar y en el 18.4 limitó el uso de los medios informáticos cuando con ellos se pudiera lesionar tal derecho. Ese derecho a la intimidad recogido en el art. 18.1, lo definiría el Tribunal Constitucional más tarde como "un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario –según las pautas de nuestra cultura– para mantener una calidad mínima de la vida humana"[23]. Esta fórmula, más o menos general, permite incluir en ese ámbito no sólo los datos, sucesos, acciones, etc., que se produzcan en la intimidad, sino también todo aquello que, aún siendo público y notorio, o bien ha sido difundido más allá del ámbito en que tenía sentido su conocimiento, o bien puede dar acceso a la intimidad al ponerlo en conexión con otros datos[24]. El segundo supuesto se enmarcaría concretamente en lo que se ha denominado "teoría mosaico": un dato conocido públicamente, pero aislado, puede ser inocuo, pero puesto en conexión con otros datos también públicos puede revelar el perfil íntimo de una persona. Las Nuevas Tecnologías permiten la obtención de estos datos, su almacenamiento, su tratamiento, su combinación, etc., hasta indicarnos, por ejemplo, si conviene a un empresario contratar a un determinado trabajador o si a una aseguradora le compensa mantener a determinados asegurados, etc.

Por ello distingue el Derecho entre la facultad de excluir los datos del conocimiento ajeno y la de controlarlos. En el primer caso nos encontraríamos ante el derecho a la intimidad, cuya función es proteger frente a cual-

23. STC 231/1988, Fundamento Jurídico 3º; esta idea ha sido reiterada en las SSTC 179/1991, Fundamento Jurídico 3º, 20/1992, Fundamento Jurídico 3º, 57/1994, Fundamento Jurídico 5º, 143/1994, Fundamento Jurídico 6º, etc.

24. Es difícil obtener una definición de dato íntimo que salve todas las dificultades. Podríamos definirlo como aquél que se produce en la intimidad y que carece de trascendencia para la vida social, de modo que ésta podría continuar su curso sin resentirse a pesar de su ignorancia. Pero esta definición nos sirve a medias solamente, pues con ella tendríamos que valorar en cada caso si algo íntimo repercute o no. Por ejemplo, puede pertenecer a la intimidad el hecho de que una persona sea heroinómana, y que no podamos ir preguntándole a los demás si son drogadictos. Pero ¿qué pasaría si esa persona es anestesista y puede contagiar una enfermedad como la hepatitis a los pacientes que entran en quirófano? Pues que entrar a conocer ese dato no supondría una violación de la intimidad, ni tampoco lo sería informar sobre ello si se hubieran producido los contagios.

quier invasión que pueda realizarse "en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad"[25]. El segundo, por el que podemos proteger nuestros datos, nos garantiza "un poder de control sobre los datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado"[26].

4. El derecho a la autodeterminación informativa

Este derecho, recogido en el art. 18.4 de la Constitución, había sido desarrollado por la LORTAD y ampliamente perfilado por la STC 254/1993, de 20 de julio[27]. Las SSTC 290/2000 y 292/2000, de 30 de noviembre, que resolvieron los recursos presentados contra la LORTAD y la LOPD supusieron un paso definitivo en su consolidación detallada, y se ha establecido un marco más acorde a los nuevos avances tecnológicos con la aprobación de la *Ley sobre la Sociedad de la Información y el Comercio Electrónico* y la *Ley de Impulso de la Sociedad de la Información*.

Aunque la generalidad de la doctrina, incluido el Tribunal Constitucional, fundamenta este derecho –también llamado derecho de libertad informática– en el art. 18.4 CE, no falta quien prefiere recurrir a otra fundamentación del mismo, como ocurre con M. Jiménez de Parga, que en su voto particular a la Sentencia 290/2000 negaba su contemplación expresa en el texto constitucional y defendía su vertebración partiendo del art. 10.1 y su configuración a partir de los arts. 18.1 y 20.1 CE[28].

La Sentencia 290/2000 resolvía en realidad una cuestión de competencias, pero dejó fuera de dudas el ámbito de aplicación definitivo de

25. STC 144/1999, de 22 de julio, Fundamento Jurídico 8°.

26. STC 292/2000, de 30 de noviembre, Fundamento Jurídico 6°.

27. Cuya doctrina ha sido reiterada con posterioridad, entre otras, en las SSTC 143/1994, de 9 de mayo (que se pronunciaba sobre el uso del NIF), 11/1998, de 13 de enero, y 94/1998, de 4 de mayo (ambas sobre datos de afiliación sindical), 202/1999, de 8 de noviembre (sobre datos médicos), etc. Sobre la acumulación de datos médicos, vid. Romero, Mª J., "A propósito de la creación por parte de una entidad bancaria de una base de datos relativa a las bajas médicas de sus trabajadores", en *Revista de Derecho Social*, 10 (2000), pp. 123-130; Rodríguez, S., "La intimidad del trabajador en el uso de diagnósticos médicos informatizados", en *Revista Española de Derecho del Trabajo*, 101 (2000), pp. 287-299.

28. Afirma que "los cimientos constitucionales para levantar sobre ellos el derecho de libertad informática son más amplios que los que proporciona el art. 18.4 CE". Voto particular, apartado 4.

la LOPD. Efectivamente, la Sentencia resolvía los recursos interpuestos contra la LORTAD en el año 1993, cuyos argumentos fueron discutidos y debatidos junto a los de la Abogacía del Estado y el Ministerio Fiscal hasta julio de 1998. Con la aprobación y entrada en vigor de la LOPD y la derogación expresa de la LORTAD, los únicos recursos que mantuvieron una razón de subsistencia fueron los presentados por el Consejo Ejecutivo de la Generalidad de Cataluña y por el Parlamento de Cataluña, pues el problema planteado en sus recursos seguía siendo el mismo[29], esto es, si el Estado tenía competencias para atribuir a la Agencia Española de Protección de Datos y al Registro General de Datos Personales –como órgano integrado de aquella– las funciones que le otorgaba sobre ficheros de titularidad privada en todo el territorio nacional. La respuesta del Tribunal fue contundente al respecto: tanto la LORTAD antes, como ahora la LOPD, tienen como objeto la protección eficaz de un derecho fundamental –común en todo el territorio nacional–, no el establecimiento de una simple regulación del uso de la informática, donde sí podrían tener consideración las cuestiones competenciales[30]. Dado que se trata de asegurar la igualdad de todos los españoles en el disfrute de los derechos fundamentales, "es claro que las funciones y potestades de este órgano [la Agencia de Protección de Datos] han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados conteniendo datos de carácter personal y sean quienes sean los responsables de tales ficheros"[31]. Por su parte, la Sentencia 292/2000 –como decía más arriba– tiene especial

29. En su Fundamento Jurídico 4º establece esta sentencia que "la regla general en este supuesto es que cuando la controversia competencial se ha planteado ante este Tribunal por el cauce del recurso de inconstitucionalidad o el conflicto de competencias y tal controversia pervive tras la derogación de la ley que ha suscitado el conflicto, es procedente que nos pronunciemos sobre el mismo".

30. Es rotundo en su Fundamento Jurídico 11º al afirmar que "si se considera la actividad aquí examinada como meramente instrumental o accesoria de otras materias competenciales, es claro que con este planteamiento se está desvirtuando cuál es el bien jurídico constitucionalmente relevante, que no es otro que la protección de los datos de carácter personal frente a un tratamiento informático que pueda lesionar ciertos derechos fundamentales de los ciudadanos o afectar al pleno ejercicio de sus derechos... El objeto de la Ley cuyos preceptos se han impugnado no es el uso de la informática, sino la protección de los datos personales. De suerte que esta protección mal puede estar al servicio de otros fines que los constitucionales en relación con la salvaguardia de los derechos fundamentales, ni tampoco puede ser medio o instrumento de actividad alguna".

31. STC 290/2000, Fundamento Jurídico 14º. Sin embargo, no hay inconveniente en que las Comunidades Autónomas tengan sus propias APD.

importancia, pues no sólo reitera la doctrina del Tribunal Constitucional sobre el derecho a la autodeterminación informativa, sino que también declara nulos determinados incisos de la LOPD, reforzando de este modo la importancia que ya se venía concediendo a este derecho fundamental.

Sobre la concreción positiva de este derecho, habría que decir que fue el Tribunal Constitucional alemán el primero en establecer unas directrices claras al enjuiciar la Ley del Censo alemana de 1983, pues vislumbró que tan importante era reconocer unas esferas personales dignas de protección y reservadas frente al conocimiento ajeno, como reconocer las facultades de control de tales zonas y de los datos que se generaran en ellas. Quedaba configurado así un derecho que otorgaba a cada persona el control sobre la información que pudiera obtener el poder público o las personas privadas y el uso que pudieran hacer de ella[32]. Nuestro Alto Tribunal tardó unos años más, pero llegado el momento admitió que "la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada *libertad informática* es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos..."[33]. La STC 292/2000 dio por admitida esta doctrina de forma unánime en sus Fundamentos Jurídicos 4º y 5º, de modo que no se cuestionaba otra posibilidad.

Afortunadamente, tanto el legislador comunitario como nuestro legislador nacional han realizado un notable esfuerzo por conseguir una legislación de desarrollo de este derecho fundamental, aunque el resultado no haya sido todo lo idóneo que se esperaba. En el ámbito comunitario contamos con tres Directivas importantes. La primera Directiva de trascendencia fue la 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que

32. RODRÍGUEZ, B., *El secreto de las comunicaciones...*, cit., pp. 14-15. Considera que este derecho es inseparable de la intimidad; sería, efectivamente, como la otra cara de la moneda, distinto, pero inseparable de la faceta negativa o excluyente (cfr. pp. 15-17). Vid. una opinión crítica sobre la argumentación del Tribunal Constitucional alemán, por su complejidad, en PÉREZ LUÑO, A.-E., "Biotecnologías e intimidad", en *La tercera generación de derechos humanos*, cit., pp. 130-132.

33. STC 254/1993, de 20 de julio, Fundamento Jurídico 7º. En el Fundamento Jurídico anterior declara que el art. 18.4 establece un derecho fundamental claro, "el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática', lo que se ha dado en llamar *libertad informática*".

respecta al tratamiento de los datos personales y a su libre circulación. La segunda es de julio de 2002 (2002/58/CE), relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. La última, es la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo, relativa a la conservación de datos generados o tratados en relación con la prestación de servicios de comunicación electrónica[34]. En el ámbito nacional tendríamos que destacar, naturalmente, la LO 15/1999, de 13 de diciembre, de *Protección de Datos de Carácter Personal* y algunos artículos de la Ley 32/2003, de 3 de noviembre, *General de Telecomunicaciones* y la Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones* (hoy recurrida ante el Tribunal Constitucional). Entre las normas de rango inferior, muy numerosas, tiene especial relevancia el RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.

