Privacidad e internet: intimidad, comunicaciones y datos personales

José Justo Megías Quirós
Profesor Titular de Filosofía del Derecho.
Universidad de Cádiz

SUMARIO: I. Objeto y contenido de la vida privada.—II. El derecho a la intimidad.—III. El derecho a la autodeterminación informativa.—IV. El derecho al secreto de las comunicaciones.

El nuevo milenio ha traído consigo un espectacular avance en todo lo concerniente a las nuevas tecnologías, poniendo al alcance de la Humanidad posibilidades difíciles de imaginar hace unos años. Pero no todo ha sido positivo desgraciadamente. Junto a las mejoras de calidad de vida que han reportado y las nuevas vías de promoción de la dignidad del hombre, también encontramos nuevas formas de ataque a los derechos personales y a los intereses sociales por quienes utilizan los nuevos medios para fines ilícitos, ataques más difícil de neutralizar y perseguir dadas las características tecnológicas actuales. Uno de los campos más afectados en este sentido es el de la privacidad —en sentido amplio—, aunque tendríamos que admitir que son los nuevos tipos de atentados contra la propiedad, tanto material como intelectual, los que más preocupan a los legisladores internacionales y nacionales[1].

En estas líneas me ocuparé exclusivamente de lo relativo a la vida privada, ámbito en el que la legislación ha

[1] Vid. J. J. Megías, *Sociedad de la Información*, en RCE nº 27 (2002), pp. 87-99.

quedado desfasada en poco tiempo por esos avances tecnológicos[2]; habría que admitir que el mayor desfase se advierte si nos fijamos en los nuevos atentados y en las medidas obsoletas de protección real con que contamos frente a ellos. Resulta muy notoria la distancia entre lo que nos promete el Derecho como garantías y protección de nuestra privacidad y lo que realmente se puede conseguir en la práctica, y es que las actividades de *hackers* y *crackers* van muy por delante de cualquier diseño de seguridad por parte de las autoridades o del sector privado, de modo que es difícil hacer efectiva la promesa de protección ofrecida por las normas jurídicas.

Habría que añadir también que en los últimos meses se han acentuado las sospechas de atentados contra la vida privada con cierto amparo legal, aunque afortunadamente se ha limitado a los Estados anglosajones y debido a la psicosis sufrida por la sociedad norteamericana tras los actos terroristas del pasado once de septiembre. Pocas horas después de los atentados contra el Pentágono y las Torres Gemelas, el FBI comenzó a solicitar a los proveedores de acceso a Internet, servicios web y correo electrónico que instalasen el sistema Carnivore de espionaje de la Red, llamado también DCS1000, y que sirve para intervenir las líneas telefónicas que fluyen a través de las redes de los ISPs. Al amparo de la *Foreing Intelligence Surveillance Act* (FISA), que limita la facultad de intervención de comunicaciones pero no en el caso de acciones criminales, America Online y EarthLink admitieron inmediatamente su colaboración con el FBI en la consecución de toda la in-

[2] Así ha venido a reconocerlo el Tribunal Constitucional en su reciente Sentencia 70/2002, de 3 de abril. Aunque no llega a entrar realmente en el fondo de la cuestión, sí que deja constancia de su sensibilidad por ella en su FJ 9º: «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».

formación necesaria para esclarecer los hechos, pero se negaron a instalar Carnivore, por considerarlo innecesario.

Dos días más tarde, el Senado aprobaba el proyecto de la *Anti-Terrorism Act*, en el que se incluía una enmienda concediendo al Gobierno un margen mayor en la utilización de la tecnología de vigilancia (intervención de la línea telefónica de Internet, sistemas de vigilancia de las comunicaciones globales, videocámaras *on line*, dispositivos de reconocimiento del rostro y escaneo de las huellas digitales) para combatir el terrorismo. Durante la última semana de septiembre se decidió la revisión de la ley —que se pasó a llamar *Provide Appropiate Tools Required to Intercept and Obstruct Terrorism* (PATRIOT) *Act*— ante el Comité de la Cámara de Representantes de Justicia. El nuevo proyecto de ley 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. A mediados de octubre era aprobada por el Senado, a pesar de las críticas de la Unión de Libertades Civiles de América, que dudaba de la constitucionalidad de algunas de sus cláusulas[3]. 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 In-