El objeto de este derecho, como tiene declarado el Tribunal Constitucional, es más amplio que el objeto del derecho a la intimidad, pues incluiría también la protección de los datos relativos al honor y al pleno ejercicio de los derechos de la persona, es decir, aquellos datos que sean relevantes para el ejercicio de cualquier derecho relacionado con el honor, la ideología, la intimidad personal o familiar, o a cualquier otro bien constitucionalmente amparado[35]. Además, como he advertido anteriormente, podríamos afirmar que su objetivo tiene un cierto carácter formal, pues trata de evitar que un extraño consiga llegar hasta lo que propiamente constituye la intimidad de la persona mediante el tratamiento de datos que han podido ser obtenidos lícitamente[36]. Por ello, fue normal la preocupación que suscitó en ciertos círculos norteamericanos el lanzamiento de Passport por parte de Microsoft

34. Sobre su posible nulidad, vid. GUERRERO PICÓ, M. C., "Operadores privados y seguridad pública: la retención de los datos de tráfico a la luz de la sentencia PNR", en *Revista Española de Protección de Datos*, 2 (2007), pp. 185-215.

35. STC 292/2000, Fundamento Jurídico 6º. En concreto, "los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo".

36. Se aprecia una diferenciación entre simples datos personales (nombre, dirección, etc.) y datos personales sensibles, referidos éstos últimos al origen racial o étnico, ideología, creencias religiosas o filosóficas, afiliación sindical, salud o vida sexual. Los segundos tienen un nivel mayor de protección, necesitándose para su tratamiento un consentimiento explícito del interesado o una causa estricta contemplada en la legislación.

hace años. El Electronic Privacy Information Center y otras organizaciones pro defensa de la privacidad presentaron el 26 de julio de 2001 una demanda formal ante la Comisión Federal de Comercio (FTC) alegando que el sistema de autenticación Passport de Microsoft, incluido en Windows XP, violaba las leyes federales de privacidad, pues obligaba a los usuarios a almacenar sus datos personales en una base de datos de la compañía. Este sistema, que recogía información personal de los consumidores –como las contraseñas e información de las tarjetas de crédito– y las almacenaba en una base para que el usuario no tuviera que reescribirlas continuamente al realizar sus compras por Internet –se introducía automáticamente–, suponía una gran comodidad para los usuarios, pero al concentrar toda la información personal de cada usuario dejaba abierta una puerta al tratamiento abusivo de los mismos, lo que suponía para los defensores de la privacidad una causa de alarma[37]. Microsoft acudió a Washington a petición del Center for Democracy & Technology, grupo que defiende los intereses de los consumidores, para discutir los detalles técnicos de Passport y rebatir todas estas acusaciones.

Se ha dado un gran paso en las garantías de la privacidad en la Sociedad de la Información con el reconocimiento de la dirección IP como dato de carácter personal. La dirección IP o serie de números que identifica un ordenador tiene hoy día la consideración indiscutible de dato de carácter personal porque puede revelar (no siempre) la identidad del usuario y la actividad que se desarrolla desde un ordenador. Así lo reiteró en el Parlamento Europeo (enero de 2008) Peter Scharr, Director de la Oficina de Protección de Datos alemana y presidente del Grupo de la UE que analiza los procedimientos de buscadores y titulares de otros servicios que pretenden servirse de esta información para remitir publicidad. Aunque en España ya había sido considerada con tal carácter por el Informe 327/2003 de la Agencia Española de Protección de Datos, la entrada en vigor del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD supone desterrar toda duda al respecto. Todos los ficheros en los que queden recopiladas estas direcciones, las direcciones de

37. Microsoft utilizaba este sistema en MSN Messenger y en los servicios de correo electrónico de Hotmail, en el acceso *online* a Microsoft Developer Network y en las adquisiciones de libros electrónicos para Microsoft Reader, entre otros productos y servicios. Además, Passport también era el sistema de autenticación para HailStorm, un conjunto de servicios web que permitiría a los suscriptores acceder a sus mensajes, listas de contactos, compras y otros servicios, tales como banca o entretenimiento.

e-mail o los nombres de personas asociados a ellas –con independencia del sistema utilizado– deberán ser comunicados a la Agencia, y su tratamiento deberá contar con el consentimiento de los afectados[38].

Para evitar que pueda resultar afectada la intimidad, las normas coinciden en establecer una serie de principios que deben regir bien en el momento de recoger los datos, bien en el momento de su tratamiento. La recolección de datos personales debe estar presidida por los principios de *justificación legal y social* (motivo lícito para llevarla a cabo), de *licitud y limitación* (a través de medios lícitos –legales y consentidos– y sólo aquellos datos necesarios para cumplir con el fin que se persigue), de *fidelidad a la información* (deben ser datos completos, exactos y actuales, con posibilidad de ser rectificados cuando falte alguna de estas características) y de *pertinencia y finalidad* (sólo se deben conservar para la finalidad perseguida lícitamente). Por lo que respecta a los principios que deben regir el tratamiento y procesamiento de los datos ya recogidos, encontramos el de *confidencialidad de los datos recogidos* (incluye a la entidad y a sus trabajadores), el de *seguridad* (el responsable de los archivos debe disponer las medidas para preservarlos del conocimiento ajeno), el de *caducidad* (deben mantenerse solamente hasta que se alcance el fin perseguido, procediéndose a la cancelación inmediatamente después) y el de *autonomía de la voluntad* (cualquier tratamiento debe ser previamente consentido por el titular de los datos). Todos estos principios han informado las Directivas citadas y las normas nacionales, pero en un principio incurrían en el error de proteger fundamentalmente frente a los abusos por parte del sector público y pasaban de puntillas por el ámbito del sector privado. Las últimas modificaciones de las normas reguladoras han introducido mecanismos para hacerlos efectivos en todo momento tanto frente a la administración pública como frente a cualquier particular.

Hemos hecho notar anteriormente que las facultades que nos otorga el derecho de intimidad son negativas, de exclusión de la mirada extraña, comprendiendo aquellos datos que siendo públicos rebasan su ámbito de conocimiento propio o aquellos que puestos en relación con otros revelan

38. Los Proveedores de Acceso a Internet tienen identificados a sus abonados, tanto si su dirección es estática como dinámica, pero tanto su dirección IP como los datos asociados (conexión, fecha, duración, etc.) tienen la consideración de dato de carácter personal y protegidos, por tanto, por las garantías establecidas legalmente. Sólo caben las excepciones establecidas por la ley o cuando los datos sean, por alguna razón, públicos, en cuyo caso quedaría excluido el tratamiento no consentido.

la intimidad. En cambio lo propio del derecho a la autodeterminación informativa es que nos otorga facultades positivas, de acciones concretas, erigiéndonos en señores de la información personal que generamos. Si en la realidad no podemos hacer uso de esas facultades, nuestro derecho será teórico, pero no un derecho real. Estas facultades se podrían resumir en: consentir la recogida –la obtención y el acceso a los datos personales–, consentir su posterior almacenamiento y tratamiento, consentir su uso o usos posibles por un tercero, saber en todo momento quién dispone de esos datos y qué usos hace de ellos, y, por último, la de denegar esa posesión y uso[39]. Es decir, la libertad informática atribuye un "haz de facultades" por las que el sujeto de derecho puede imponer a terceros la realización u omisión de determinados comportamientos relacionados con el uso de la informática que le afectan a él personalmente[40].

¿Por qué el Tribunal Constitucional declaró inconstitucionales y anuló determinados incisos de la LOPD? Precisamente por no haber establecido unas garantías precisas y eficaces de estas facultades, que podían quedar convertidas en facultades teóricas –pero no reales– y convertir el derecho a la autodeterminación informativa en un derecho impracticable. En concreto, los arts. 21 y 24 abrían las puertas a cesiones de datos sin previa información (y preceptiva autorización) a través de normas reglamentarias, lo que suponía una restricción del derecho contraria a Derecho, que exige una norma de rango legal: en el caso del "derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad

39. STC 292/2000, Fundamento Jurídico 7º. Lo realmente importante será conseguir un control efectivo sobre los datos personales y la información personal que generamos, no sólo para evitar la consecución de perfiles que puedan interesar desde un punto de vista comercial, sino para evitar cualquier retrato de la intimidad de una persona.

40. Un ejemplo reciente, fuera de España, que nos puede servir para poner de manifiesto la facilidad con la que se vulneran estas facultades se produjo en Italia en mayo de 2008. La Agencia Tributaria italiana colgó durante unas horas en Internet los datos de todas las declaraciones correspondientes al año 2005. La Autoridad Garante de la Protección de Datos Personales requirió horas después su retirada por vulnerar la ley de protección de datos personales; al día siguiente prohibió definitivamente su publicación. Fuentes del Gobierno comunicaron que se trataba de favorecer la democracia y la transparencia. La Autoridad Garante reconoció que la ley permitía a la Agencia Tributaria elaborar esas listas, pero no elegir los modos de publicación (sin filtros ni protección). Codacons, asociación de consumidores, interpuso demanda contra el ex-Secretario de Estado de Economía (responsable de la decisión) por la que solicitaba una indemnización de 20.000 millones de euros (520 por cada contribuyente afectado).

de la Administración Pública. Ni es suficiente que la ley apodere a ésta para que precise en cada caso sus límites". Es el legislador y sólo él quien debe determinar cuándo concurre un bien o un derecho que justifique una restricción, en qué circunstancias cabe la limitación y qué reglas precisas deben seguirse, de modo que el afectado pueda prever las consecuencias. Y ello requiere también desterrar las expresiones "interés público" o "intereses de terceros más dignos de protección" por constituir fórmulas abiertas y ambiguas que pueden suponer una restricción arbitraria del derecho en cuestión por parte de las administraciones públicas.

Junto a lo anterior, uno de los mayores problemas que se nos plantea viene derivado de la internacionalidad de la red. Aunque un país establezca una regulación protectora, puede ocurrir que los datos salgan de su ámbito territorial de protección a otro país que carece de una protección similar. La Unión Europea, consciente de este problema ante el avance de las comunicaciones electrónicas, propuso en agosto de 2000 el texto de una Directiva que contemplaba también el tratamiento de los datos personales y la protección de la intimidad en este tipo de comunicaciones[41]. El 28 de enero de 2002 se aprobó la Posición Común nº 26/2002 sobre esta nueva Directiva, con la aprobación por el Consejo de un buen número de enmiendas realizadas por el Parlamento Europeo; la Directiva fue aprobada definitivamente unos meses más tarde. Este nuevo texto, junto a las Directivas 95/46/CE y 97/66/CE, establecerá el marco jurídico de cesión de datos personales a terceros países siempre que se garantice una "protección adecuada". No obstante, las asociaciones de usuarios han vuelto a denunciar en mayo de 2008 que los últimos convenios establecidos entre la Unión Europea y terceros países sobre esta materia no respetan íntegramente el contenido del Derecho comunitario[42].

La trascendencia de este derecho fundamental se puso de manifiesto, por ejemplo, con el aumento de los mensajes electrónicos no solicitados

41. En el quinto considerando reconoce que "el éxito del desarrollo transfronterizo de estos servicios (se refiere a las comunicaciones electrónicas) depende en gran parte de la confianza de los usuarios en que no se pondrá en peligro su intimidad", para añadir en el sexto que "los servicios de comunicaciones electrónicas disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad". Sus veinte artículos tienen como objetivo que puedan seguir desarrollándose las comunicaciones electrónicas, pero sin que ello suponga abrir las puertas a los posibles abusos en el tratamiento de datos tanto por los prestadores del servicio como por las autoridades.

42. Vid. sobre esta cuestión, por ejemplo, el Informe Jurídico 0391/2007 de la Agencia Española de Protección de Datos sobre *Cribado de correo electrónico*.

(*spam*), que destaparon el tráfico de datos existente sin que los usuarios tuvieran conocimiento[43]. Estas conductas, cada vez más extendidas, son constitutivas de verdaderos atentados difíciles de evitar y su fin más común suele ser la venta a otras compañías de los datos de clientes propios o de personas ajenas que han utilizado determinados servicios. Uno de los casos más relevantes en este terreno fue el de Toysmart.com, que pretendió vender las bases de datos de sus clientes antes de proceder a su cierre[44]. En Europa –como hemos visto– la protección jurídica es mayor, aunque el problema es que muchos europeos contratan directamente con empresas norteamericanas o de otros países, que no resultan obligadas jurídicamente al respeto de las garantías europeas.

Entre los medios utilizados para conseguir datos personales destaca la implantación de *cookies* en el disco duro del usuario, de modo que, cada vez que comienza una sesión de navegación en Internet, estará enviando información hacia algún lugar sin que tenga conocimiento de ello. Algunos países han decidido regular restrictivamente estas prácticas, como Francia, que modificó su legislación para autorizar las *cookies* únicamente si el usuario había "recibido previamente una información clara y completa sobre las finalidades del tratamiento y los medios de los que dispone para oponerse a el"[45]. Los organismos comunitarios no pudieron llegar a un acuerdo unánime sobre su regulación, pues algunos Estados miembros se encontraron con la presión del sector publicitario y al final se optó por dejar un margen de libertad en la regulación nacional[46].

43. Vid., por ejemplo, los dictámenes del Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE, en particular el Dictamen 2/2006 sobre el Respeto de la Privacidad en relación con la prestación de servicios de cribado de correo electrónico.

44. Tras un largo proceso, un juez federal de EE.UU. lo evitó a principios de 2001 ordenando la destrucción de la lista. Dos meses más tarde el Senado estadounidense aprobaba una ley, por 83 votos a favor y 15 en contra, prohibiendo a las compañías vender o alquilar los datos de clientes cuando para su obtención se habían comprometido a no hacerlo.

45. Sin embargo, contempla la legalidad del uso de estos ficheros siempre que sean empleados exclusivamente para facilitar las comunicaciones, prohibiendo además que el acceso a un sitio quede condicionado a la aceptación por parte del internauta de que sus datos sean almacenados en su ordenador para otros fines que no sean los autorizados.

46. J. A. Ureña propone, como única solución a los problemas de injerencia en la intimidad que suponen las cookies, la combinación de medidas de protección basadas en autoprotección, códigos de conducta y acuerdos internacionales. A pesar de que coincido con este planteamiento, entiendo que ni aún así quedaría garantizada de forma efectiva la intimidad. Vid. URE-ÑA, J. A., "Internet y la protección de datos personales", en *Internet y Derecho.* Monografías de la Revista Aragonesa de Administración Pública IV. Gobierno de Aragón, Zaragoza, 2001, pp. 128-141.

En cuanto a los seguimientos y obtención de datos por parte de las Fuerzas de Seguridad del Estado, es preciso hacer notar que debe existir un equilibrio entre los derechos individuales y los intereses generales, y para ello es necesario que los datos sean obtenidos y procesados legítimamente (legalidad y justicia), con fines específicos previamente establecidos (legalidad) y asegurando la proporcionalidad entre medios utilizados (lo que podemos perder en el camino) y los objetivos que pretendemos alcanzar. No podemos ignorar que para perseguir a "posibles terroristas" se procesan datos (viajes, finanzas, telecomunicaciones, etc.) que afectan a otras muchas personas inocentes; si se permitiera que el control y seguimiento fuera previo a cualquier control judicial que pudiera velar por la legitimidad, nuestra vida privada sería una quimera.

5. El derecho al secreto de las comunicaciones

Tuvo un reconocimiento en los textos constitucionales muy anterior al derecho a la intimidad, quedando recogido en España por primera vez en los arts. 7 y 8 de la Constitución de 1869, y reconocido de nuevo en las de 1876 (art. 7) y 1931 (art. 32). Nuestra Constitución establece en su art. 18.3 textualmente que "se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial". Aunque tan sólo recoge las más comunes, la expresión "en especial" supone que pueda quedar protegida cualquier tipo de comunicación realizada a distancia, por lo que no se puede albergar dudas sobre si la comunicación electrónica queda amparada o no: "se limita a actuar como fórmula de apertura de cara al desarrollo futuro de nuevas formas de comunicación a distancia por canal cerrado"[47]. La STC 70/2002, de 3 de abril, tuvo que realizar una llamada de atención al legislador al afirmar en su noveno Fundamento Jurídico que "Ciertamente los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto de protección del derecho fundamental, que extienda la protección a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del art. 18.3 CE". No entró en más profundidades,

47. Rodríguez, B., *El secreto de las comunicaciones...*, cit., p. 67.

pero al menos dio a entender que no era ajeno a los avances en este terreno.

El derecho al secreto de las comunicaciones, al igual que el derecho al control de nuestros datos, se caracteriza por ser al mismo tiempo un derecho *autónomo* del derecho a la intimidad e *inseparable* de ésta[48], pues lo que se pretende salvaguardar es precisamente tanto la intimidad en las comunicaciones privadas –aquí radica la autonomía– como el acceso al resto de la intimidad a través de la interceptación de las comunicaciones, sean orales o escritas. A diferencia de la intimidad, ha sido entendido mayoritariamente como un derecho de carácter formal, es decir, que siempre que se produce una injerencia sin la correspondiente autorización judicial, se consuma un atentado contra este derecho. Sin embargo, el Tribunal Constitucional no lo ha entendido así, pues su modo de enjuiciar las demandas de amparo consiste en constatar primero si se ha producido una injerencia y, en caso afirmativo, valorar si tiene algún tipo de justificación, aunque se haya producido sin la preceptiva resolución judicial[49]; combina, pues, el carácter formal y el material para realizar un juicio de valor[50]. Con

48. Esta idea es repetida constantemente a lo largo de la obra de RODRÍGUEZ, B., *El secreto de las comunicaciones...*, cit., pp. 1, 4, 14, 20-21, 24, etc. Considera que la intimidad constituye un derecho más flexible en cuanto a su contenido (puede proteger también las conversaciones y comunicaciones privadas), por ello, cuando alguna de sus zonas de protección pueden ser bien definidas, como ocurre con las comunicaciones, "dichas zonas deben ser reconocidas como derechos independientes" (p. 4).

49. En sentido contrario a este modo de proceder se pronuncia J. Jiménez Campos, que entiende que la intimidad tiene siempre un contenido material, mientras que el secreto de las comunicaciones es rigurosamente formal, pues "toda comunicación es, para la norma fundamental, secreta; aunque sólo algunas, como es obvio, serán íntimas". JIMÉNEZ CAMPOS, J., "La garantía constitucional del secreto de las comunicaciones", en *Revista Española de Derecho Constitucional*, 20 (1987), p. 41.

50. Así, podemos leer en la STC 70/2002, de 3 de abril, Fundamento Jurídico 9º que "Esta doctrina –establecida ciertamente en otro ámbito diferente, pero conexo– resulta aplicable también a los supuestos que nos ocupan. La regla general es que el ámbito de lo íntimo sigue preservado en el momento de la detención y que sólo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial motivada conforme a criterios de proporcionalidad. De no existir ésta, los efectos intervenidos que puedan pertenecer al ámbito de lo íntimo han de ponerse a disposición judicial, para que sea el juez quien los examine. Esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad"; y más adelante: "La valoración de la urgencia y necesidad de la intervención policial ha de realizarse *ex ante*, y es susceptible de control judi-

ello se sitúa en una posición intermedia entre la mantenida por el Tribunal Constitucional alemán, más abierto a las limitaciones del derecho, y la que defiende el Tribunal Europeo de Derechos Humanos, que admite como única justificación de la injerencia el cumplimiento de todos los requisitos establecidos legalmente para llevarla a cabo[51]. La suspensión del derecho está contemplada por el art. 55 CE para los casos de estado de excepción o sitio y en la persecución de las actividades de bandas armadas y terroristas, en cuyo caso podría hablarse más de una restricción especial que de una suspensión, pues la CE es más permisiva en este caso si se rebasaran los límites legales. La razón de esta mayor permisibilidad es que se pretende evitar un daño a la sociedad –mediante el ataque de sus valores y principios constitucionales– causado por uno o varios ciudadanos con el ejercicio abusivo de un derecho fundamental, como es el secreto de las comunicaciones en este caso.

Por otro lado, es preciso resaltar que el secreto de las comunicaciones no afecta solamente al contenido de las mismas, sino a determinados datos relacionados con las comunicaciones que nos podrían revelar información relevante de la vida privada de los comunicantes. Así lo han puesto de manifiesto todos los tribunales. Baste citar la Sentencia del Tribunal Constitucional 230/2007, de 5 de noviembre, que recoge la doctrina reiterada en otras anteriores. En su Fundamento Jurídico segundo afirma que "el bien constitucionalmente protegido es así –a través de la imposición a todos del 'secreto'– la libertad de las comunicaciones, por lo que dicho derecho puede resultar vulnerado tanto por la interceptación en sentido estricto –que

cial *ex post*, al igual que el respeto del principio de proporcionalidad. La constatación *ex post* de la falta del presupuesto habilitante o del respeto al principio de proporcionalidad implicaría la vulneración del derecho fundamental y tendría efectos procesales en cuanto a la ilicitud de la prueba en su caso obtenida, por haberlo sido con vulneración de derechos fundamentales".

51. Cfr. RODRÍGUEZ, B., *El secreto de las comunicaciones...*, cit., pp. 55-62. Habría que decir, a favor de nuestro Tribunal Constitucional, que no se conforma con que exista una resolución judicial puramente formal, sino que le exige a ésta la superación de un *juicio de razonabilidad*, lo que "significa, ante todo, que la limitación debe perseguir un *fin legítimo y constitucionalmente protegido*; debe ser, además, necesaria o, mejor, *indispensable* para alcanzar ese fin, de forma que sólo es legítima imponerla cuando se justifique que no existen medios alternativos, menos lesivos para el disfrute de los derechos fundamentales, de llegar a él; y, por último, la envergadura de la limitación debe ser *proporcional* a la importancia de la finalidad que persigue" (SSTC 7/1994, de 17 de enero, Fundamento Jurídico 3º, 57/1994, de 28 de febrero, Fundamento Jurídico 6º, 49/1996, de 26 de marzo, Fundamento Jurídico 3º, 54/1996, de 26 de marzo, Fundamento Jurídico 7º. En el mismo sentido y más recientes, cfr. SSTC 299/2000, de 11 de noviembre, y 17/2001, de 29 de enero).

suponga aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación, de otra forma, del proceso de comunicación– como por el simple conocimiento antijurídico de lo comunicado –apertura de la correspondencia ajena guardada por su destinatario, por ejemplo–. Igualmente se ha destacado que el concepto de secreto de la comunicación cubre no sólo el contenido de la comunicación, sino también la identidad subjetiva de los interlocutores, de ahí que se haya afirmado que la entrega de los listados de llamadas telefónicas por las compañías telefónicas a la policía, sin consentimiento del titular del teléfono, requiere resolución judicial, toda vez que el acceso y registro de los datos que figuran en dichos listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones".