[3] También el Parlamento británico aprobaba, sin problemas, una ley similar a mediados de diciembre de 2001, mientras que por las mismas fechas Argentina otorgaba al correo electrónico el mismo *status* que a las comunicaciones escritas en papel, haciendo necesaria la orden judicial para su intervención, con sanciones de 15 días a seis meses de prisión y 90.000 dólares de multa para los infractores.

ternet de contribuir en esta intervención, permitiendo a las autoridades capturar información o facilitándola[4]. En febrero de 2002 era enviada al Congreso una nueva propuesta de ley, la *Cyber Security and Enhancement Act*, que propone el endurecimiento de las penas para los *hackers* y *crackers* y obliga 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*[5].

Por lo que se refiere a la regulación jurídica en nuestro territorio, el año 2000 fue especialmente significativo, no sólo por la entrada en vigor de la *Ley Orgánica* 15/1999, de 13 de diciembre, *de Protección de Datos de Carácter Personal* (LOPD), sino también por las dos Sentencias de nuestro Tribunal Constitucional que vieron la luz a finales de ese año y 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 las nuevas tecnologías, en las que no dejan de apreciarse los diferentes criterios que pueden ser de utilidad para la resolución de los nuevos conflictos.

En el marco comunitario también se aprecia el interés por la materia, concretamente con la aprobación a princi-

---

[4] 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.

[5] El 8 de mayo hacía público Statewotch un comunicado de prensa en el que ponía de manifiesto las intenciones del Consejo de la UE —contra el parecer del Parlamento Europeo— de modificar mediante una Decisión Marco lo establecido en la Directiva 97/66/CE respecto a la conservación de datos de tráfico de telecomunicaciones. El Parlamento prefiere que que siga como hasta ahora, de modo que sean retenidos tan sólo durante el periodo imprescindible para salvar posibles reclamaciones de tarifación y que sólo sean accesibles por fines de seguridad nacional e investigación criminal con previa autorización judicial. Sin embargo, algunos Estados Miembros prefieren que sean retenidos durante un periodo superior y se facilite el acceso a las agencias de policía, aduanas, inmigración y seguridad interna (cfr. *Los gobiernos europeos mueven ficha para acabar con la privacidad en la red,* en www.kriptopolis.com/net/article.php?sid=607)

pios de diciembre de 2000 de la *Carta Europea de Derechos Fundamentales* por los Jefes de Estado en la Cumbre de Niza, que reforzó el estatuto jurídico de los derechos que conforman la vida privada. Pero también hemos asistido recientemente a un nuevo impulso de la *Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas*, cuyo texto se publicó el 19 de diciembre de 2000 en el DOCE, y que ha dado un paso decisivo el pasado mes de enero, al ser aprobada la Posición Común (CE) nº 26/2002 por el Consejo, lo que hace suponer su aprobación definitiva en un plazo breve[6].

La LOPD desarrolla la protección del derecho a la «autodeterminación informativa», cumpliendo así con el mandato constitucional del art. 18.4. 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 quedarían bajo el paraguas de lo que nuestro Tribunal Constitucional entiende como vida privada[7]. Por

---

[6] Una vez aprobada, se sumará y complementará con 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, y con la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