6. Supuestos más frecuentes de atentados contra la privacidad

Son numerosas las modalidades de vulneración de la privacidad que facilitan las Nuevas Tecnologías. Sólo destacaré, por su importancia, las más frecuentes en el ámbito laboral, en el que se han cuestionado determinadas prácticas por parte de la empresa respecto de los derechos de los trabajadores y, de un modo más genérico, respecto de la libertad de información sindical. Terminaré aludiendo a vulneraciones de carácter más general.

6.1. *Los riesgos para los empleados en el ámbito laboral*

Uno de los supuestos más repetidos en los últimos años es la injerencia por parte del empresario, público o privado, en la privacidad de los empleados, derivada del control tanto del ordenador que la empresa pone a disposición de éstos para desempeñar sus tareas, como del uso de Internet que los trabajadores puedan realizar desde su puesto de trabajo[52]. A ello se

52. Vid. Vicente, F. de, *El derecho del trabajador al respeto a su intimidad*, Consejo Económico y Social, Madrid, 2000; García, J. y Val, A.L. de, "Incidencia de las nuevas tecnologías en las relaciones laborales", en *Internet y Derecho*. Monografías de la Revista Aragonesa de Administración Pública IV. Gobierno de Aragón, Zaragoza, 2001; Luján, J., "Uso y control en la empresa de los medios informáticos de comunicación", en *Aranzadi Social*, 3 (2001); Mercader, J. R., "Derechos fundamentales de los trabajadores y nuevas tecnologías", en *Relaciones Laborales*, 10 (2001); Escribano, J., "El derecho a la intimidad del trabajador. A

debe que contemos ya con la primera sentencia del Tribunal Europeo de Derechos Humanos, dictada el 3 de abril de 2007 en el caso *L. Copland vs. Reino Unido*. Durante seis meses se había controlado el teléfono, el correo electrónico (direcciones, fechas y horas en las que se enviaban) y la navegación por Internet (páginas visitadas, fecha, hora y duración) de una trabajadora de un College público sin su conocimiento, sin autorización judicial y sin base legal alguna que permitiera tal control[53]. La doctrina sentada por el Tribunal es clara:

a) Toda comunicación efectuada desde el centro de trabajo quedan incluidas en el concepto de "vida privada", ya sea telefónica, electrónica o de navegación en Internet[54];
b) no existía advertencia previa del control, luego cabía esperar que la trabajadora confiara en la privacidad de sus acciones[55];
c) la información relativa a la fecha y duración de las conversaciones telefónicas y de los números marcados forman parte de las comunicaciones y, aunque se hayan conseguido estos datos legítimamente (facturas), su conocimiento constituye una injerencia en la vida privada[56];

propósito de la STC 186/2000, de 10 de julio", en *Relaciones Laborales*, 10 (2001); RODRÍGUEZ-PIÑERO, M. y LÁZARO, J. L., "Los derechos on-line en el ordenamiento laboral español: estado de la cuestión", en *Derecho y Conocimiento*, vol. 2 (2003); RODRÍGUEZ ESCANCIANO, S., "La potencialidad lesiva de la informática sobre los derechos de los trabajadores", en *Revista Española de Protección de Datos*, 2 (2007).

53. El Gobierno británico alegó tras la demanda que no se había llegado a interceptar las llamadas, ni a analizar el contenido de las páginas, ni el de los correos, y que sólo pretendía realizar un análisis para comprobar si se hacía un uso personal de los medios del College; entendía que no se trataba de una injerencia en la vida privada y que, aun constituyéndolo, estaría justificada por constituir una medida proporcionada para preservar un interés (fondos) público. La demandante dudaba que no se hubieran leído sus correos y alegaba, además, que el College carecía de legitimidad para vigilar a los trabajadores y que lo había efectuado con medios innecesarios y desproporcionados.

54. Sentencia Copland, núm. 41: "Según 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 artículo 8.1 (...) Es lógico pues que los correos electrónicos enviados desde el lugar de trabajo estén protegidos en virtud del artículo 8, como debe estarlo la información derivada del seguimiento del uso personal de Internet".

55. En el número 42 especifica que no se advirtió a la demandante de que estaba siendo controlada, por lo que "podía razonablemente esperar que se reconociera el carácter privado" de sus llamadas, su correo y su navegación.

56. Cfr. Sentencia Copland, núm. 43. Habría que incluir las direcciones electrónicas y también los datos relativos a los correos.

d) la ley puede regular la posibilidad del control y seguimiento con fines legítimos, pero el vacío legal no puede dejar al trabajador a merced del control indiscriminado del empresario[57].

"En consecuencia, 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 artículo 8 del Convenio"[58].

De la jurisprudencia de nuestro Tribunal Constitucional también podemos concluir algunos principios básicos a la hora de enjuiciar este control. La STC 281/2005, de 7 de noviembre, reconocía el poder de la empresa sobre los ordenadores de su propiedad, pero sin un carácter "omnímodo e indiscriminado", por lo que no goza de una "libérrima facultad de control de su contenido, haya o no documentos personales del actor". Por su parte, en las SSTC 98/2000, de 10 de abril, y 186/2000, de 10 de julio, se reconocía que al trabajador le corresponde también en el desempeño de su trabajo un "ámbito propio y reservado frente a la acción y conocimiento de los demás", incluido el empresario; es cierto que no se trata de un derecho absoluto y que puede, por tanto, ceder ante intereses constitucionalmente relevantes, pero para ello se exige la conclusión satisfactoria de tres juicios conjuntamente: a) *de idoneidad*, es decir, que con tal medida se pueda lograr el objetivo propuesto; b) *de necesidad*, es decir, que no exista otra medida más moderada para lograr el mismo objetivo con igual eficacia; y c) *de proporcionalidad*, esto es, que la medida sea ponderada y equilibrada, de modo que deriven de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto[59].

En nuestro ordenamiento existe una diferencia con respecto al británico en esta materia y es que, aunque no existen normas específicas sobre el

57. "El Tribunal no excluye que el seguimiento del uso por parte de un trabajador del teléfono, el correo electrónico e Internet en el lugar de trabajo pueda considerarse 'necesario en una sociedad democrática' en ciertas situaciones que persigan un fin legítimo", pero debe estar regulado explícitamente para evitar la arbitrariedad. Cfr. Sentencia Copland, núm. 48.

58. Sentencia Copland, núm. 44. Más adelante (núm. 54) da a entender que la injerencia hubiera sido más grave si hubiera interceptado las llamadas, conocido el contenido de los correos o analizado el contenido de las páginas visitadas, pero el hecho de no hacerlo no convierte el seguimiento en lícito, simplemente es menos grave.

59. Cfr. STC 186/2000, Fundamento Jurídico 6º.

control de los ordenadores de la empresa, contiene unos preceptos en el Estatuto de los Trabajadores que permiten al empresario dos tipos de control sobre sus empleados y los bienes materiales. Uno de ellos es el art. 20.3, que permite a la empresa adoptar las medidas oportunas para controlar y vigilar el cumplimiento de las obligaciones laborales por parte de sus trabajadores, así como el control de los bienes de la empresa. Sería un "poder ordinario" o normal, sujeto siempre al respeto de la dignidad e intimidad de los trabajadores, como establece el art. 4.2 del mismo texto legal. El otro precepto es el art. 18, que otorga un "poder extraordinario" de control que permite el registro sobre la persona del trabajador, así como el registro de sus taquillas y efectos personales, en cuyo caso sería preciso, en primer lugar, contar con una razón que lo justifique –que puede ser perfectamente la protección del patrimonio empresarial y del resto de los trabajadores– y, en segundo lugar, que su realización se efectúe en presencia de un representante de los trabajadores.

Este art. 18 había servido a los tribunales españoles para resolver los primeros supuestos planteados. Así lo entendió el Tribunal Superior de Justicia de Andalucía[60] y también el Tribunal Superior de Justicia del País Vasco en dos sentencias, la primera de ellas de 21 de diciembre de 2004[61] y la segunda de 12 de septiembre de 2006. En el supuesto de esta segunda

60. La Sala de lo Social (Málaga) del Tribunal Superior de Justicia de Andalucía, en su Sentencia 389/2000, de 25 de febrero, condenó al Instituto Municipal de la Vivienda del Ayuntamiento de Málaga por haber procedido al registro del ordenador y copia de ficheros de un trabajador sin justificar previamente su acción, lo que constituía una intromisión ilegítima en la intimidad de éste. En su Fundamento Jurídico 7º, tras admitir que el art. 18 ET habilita al empresario a realizar los registros, "lo condiciona a que ello sea necesario para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, cosa que la demandada ni siquiera ha alegado en el supuesto de autos, pues de un somero examen del acta de registro se desprende que la empresa ni siquiera adujo causa o motivo alguno para la realización del registro en cuestión. Por ello, consideramos que dicho registro violó el derecho a la intimidad del trabajador, garantizada en el plano estrictamente laboral por el art. 4.2 e) del Estatuto de los Trabajadores". En el mismo sentido se pronunció posteriormente también el Tribunal Superior de Justicia de Galicia.

61. En ella se juzgaba el uso del acceso a Internet para entretenimiento personal y del correo electrónico con fines particulares, sin que existiera norma expresa de la empresa que lo excluyera. El TSJPV estimó que constituía una intromisión ilegítima en la vida privada del trabajador. Posteriormente el Tribunal Supremo, en sentencia de 28 de junio de 2006, entendió que la empresa había dado al trabajador acceso a Internet y cuenta de correo para uso privado sin prohibición expresa de utilizarlo con fines personales, lo que le otorgaba un marco de "ámbito privado y particular para hacer las comunicaciones con otras personas", de modo que todo control vulneraba el art. 18 CE y convertía en nulas las pruebas aportadas para el despido (Fundamento Jurídico 4º).

sentencia, el trabajador había utilizado el ordenador de la empresa para almacenar –además de sus documentos de trabajo– música, fotografías personales y contenido sensible para la empresa en una carpeta con su propio nombre. No existían normas ni advertencia expresa sobre la prohibición de uso con fines personales. La empresa practicó un registro sin conocimiento del trabajador y sin autorización judicial, realizando copia del contenido de la carpeta personal. Más tarde solicitó al trabajador la clave de acceso del ordenador y el consentimiento para el registro, que fue denegado por éste. El tribunal consideró nulas las pruebas obtenidas porque debería haber solicitado al trabajador el permiso de registro desde un principio y, en caso de negativa, haber solicitado autorización judicial[62]. En última instancia podría, al menos, haber realizado el registro con las garantías mínimas exigidas por el art. 18 del Estatuto de los Trabajadores para las taquillas. La omisión de estas garantías le llevó a declarar vulnerado el art. 18 CE[63].

Similar fue la argumentación realizada por el Tribunal Superior de Justicia de Galicia en su sentencia de 25 de enero de 2006. El recurso para unificación de doctrina presentado contra ella ha dado lugar a la sentencia del Tribunal Supremo 8807/2007, de 26 de septiembre, que ha venido a cerrar las discusiones no sin causar ciertas perplejidades. El motivo de litigio era el despido de un trabajador por utilizar el ordenador de la empresa para acceder a páginas pornográficas, lo que ocasionó la entrada de virus en el sistema; el efecto de los virus hizo que la empresa solicitara a los técnicos su reparación, en cuyo transcurso se registró el contenido del ordenador en presencia del Administrador (no del trabajador ni de representante sindical), haciendo copia de los archivos temporales antiguos que demostraban el acceso a las citadas páginas. Reparado el ordenador, se repitió veinte días más tarde la operación de registro y copia en presencia de dos delegados de personal, pero ausente el trabajador y sin su consentimiento.

La sentencia del Tribunal Supremo refunde los argumentos esgrimidos por el Tribunal Europeo de Derechos Humanos en la Sentencia Copland y por los Tribunales Superiores de Justicia españoles. Ello se aprecia desde un primer momento, en el que advierte que el control de uso de los medios informáticos facilitados por la empresa puede afectar al derecho a la intimidad y al secreto de las comunicaciones cuando incide sobre el correo

62. En este caso, podría haber retirado del uso el ordenador hasta conseguir la autorización, a fin de evitar la destrucción de la prueba.

63. Fundamento Jurídico 2º.

electrónico, sobre la navegación por Internet y sobre los archivos personales en él almacenados. El conflicto puede derivar, en estos casos, de las "dificultades prácticas de establecer una prohibición absoluta del empleo personal del ordenador (...) y de la generalización de una cierta tolerancia con un uso moderado de los medios de la empresa", al tiempo que constituye una herramienta propiedad de la empresa facilitada por ésta para cumplir la prestación laboral, por lo que quedaría "dentro del ámbito del poder de vigilancia del empresario" (art. 20.3 ET) siempre que se respete la dignidad del trabajador[64].

Y a continuación afirma, en contra de la doctrina mayoritaria y de la jurisprudencia producida hasta la fecha, que el art. 18 ET no es aplicable a los medios informáticos facilitados por la empresa para la ejecución de la prestación laboral, porque en los registros de taquillas y efectos personales de los trabajadores amparados por este artículo, el empresario actúa de forma excepcional como "policía empresarial" y al margen de lo que le permite el marco contractual. Sin embargo, "las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes [de control]: el ordenador es un instrumento de producción del que es titular el empresario 'como propietario o por otro título' y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen"[65]. Viene a afirmar que el hecho de que se ejecute la prestación de trabajo con el ordenador habilita al empresario para verificar en él su correcto cumplimiento, y se trata, por tanto, de un control normal de los medios de producción.

Ofrece, para sustentar esta doctrina, cuatro razones –todas ellas en el Fundamento Jurídico 3º– que en mi opinión pueden ser susceptibles de crítica. La primera, es que no hay analogía con la taquilla porque su control no tiene que justificarse por "la protección del patrimonio empresarial y de los demás trabajadores de la empresa", sino por su carácter de instrumento de producción y es lógico que compruebe tanto si se realizan actividades extralaborales en horario de trabajo (lo que supondría una retribución injusta) como que se obtiene el resultado debido. Se justifica también por "la necesidad de coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencia de los trabajadores (pedidos, relaciones con

64. Cfr. Fundamento Jurídico 2º. En el mismo sentido, cfr. Informe Jurídico 0391/2007 de la Agencia Española de Protección de Datos sobre *Cribado de correo electrónico*, cit., pp. 6-7.

65. Fundamento Jurídico 3º.

clientes...), por la protección del sistema informático de la empresa, que puede ser afectado negativamente por determinados usos, y por la prevención de responsabilidades que para la empresa pudiera derivar también de algunas formas ilícitas de uso frente a terceros". Pero ¿no pertenece todo esto al "patrimonio empresarial"?

"En segundo lugar, (...) el hecho de que un trabajador no esté presente en el control no es en sí mismo un elemento que pueda considerarse contrario a su dignidad". Es cierto, pero a medias, porque dependerá de lo que se controle y cómo se controle. Un ordenador permite guardar documentos, fotos, vídeos, etc., en los que estén muy presentes rasgos y datos que aporten información muy sensible relacionada con la ideología, religión, moral, orientación sexual, etc. que pertenecen al ámbito de la privacidad del usuario. Si se exige esa presencia en otros supuestos es porque se considera una garantía para el respeto de su dignidad e intimidad.

En tercer lugar, entiende el Tribunal Supremo que la exigencia de que el registro de la taquilla se practique en el centro de trabajo y en las horas de trabajo "tiene por objeto permitir la presencia del trabajador y de sus representantes", no preservar su intimidad. También es cierto, pero constituye un medio indirecto añadido de preservar la intimidad, de modo que el empresario no pueda actuar indiscriminada y arbitrariamente. En una máquina de hacer tornillos no puede reflejarse la intimidad del trabajador, en un ordenador sí, por muy de la empresa que sea, de modo que la presencia añade un plus que garantiza de modo más real el respeto de los derechos fundamentales.

"Por último, la presencia de un representante de los trabajadores o de un trabajador de la empresa tampoco se relaciona con la protección de la intimidad del trabajador registrado; es más bien (...) una garantía de la objetividad y de la eficacia de la prueba"[66]. Al igual que en la razón anterior, se trata de un medio indirecto de preservar la intimidad, por cuanto impide el control indiscriminado por parte del empresario cuando puede estar comprometida la intimidad y el secreto de las comunicaciones. No creo

66. Estos cuatro argumentos le lleva a concluir que "No cabe, por tanto aplicación directa del artículo 18 del ET al control del uso del ordenador por los trabajadores, ni tampoco su aplicación analógica, porque no hay ni semejanza de los supuestos, ni identidad de razón en las regulaciones"; En definitiva, quedaría regulado por el art. 20.3 ET. Cfr. Fundamento Jurídico 3º. El ordenador no es equiparable a un destornillador, un torno, un bolígrafo, una mesa, etc.; se trata de un medio de producción con características específicas que lo hacen idóneo para recoger datos sensibles que pertenecen a la intimidad.

que se trate simplemente de una garantía de objetividad, al alcance por otras vías –grabación del registro, por ejemplo–, sino de estar sometido a otra opinión sobre la proporcionalidad y control de legalidad de lo que se va a llevar a efecto sin una previa autorización judicial.

En definitiva, los criterios fijados por el Tribunal Supremo son los siguientes:

1.º El poder que corresponde al empresario sobre el uso del ordenador por parte de los trabajadores (almacenamiento, comunicaciones electrónicas y navegación, incluidos los archivos temporales que se guarden automáticamente como resultado de ésta[67]) se encuentra regulado por el art. 20.3 ET, y por lo tanto debe ser considerado como el control normal y similar al que puede realizarse sobre cualquier otro bien de producción, sin requerir garantías especiales como pudiera ser la presencia de representantes sindicales.

2.º Tal poder sólo está limitado por el respeto de la dignidad e intimidad de los trabajadores, pero éstas carecen de carácter absoluto y no excluyen todo control[68].

3.º El empresario debe fijar claramente unas normas de uso del ordenador y del acceso a Internet, que pueden excluir cualquier uso personal[69].

67. Las garantías derivadas de la intimidad y del secreto de las comunicaciones son extensibles a las comunicaciones telefónicas, correos electrónicos y a los archivos personales; aunque puedan caber dudas sobre la inclusión de los archivos temporales guardados automáticamente por el ordenador como resultado de la navegación, "hay que entender que estos archivos también entran, en principio, dentro de la protección de la intimidad", porque pueden tener datos sensibles en orden a la intimidad (ideología, orientación sexual, religión, etc.). Cfr. Fundamento Jurídico 4º.

68. Debe respetar la intimidad en los términos dictados por el Tribunal Constitucional en sus Sentencias 98 y 186/2000, teniendo en cuenta "el hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores", lo que crea "una expectativa también general de confidencialidad en esos usos". Dicha expectativa no puede ser desconocida, pero tampoco convertirse en causa de exclusión absoluta de control si se han establecido instrucciones para su uso y controles para verificar la correcta utilización que garantice la permanencia del servicio. Cfr. Fundamento Jurídico 4º.

69. Los límites que puedan establecer estas normas dependerán del empresario o de la negociación con sus trabajadores, pero pueden ser exhaustivos. Puede servir de ejemplo, la Instrucción 2/2003, de 26 de febrero, del Pleno del Consejo General del Poder Judicial, que en su art. 9 impone a todos los usuarios de equipos y sistemas informáticos al servicio de la Administración de Justicia –incluidos los magistrados– la prohibición de utilizar el "correo electrónico para actividades personales restringidas en las que pueda haber alguna expectativa de privacidad o secreto en las comunicaciones".

Tales normas deben explicitar los medios de control que serán efectuados[70].

4.º Si no existen tales normas, debe presumirse que existe autorización para una utilización personal moderada, siendo preciso en estos casos el consentimiento del trabajador o la previa autorización judicial para efectuar el registro[71].

En mi opinión, estos criterios conllevan una disminución de las garantías legales de derechos tan importantes como la intimidad y el secreto de las comunicaciones del trabajador. Nadie pone en duda que el ordenador es propiedad de la empresa y que puede ser esencial para la producción, pero igual de evidente es que constituye una herramienta peculiar en la que puede quedar reflejada con gran facilidad información íntima del usuario, lo que requiere un tratamiento distinto al resto de las herramientas profesionales. Creo que, existiendo o no normas de uso, es preciso excluir cualquier control indiscriminado y arbitrario del empresario o directivos[72], lo que podría lograrse con la necesidad de aportar una razón justificada para llevarlo a cabo y la presencia de un representante del trabajador, como exige el art. 18 ET. En el caso Copland el Tribunal Europeo de Derechos Humanos no puede entrar en esta cuestión porque el Reino Unido carecía de regulación similar. Nuestra regulación laboral es más respetuosa con la

70. "Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios –con aplicación de prohibiciones absolutas o parciales– e informar a los trabajadores de que va a existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos (...) De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizar el control, se ha vulnerado 'una expectativa razonable de intimidad' en los términos que establece el Tribunal Europeo de Derechos Humanos en las Sentencias Halford y Copland". Cfr. Fundamento Jurídico 4º.

71. En el supuesto enjuiciado entendió vulnerada la intimidad del trabajador por proceder al registro sin que existieran normas previas que prohibieran el uso personal. Cfr. Fundamento Jurídico 5º.

72. La ya citada STC 98/2000, de 10 de abril, establece que la relación laboral no supone una renuncia absoluta a la intimidad, siendo necesario en cada caso concreto valorar si las medidas de vigilancia y control establecidas pueden dañar el derecho a la intimidad de los trabajadores. En su Fundamento Jurídico 6º concreta esta valoración en "si la instalación se hace o no indiscriminada y masivamente, si los sistemas son visibles o han sido instalados subrepticiamente, la finalidad real perseguida con la instalación de tales sistemas, si existen razones de seguridad, por el tipo de actividad que se desarrolla en el centro de trabajo de que se trate, que justifique la implantación de tales medios de control, etc."

intimidad y sería preciso aprovecharlo como un plus en la garantía de los derechos humanos[73].

Además, creo que hay que establecer una clara diferencia entre el simple control del ordenador y el control del contenido de los correos electrónicos, pues en éste no sólo queda afectada la intimidad, sino también el secreto de las comunicaciones con todas sus características peculiares. Los mensajes electrónicos de los empleados (recibidos o enviados) desde sus puestos de trabajo y en horario laboral pueden contener referencias íntimas del trabajador y de terceros sin relación alguna con el entorno laboral[74].

Debemos partir de la premisa de que es cierto que el trabajador no tiene reconocido ni de modo universal ni en nuestro ordenamiento jurídico un derecho a usar de forma privada los medios tecnológicos que la empresa pone a su disposición para el desempeño de su cometido laboral, pero tampoco se lo prohíbe expresamente. La solución definitiva, como han reiterado todos los tribunales, tendrá que venir de la mano de una nueva regulación legal que se enfrente a este problema, pero mientras tanto debe ser la negociación colectiva o los empleados y empresarios, en particular, los que tengan que pactar unas medidas concretas. La doctrina mayoritaria entiende, al igual que la jurisprudencia –como ya hemos visto–, que las medidas de control son lícitas cuando existe una política clara de la empresa, estableciéndose un código de conducta conocido por los trabajadores y unas reglas accesibles y admitidas por éstos. Tales medidas –que restringen derechos fundamentales– deben cumplir unos requisitos como

73. Esta es la impresión que se obtiene a partir de los documentos elaborados en el seno de la Unión Europea por el *Grupo del Artículo 29* (Recomendación 1/2001 sobre datos de evaluación de los trabajadores, Dictamen 8/2001 sobre tratamiento de datos personales en el contexto laboral, Documento de Trabajo de 29 de mayo de 2002, relativo a la vigilancia por parte del empleador de la utilización del correo electrónico e Internet por parte de los trabajadores y Dictamen 2/2006 sobre el Respeto de la Privacidad en relación con la prestación de servicios de cribado de correo electrónico) y por el *Grupo Berlín* (Informe y Recomendaciones sobre las Telecomunicaciones y la Privacidad en las relaciones laborales).

74. Vid. CARDONA, Mª B., "Correo electrónico de los empleados. Transgresión de la buena fe contractual", en *Aranzadi Social*, T. III (2000); VAL ARNAL, J.J. DE, "El correo electrónico en el trabajo y el derecho a la intimidad del trabajador", en *Aranzadi Social*, T. III (2000); SANFULGENCIO, J. A., "Reflexiones prácticas sobre el uso del correo electrónico en el trabajo y la utilización del ordenador para fines particulares", en *Revista de la Asociación Española de Dirección de Personal*, 18 (2001); GARCÍA, J. I., "Sobre el uso y abuso del teléfono, de fax, del ordenador y del correo electrónico de la empresa para fines particulares en lugar y tiempo de trabajo. Datos para una reflexión en torno a las nuevas tecnologías", en *Tribuna Social*, 127 (2001).

son la idoneidad para conseguir el objetivo propuesto, la necesidad de las mismas sin que se puedan utilizar otras menos restrictivas y, por último, un equilibrio entre los perjuicios ocasionados y el bien que se produce para el interés general[75]. Por tanto, habría que descartar a priori que sea lícita cualquier medida de control sin más como facultad del "poder normal" del empresario.

Además, habría que distinguir entre el uso para fines particulares de mi dirección desde el trabajo (minombre@miservidor.com), el uso de mi dirección particular pero creada para el trabajo (minombre@empresa.com) y el uso con fines exclusivamente profesionales (departamentodeempresa@empresa.com). En el primer supuesto nos encontraríamos ante un posible uso indebido de la red en horario laboral, por lo que la cuenta de correo será intocable por parte de la empresa. Equivale a la carta privada que recibe un trabajador en su lugar de trabajo y que dejan sobre su mesa al repartir el correo, por lo que nadie tiene derecho, ni siquiera el empresario, a abrir esa correspondencia[76]; el simple hecho de utilizar identificadores privados hace presumir que el trabajador lo utiliza para fines privados, aunque podría desvirtuar esta presunción en caso de ser requerido por la empresa y mostrar su contenido si así lo desea.

En el segundo supuesto resulta afectado el nombre de la empresa, por lo que se deben fijar unas reglas de uso –mejor pactadas– y, en caso de indicio de uso inadecuado, el control del contenido deberá motivarse y requerirse autorización judicial o consentimiento del usuario. La propiedad del ordenador y la titularidad sobre la dirección electrónica no faculta al empresario a un control indiscriminado de su uso, no tanto por una vulneración de la intimidad (más complicado en el ámbito laboral)[77], sino por el

75. Cfr. STC 186/2000, de 10 de julio, Fundamentos Jurídicos 6º y 7º.

76. El Tribunal Superior de Justicia de Valencia condenaba, en Sentencia de diciembre de 2000, a un empresario que había manipulado una carta recibida a nombre de uno de sus trabajadores a fin de conocer su contenido.

77. Afirma el Tribunal Constitucional en su Sentencia 186/2000, de 10 de julio, Fundamento Jurídico 6º, que "también hemos afirmado que el atributo más importante del derecho a la intimidad, como núcleo central de la personalidad, es la facultad de exclusión de los demás, de abstención de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimientos intrusiva, como a la divulgación ilegítima de esos datos. La conexión de la intimidad con la libertad y dignidad de la persona implica que la esfera de la inviolabilidad de la persona frente a injerencias externas, el ámbito personal y familiar, sólo en ocasiones tenga proyección hacia el exterior, por lo que no comprende, en principio los hechos referidos a las relaciones sociales y profesionales en que se desarrolla la actividad laboral, que están más allá del ámbito del espacio de intimidad personal y familiar sustraído a intromisiones extrañas por formar

derecho al secreto de las comunicaciones (garantía formal) y por mermar la libertad de autodeterminación y la dignidad en el trabajo. Así lo reconoció, por ejemplo, el Tribunal Supremo francés, en su Sentencia de 3 de octubre de 2001 cuando afirmaba que "un empresario no puede tener conocimiento de los mensajes personales enviados por un trabajador y recibidos por éste a través de un útil informático puesto a su disposición para su trabajo" sin que ello suponga una violación del secreto de comunicación, aunque previamente se hubiera "prohibido la utilización no profesional del ordenador". El Tribunal dio la razón a un ingeniero de Nikon France despedido en 1995, al que los magistrados reconocían que "el trabajador tiene derecho, incluso en su tiempo y lugar de trabajo, al respeto a su intimidad y su vida privada"[78].

Nuestra Constitución también ampara el derecho al secreto de las comunicaciones en el trabajo, y el art. 197 de nuestro Código penal también es aplicable en el entorno laboral[79]. Si se ha prohibido expresamente el uso privado de esta cuenta de correo por parte del trabajador, el empresario podría ejercer un control sobre la misma con los límites establecidos por el Tribunal Constitucional: idoneidad del medio de control, necesariedad y proporcionalidad. Por ello, si existen indicios de uso indebido que justifiquen el control, éste debe ser lo más inocuo posible para los derechos fundamentales, por lo que debería centrarse en el número de mensajes enviados y recibidos, destinatarios y remitentes, asunto contenido en la cabecera, ficheros ligados, dimensión de los mensajes, etc. Si esto no fuera suficiente, al ser la cuenta de correo propiedad de la empresa, debería –a mi juicio– tener la misma consideración que una taquilla, por lo que podrían ser abiertos en presencia de un representante sindical o equivalente en determinados supuestos. Así como el derecho a la intimidad en el trabajo admite limitaciones, también el derecho al secreto de las comunicaciones las puede admitir, aunque ello no debe suponer que se produzcan conductas arbitrarias por parte del empresario.

parte del ámbito de la vida privada". Con todo, hay que decir que el derecho a la intimidad "en principio" queda excluido del ámbito laboral, pero no definitivamente; y lo mismo ocurre con el derecho al secreto de las comunicaciones. El trabajador no pierde estos derechos mientras realiza su trabajo, aunque pueden resultar limitados por exigencias de las circunstancias.

78. En idéntico sentido se había manifestado el Tribunal de Trabajo de Bruselas en Sentencia de 2 de mayo de 2000.

79. Sobre las consecuencias penales, vid. ROMEO CASABONA, C. Mª, "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet", en *Derecho y Conocimiento*, vol. 2 (2003), pp. 123-149.

Esta ha sido la doctrina establecida por la Sala de lo Penal del Tribunal Supremo en sus Sentencias 666/2006, de 19 de junio, y 358/2007, de 30 de abril. Esta última resuelve el recurso de Casación interpuesto por un trabajador municipal que entendía vulnerada su intimidad y el secreto de sus comunicaciones al ser copiado uno de sus correos electrónicos durante una prolongada baja laboral. El Tribunal Supremo entiende que cuando el ordenador es de titularidad de la empresa o de la Administración y la cuenta electrónica tiene como fin el desempeño de las funciones laborales, ante una baja laboral y la necesidad de continuar con el normal desarrollo de las prestaciones de la empresa hacia sus clientes, es lícito abrir el correo si esa es la única posibilidad de cumplir con las obligaciones adquiridas por la empresa o por la entidad pública implicada[80]. En ningún momento admite que tales circunstancias justifiquen el visionado de todos los correos electrónicos recibidos o enviados, sino el de aquellos que tengan como objeto el desarrollo de las normales prestaciones laborales. Por ello afirma el tribunal Supremo que "se podrían haber planteado cuestiones distintas en el caso de que, aun cuando no fuera previsible el hallazgo de datos reservados o íntimos, tal hallazgo se hubiera producido, pues en ese caso sería valorable la reacción de los autores ante tal suceso"[81].

El último tipo de cuenta de correo (empresa@empresa.es) es el más claro de todos, pues lo que hace el trabajador es operar en nombre de la empresa con una cuenta de correo de ésta, por ello debe excluirse el uso personal; la empresa podría controlar perfectamente el contenido y abrir los mensajes sin necesidad del consentimiento de ninguno de los emplea-

80. Se trataba de un ordenador de titularidad pública –utilizado en ocasiones por otros trabajadores– y una cuenta de correo electrónico para el desempeño del trabajo, de cuya apertura se obtuvo el documento de naturaleza pública buscado e imposible de conseguir por otras vías dada la enfermedad del trabajador. Por ello afirma el Tribunal Supremo que "no es posible afirmar que la voluntad de los acusados estuviera caracterizada por la finalidad de vulnerar la intimidad del recurrente, pues razonablemente solo era posible esperar el hallazgo de datos públicos en los archivos revisados. Ello coincide además con la conducta posterior de aquellos una vez accedieron al ordenador, pues exclusivamente utilizaron un mensaje de correo electrónico con las características expuestas en el hecho probado, que excluye en su contenido tanto la naturaleza de datos íntimos como la de datos reservados, en cuanto que se trataba de un reenvío procedente de la Alcaldía de un mensaje que previamente había sido remitido precisamente al Alcalde, y relacionado con un borrador de un convenio urbanístico. Es decir, exclusivamente en relación con actuaciones administrativas de los órganos municipales". STS 358/2007, de 30 de abril, Fundamento Jurídico 1º.

81. STS 358/2007, de 30 de abril, Fundamento Jurídico 1º, último párrafo.

dos que tengan acceso a la misma[82]. Pensemos, por ejemplo, que una enfermedad del trabajador que normalmente opera con esa dirección de correo podría dejar inoperantes los servicios de pedidos, atención al cliente, servicio técnico, etc.

6.2. *Las comunicaciones electrónicas y la libertad sindical*

Otro de los supuestos que dio origen a una gran disputa relacionado con el secreto de las comunicaciones y el uso de las Nuevas Tecnologías en el ámbito laboral tuvo lugar con motivo del conflicto entre el BBVA y CCOO por el envío a los empleados de mensajes de contenido sindical, considerando el sindicato que se había vulnerado su derecho de información sindical al ser bloqueados por el banco[83]. La Sala de lo Social de la Audiencia Nacional dio la razón en su sentencia de 6 de febrero de 2001 al sindicato siempre que utilizara la mensajería electrónica con "mesura y normalidad", al tiempo que instaba a regular el uso de las nuevas tecnologías en la empresa en la negociación colectiva mientras no existiera norma legal que lo hiciera[84]. La Sala de lo Social del Tribunal Supremo decidió anular, en su sentencia de 26 de noviembre de 2001, la dictada por la Audiencia Nacional sin entrar en la cuestión más interesante para nuestro estudio: la licitud de la interceptación de la correspondencia electrónica por parte del empresario[85]. Pero sí que reconoció en ella que

82. En este último caso se podría ejercer todo tipo de control, tanto el formal (número de envíos, duración, destinatarios, tipo de archivos, etc.) como el material (propiamente del contenido, con apertura de los mensajes y ficheros).

83. Vid. CORREA, M., "Libertad sindical y libertad informática en la empresa", en *Revista de Derecho Social*, 2 (1998); MARÍN, I., "La utilización del correo electrónico por los sindicatos o sus secciones sindicales para transmitir noticias de interés sindical a sus afiliados o trabajadores en general", en *Aranzadi Social*, 1 (2001).

84. El sindicato se amparaba en un *ius usus inocui* de la red, que no impedía el normal desarrollo de la actividad empresarial, mientras que la entidad bancaria alegaba que entre las normas de uso facilitadas a sus empleados se recogía que "el correo electrónico es una herramienta de productividad que el grupo pone a disposición de sus empleados para el desarrollo de las funciones que les tiene recomendadas. Los usos ajenos a estos fines son por tanto considerados inapropiados y en el límite podrían configurar falta laboral. En particular la remisión a uno o varios usuarios de correos no solicitados (actividad conocida como 'spam') es una práctica rechazable y, dependiendo de las circunstancias que concurran, puede llegar a ser perseguible".

85. Es cierto que en ningún momento se le pidió al Tribunal Supremo que se planteara esta cuestión, pues el recurso había sido interpuesto por el BBVA –convencido del derecho que tiene el empresario a controlar el uso de la red– y la única cuestión esencial planteada

la empresa no tenía obligación de facilitar los medios materiales de comunicación a los sindicatos y trabajadores, salvo que se hubiera pactado expresamente.

El Tribunal Constitucional –con criterio mantenido invariablemente desde su Sentencia 114/1984, de 29 de noviembre– ha entendido el derecho al secreto de las comunicaciones "rectamente entendido, [como] el derecho fundamental [que] consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto"[86]. Estas dos apreciaciones convertían en dudosa la legitimidad del BBVA para discriminar los mensajes sindicales dirigidos a sus empleados. Siendo cierto que los medios pertenecen a la empresa y que cumplen un fin determinado, se hace necesario compaginar el uso empresarial de los medios con esa libertad de las comunicaciones reconocida por el Tribunal Constitucional. Por ello, contrariamente a lo fijado por el Tribunal Supremo y dado que es fácil conocer el tráfico usual de la red, se trataría de establecer tan sólo limitaciones a los posibles horarios de envíos y a la cantidad de mensajes ligados, evitando de este modo que se pudiera producir un colapso de la red, que es lo que pretendía evitar la empresa (cfr. STC 281/2005)[87].

Como bien había manifestado la Audiencia Nacional, ni la Constitución ni la Ley Orgánica de Libertad Sindical "permiten reconocer en términos absolutos... el derecho a utilizar el medio del correo electrónico a través del servidor de la Empresa para el ejercicio de la actividad sindical en la misma o recibir la información que le remita su Sindicato"[88], pero

era si la representación sindical tenía derecho o no a usar la red de la empresa para remitir su información sindical.

86. STC 114/1984, de 29 de noviembre, Fundamento Jurídico 7º. También lo recoge literalmente la STC 70/2002, Fundamento Jurídico 9º: "Rectamente entendido, el derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas. El bien constitucionalmente protegido es así –a través de la imposición a todos del 'secreto'– la libertad de las comunicaciones, siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje –con conocimiento o no del mismo– o captación de otra forma del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo)..."

87. Si los representantes sindicales no respetaran estas limitaciones y causaran perjuicio demostrable a las empresas por dejar bloqueados los sistemas informáticos (ocasionando pérdidas o lucro cesante), deberían responder de los daños causados, como lo hacen en Gran Bretaña y EE.UU.

88. SAN 17/2001, de 6 de febrero de 2001, Fundamento Jurídico 4º.

sí un derecho "a transmitir noticias de interés sindical a sus afiliados y a los trabajadores en general a través del correo electrónico (e-mail) con la mesura y normalidad inocua" (FJ 5°) como lo venía realizando antes de ocasionar los problemas. Sin embargo, el Tribunal Supremo se situó en una posición estricta de justicia formal: no hay precepto legal que reconozca tal derecho, no existe acuerdo entre las partes al respecto (ni siquiera tácito, como podría ser el uso pacífico previo) y tampoco existe autorización unilateral del empresario, por lo que CC.OO debía cesar en el uso de la red del banco mientras no cambiara una de las tres posibilidades[89]. Los últimos convenios colectivos suelen hacer ya mención expresa de estas cuestiones, bien para conceder acceso en condiciones determinadas, bien para denegarlo[90].

En estos supuestos es preciso plantearse si las interceptaciones de los correos electrónicos de contenido sindical, además de afectar a la libertad de comunicaciones, afectarían también al secreto de las comunicaciones. La respuesta debe ser negativa, puesto que la interceptación realizada con filtros por parte del banco permite rechazar los mensajes sin acceder a su contenido y con independencia de los destinatarios, por lo que quedaría amparada tal conducta por la facultad de control en el entorno laboral que corresponde al empresario.

6.3. *Vulneración de la intimidad y del secreto de las comunicaciones en general*

Un supuesto de carácter internacional y de importancia considerable, fue el de la famosa red *Echelon*, de la que se confirmó su existencia en

89. En los Fundamentos Jurídicos 2° y 3° resalta el TS que la cuestión verdaderamente importante es si el sindicato tiene derecho a esos medios tecnológicos, por ello pasa por alto incluso la posible nulidad de la Sentencia recurrida por su imprecisión. En el Fundamento Jurídico 4° expone que "descartada la adquisición del derecho por el consentimiento de su ejercicio, es lo cierto que no hay norma jurídica alguna que conceda al Sindicato el derecho a utilizar los medios informáticos del Banco para realizar la comunicación con sus afiliados y con las Secciones sindicales... Podrá ser objeto de negociación colectiva o acuerdo de cualquier tipo, pero, mientras no se obtenga, la utilización deberá ser expresamente consentida por la demandada".

90. Por ejemplo, el *I Convenio Colectivo Getronics Grupo CP S.L.*, en su Sección 10ª ya reconocía el acceso de los sindicatos a la red y el derecho a enviar correos de contenido sindical a los empleados, aunque con "previo conocimiento y aceptación de la empresa". Sin embargo el *Convenio Mapfre, Grupo Asegurador 2002-2004* (firmado el 21 de febrero de 2002) concedía acceso a la red en su art. 55, pero establecía expresamente que "Los representantes de los trabajadores no utilizarán como medio de comunicación el envío de correos electrónicos a grupos de empleados".

marzo de 2001 por parte de una Comisión del Parlamento Europeo que le atribuyó un papel fundamental en la interceptación de mensajes electrónicos. Gerhard Schimd, parlamentario y ponente de la Comisión, recomendó en su exposición a los gobiernos, empresas y ciudadanos la utilización de sistemas de cifrado seguro[91]. Ni la erradicación del terrorismo, ni la seguridad del Estado, ni la persecución de la pedofilia, etc., justificarían la interceptación indiscriminada por parte de los poderes públicos. Debe existir una razón y una resolución judicial motivada o, en caso de urgencia, la autorización de una instancia gubernativa prevista en la ley y que pueda responder después de la decisión tomada[92]. Los atentados de Nueva York, Madrid y Londres sirvieron de justificación para que algunos gobiernos –nacionales o locales– promovieran la aprobación de normas vulneradoras de la privacidad. Ya nos hemos referido a la Sentencia del Tribunal Constitucional alemán de 27 de febrero de 2008 que declaraba la inconstitucionalidad de una norma del Estado de Renania del Norte-Wesfalia que permitía a la policía las injerencias tecnológicas sin autorización judicial. El Reino Unido también ha tenido que modificar algunas de sus normas en este sentido[93].

En España la denuncia más notoria se ha producido sobre la red SITEL. En el año 2000 comenzó a desarrollarse un sofisticado software, con este nombre, que permitía la interceptación de comunicaciones y la recogida de ciertos datos anexos (números y nombres de los usuarios, localización geográfica, DNI u otro documento identificativo, NIF o CIF, etc.) que las operadoras debían entregar a unos "agentes facultados" antes de intervención

91. El Parlamento Europeo aprobó por 367 votos a favor, 159 en contra y 34 abstenciones, el informe definitivo de 120 páginas sobre las actividades de la red de espionaje *Echelon*. Gerhard Schmid –autor del informe– consideró probado que este sistema de interceptación electrónica de las comunicaciones privadas y de carácter económico contaba con la cooperación de Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda.

92. El *Informe Cappato* –aprobado en julio de 2001 por 22 votos a favor, 12 en contra y 5 abstenciones por el Comité de Libertades Civiles del Parlamento Europeo– proponía restricciones a las autoridades policiales comunitarias para interceptar el tráfico de las comunicaciones y su localización, y desestimaba la propuesta de guardar los datos del tráfico de las comunicaciones electrónicas durante siete años, proponiendo alternativamente un plazo máximo de 30 días. La falta de consenso entre los Estados miembros hizo que se retrasara sucesivamente su aprobación definitiva en sesión plenaria del Parlamento.

93. En mayo de 2008 se presentó un nuevo proyecto de norma que permite la creación de base de datos, cedidos por compañías telefónicas y operadoras de Internet, sobre detalles de llamadas y correos electrónicos que serán guardados durante 12 meses, pero exige autorización judicial para que puedan ser procesados

judicial alguna. En marzo de 2004 comenzó la fase de prueba bajo riguroso control judicial, pero carecía de base legal para su utilización generalizada. El Ministerio de Industria aprobó en abril de 2005 el *Reglamento sobre las condiciones para la prestación del servicio de comunicaciones electrónicas, el servicio universal y la protección a los usuarios* (RD 424/2005, de 15 de abril)[94] que incluía en su articulado (arts. 88, 89, 95, 96 y 97) la interceptación de las comunicaciones sin previa autorización judicial.

La Asociación de Internautas recurrió la norma ante el Tribunal Supremo por entender que suponía la restricción de derechos fundamentales (intimidad, protección de datos y secreto de las comunicaciones) y precisaba, por tanto, una regulación mediante ley orgánica.

En octubre de 2007, antes de que se produjese fallo alguno del Tribunal Supremo, fue aprobada la Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*, lo que otorgaba rango legal al contenido del Reglamento recurrido. Aprobada esta ley, el Tribunal Supremo preguntó a los recurrentes sobre su desistimiento, pero éstos mantuvieron que debía ser una ley orgánica y no ordinaria la que regulara tal materia y, además, que seguía sin exigirse el control judicial previo.

El 5 de febrero de 2008 el Tribunal Supremo desestimaba el recurso por entender que la ley cumplía todos los requisitos exigibles al permitir simplemente la recogida de datos instrumentales sin afectar al contenido de la comunicación[95]. En marzo de 2008 se interpuso Recurso de Amparo ante el Tribunal Constitucional alegando que el Tribunal Supremo había vulnerado el sistema de competencias al valorar la constitucionalidad de la norma sin plantear la cuestión de inconstitucionalidad al Alto Tribunal, y que la norma no respetaba las garantías de derechos fundamentales[96].

Es de destacar que el Tribunal Supremo ha considerado lícita la obtención de datos personales –sin previa autorización judicial– disponibles en

94. El Reglamento desarrollaba la Ley 32/2003, de 3 de noviembre, *General de Telecomunicaciones*.

95. En voto particular, uno de los Magistrados manifestaba su disconformidad con el fallo argumentando que no se garantizaba un control judicial del tipo de datos a recoger y del alcance del seguimiento (autorizados genéricamente por la ley), por lo que entendía precisa la presentación de una cuestión de inconstitucionalidad.

96. Aún no se ha pronunciado nuestro Tribunal Constitucional y, dado el ritmo de resolución de los recursos, es probable que debamos esperar un par de años.

las redes de intercambio P2P cuando es la policía quien los obtiene, y así se recoge en la Sentencia 236/2008, de 9 de mayo. En ella consideraba que las pruebas obtenidas por la policía en este tipo de redes son válidas, porque todo lo que se puede obtener en ellas (datos, ficheros, etc.) son puestos a disposición del resto de usuarios voluntariamente por sus titulares, por lo que debe entenderse que tienen carácter público[97]. Pero en contradicción con la sentencia de 5 de febrero anteriormente citada, entiende el Tribunal Supremo en esta posterior que las pruebas obtenidas resultan válidas porque la policía, una vez que comprueba los indicios de comisión de un delito desde una determinada dirección IP, solicita autorización judicial para identificar al usuario. Este modo de proceder es el más acorde con una garantía efectiva de los derechos fundamentales, que solicita la autorización judicial antes de identificar al usuario de la IP.

Desgraciadamente el riesgo que sufre nuestra privacidad no proviene solamente de instancias oficiales, sino también por parte de hackers y de empresas que desean obtener algún beneficio con los datos obtenidos. La primera demanda se formuló contra Netscape por obtener información de los usuarios no autorizada por éstos mediante su SmartDownload, programa que se activaba automáticamente al descargar archivos de la red y transmitía a Netscape información sobre lo realizado para crear un perfil de descargas. Poco más tarde fue DoubleClick la demandada por procesar los hábitos de navegación de quienes usaban sus banners, mientras que Avenue A y MatchLogic lo fueron por implantar cookies en los discos duros de los internautas sin su consentimiento. ¿Constituyen estos hechos un atentado contra la intimidad? Naturalmente, aunque habría que admitir que viene precedido por la violación de otro derecho, el de la autodeterminación informativa, pues se ha llegado a conocer nuestra intimidad mediante la recolección y tratamiento de datos personales sin nuestro consentimiento[98].

97. Esta sentencia anulaba otra de la Audiencia de Tarragona que consideraba nulas las pruebas obtenidas por vulnerar el derecho al secreto de las comunicaciones al "rastrear" las descargas de la usuaria denunciada sin control judicial. El Tribunal Supremo estimaba que esos rastreos se pueden llevar a cabo, dadas las características del P2P, sin violentar la privacidad de los usuarios, que consienten esa posibilidad si quieren utilizar dichos programas (no vulnera el art. 18, 1º y 3º CE). Se trata de una doctrina muy cuestionable, puesto que abre la puerta a todo tipo de abusos.

98. Las demandas no animaron al sector privado a erradicar estas prácticas, como pusieron de relieve, por ejemplo, las actividades de la compañía norteamericana Comcast, tercera operadora de cable que reconocía haber registrado toda la actividad en Internet del millón de

En la actualidad, los intentos de frenar los intercambios de contenidos digitales protegidos por derechos de autor ha elevado el riesgo de vulneración de la privacidad. Las sociedades de autores han contratado empresas y el desarrollo de software espía para identificar a los usuarios infractores. Dado que no constituyen elemento de prueba los datos obtenidos ilegalmente, en algunos países han intentado forzar a las operadoras para que entreguen esos datos, pero con resultado negativo. La Sentencia del Tribunal de Justicia de las Comunidades Europeas de 29 de enero de 2008, Asunto C-275/06, *Promusicae vs. Telefónica de España*, ha resuelto que el derecho comunitario no obliga a los Estados a facilitar los datos personales para garantizar los derechos de autor frente a infracciones civiles (sí en los casos de investigación criminal y para la salvaguardia de la seguridad pública y de la defensa nacional). En el caso de protección de derechos y libertades personales que sólo constituyen ilícitos civiles, cada Estado tiene libertad para exigir la facilitación de datos (proporcionalidad), pero debe ser restrictivo. En el caso de España, la legislación vigente no lo permite[99].

7. Conclusiones

Era imposible reflejar en 1948 en el texto de la Declaración Universal algo tan concreto como las incidencias de las Nuevas Tecnologías en la vida privada y su trascendencia para el desarrollo personal. Pero, afortunadamente, la redacción de los artículos que la reconocen y garantizan es tan abierta que permite la exigencia de una protección adecuada a las circunstancias contemporáneas. Sesenta años después de su aprobación corresponde a los legisladores y a los jueces la obligación de habilitar los mecanismos y vías necesarias para que la protección de la privacidad no

clientes a los que daba servicio sin haberlo notificado previamente. Aunque negó cualquier intención de tratamiento para obtener rendimientos de ellos y aseguró que sólo trataba de optimizar la navegación, la compañía responsable de la tecnología –Inktomi– admitió que los datos recogidos sobrepasaban los necesarios.

99. En Francia y en el Reino Unido los gobiernos han llegado a acuerdos con las operadoras para que éstas desconecten temporal o definitivamente –en caso de reincidencia– a los usuarios infractores. La medida no deja de ser problemática, por cuanto convierte a las operadoras en policías de la Red. En España, el portavoz del Consejo General del Poder Judicial declaró en mayo de 2008 que se trata de una materia que debería ser regulada mediante ley, no al margen de ella.

tenga que discurrir por los senderos propios del mercantilismo, es decir, que tuviéramos que recurrir al derecho de propiedad sobre lo íntimo y sobre los datos para obtener una garantía efectiva. Es preciso establecer unos mecanismos propios y adecuados en la Sociedad de la Información, complementados por la autorregulación, pero sin dejar todo en manos de ésta con el peligro del sometimiento a los más fuertes (las grandes empresas).

No es sencillo, pues los Estados suelen apelar continuamente a la seguridad nacional para establecer limitaciones excesivas, facultando incluso a entidades privadas que le faciliten la labor mediante el almacenamiento de datos y su procesamiento posterior. Es preciso hacerse cargo de que lo que está en juego es la dignidad del ser humano y su desarrollo como persona, lo que requiere el establecimiento de normas protectoras adecuadas. La protección de datos personales no tiene como fin únicamente la simple protección formal de éstos frente al conocimiento de terceros, sino algo más elevado como es preservar la intimidad y la libertad para tomar decisiones personales sin injerencias externas que nos condicionen. En este sentido se inclinan los altos tribunales, que una y otra vez instan al legislador al establecimiento de normas que recojan de modo claro los fines que persiguen los bancos de datos autorizados y las limitaciones incuestionables. De igual modo se ha exigido que dichas normas establezcan unas exigencias mayores en torno al consentimiento otorgado por los usuarios sobre sus datos, exigencias que contemplen una mayor claridad en cuanto a su recolección –en cláusulas contractuales en lugar preeminente, por ejemplo– y en cuanto a su destino.

Es preciso también que las normas no contengan conceptos abstractos que den pie a interpretaciones ambiguas. La Sociedad de la Información requiere normas precisas adaptadas a las nuevas circunstancias. No basta con extender la aplicación de las ya existentes, forzando su interpretación para encajar en ellas las nuevas situaciones derivadas del uso de las Nuevas Tecnologías. El legislador debe partir de la nueva realidad tecnológica y elaborar normas adecuadas a ella, única vía para asegurar los derechos fundamentales de los ciudadanos correctamente. Resulta fundamental en este sentido eliminar lo antes posible las lagunas jurídicas resultantes de las innovaciones tecnológicas, evitando de este modo que lo "técnicamente posible" adquiera visos de legalidad porque no exista una norma que lo impida.

Y, por último, precisamos normas que tengan un carácter dinámico, susceptibles de adaptarse a la variabilidad propia de la Sociedad de la In-

formación. Las continuas innovaciones que se producen en este ámbito obligan a diseñar nuevas estrategias de regulación que doten de agilidad al legislador. Quizá pueda ser útil la formación de comisiones de expertos en los campos más afectados (privacidad, propiedad intelectual, seguridad, etc.) que propongan los cambios normativos precisos sin esperar a que los problemas desborden a los tribunales, facilitando la labor de éstos a la hora de proteger los derechos de todos los ciudadanos.