[7] 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. Estas obras son: A. E. PÉREZ LUÑO, *Manual de Informática y Derecho*. Ariel, Barcelona, 1996; Mª. L. FERNÁNDEZ, *Nuevas tecnologías, Internet y Derechos Fundamentales*. McGraw-Hill, Madrid, 1998; A. I. HERRÁN, *La violación de la intimidad en la protección de datos personales*. Dykinson, Madrid, 1998; B. RODRÍGUEZ RUIZ, *El secreto de las comunicaciones: tecnología e intimidad*. McGraw-Hill, Madrid, 1998; F. HERRERO TEJEDOR, *La intimidad como derecho fundamental*. Colex, Madrid, 1998; M. A. DÁVARA RODRÍGUEZ (coord.), *XII Encuentros sobre Informática y Derecho*. Aranzadi, Pamplona, 1999; J. Mª. ÁLVAREZ-CIENFUEGOS, *La defensa de la intimidad de los ciudadanos y la tecnología informática*. Aranzadi, Pamplona, 1999; L. REBOLLO DELGADO, *El derecho fundamental a la intimidad*. Dykinson, Madrid, 2000; T. DE DOMINGO PÉREZ, *El conflicto entre las libertades de expresión e información y los derechos al honor y la intimidad como base para una teoría general de los conflictos de derechos*. Tesis Doctoral. Universidad Miguel Hernández, Elche, 2000 (cito por el manuscrito original); H. CAMPUZANO TOMÉ, *Vida privada y datos personales*. Tecnos, Madrid, 2000.

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. Junto a la intimidad y la autodeterminación informativa, la vida privada estaría constituida también por el derecho al secreto de las comunicaciones (art. 18.3 CE) y la inviolabilidad del domicilio (art. 18.2 CE)[8].

I. Objeto y contenido de la vida privada

La primera dificultad que encontramos al tratar esta cuestión es puramente terminológica, originada por la identificación inicial entre *privacy* —en ocasiones traducida como privacidad— e intimidad, identificación que debe ser desestimada. Aunque ya traté esta cuestión en otro lugar[9], no está de más recoger brevemente la diferencia entre unos términos y otros para evitar las confusiones más comunes que continuamente se producen.

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 unos años más tarde los abogados Warren y Brandeis para escribir su artículo *The Right to Privacy*[10], en el que defen-

---

[8] 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 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, FJ 3º).

[9] *Vida privada y nuevas tecnologías*, en RCE nº 17 (2001), pp. 3-27.

[10] Ch. Warren y L. D. Brandeis, *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 —y también abogado— Brandeis con la propuesta de iniciar un trabajo que justificara la necesidad de proteger jurídicamente aquello que veía ataca-

dieron 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 del entorno personal que hasta el momento no había existido. 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, pues reconocería que la persona contaba con unos derechos, entendidos como derechos naturales, que debían ser respetados tanto por las autoridades legítimas como por los particulares. Entre estos derechos se encontraba el de la «libertad personal», tanto en su vertiente de derecho a la vida pública como del derecho correlativo a la intimidad[11].

Unos años más tarde Brandeis se convirtió en magistrado de la Corte Suprema de EE.UU., que al amparo de la Cuarta Enmienda a la Constitución consagraría definitivamente el reconocimiento de ese nuevo ámbito personal merecedor de protección jurídica. Aunque esta enmienda —referida a la propiedad privada— trata de proteger el derecho de los ciudadanos a la seguridad en sus personas, casas, documentos y efectos de registros, arrestos y embargos sin causa suficiente, también contempla la ilicitud de cualquier orden de registro o arresto que no contenga una motivación fundada, así como la descripción del lugar que debe ser registrado o de las personas o cosas sobre las que recaiga la orden. A partir de los años 30 comenzó a servir de fundamento para proteger la intimidad, pero fue en 1965 cuando esta protección adquirió el rango de derecho constitucional con un contenido identificado con la «autonomía para tomar decisiones íntimas»[12], y con la característica más propia de los derechos humanos de la pri-

---

do en su familia sin causa legítima, limitando así la intrusión de la prensa y cualquier otro sujeto en determinadas esferas que debían tener la consideración de privadas.

[11] Cfr. L. REBOLLO, *El derecho fundamental a la intimidad*, cit., pp. 62-63.

[12] Cfr. B. RODRÍGUEZ RUIZ, *El secreto de las comunicaciones...,* cit., pp. 4-6 y 20-21.

mera generación: la exclusión de terceros de ámbitos que se entienden reservados al titular del derecho[13]. 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 determinadas acciones o en controlar determinados datos[14].

La mentalidad continental europea, por el contrario, sostiene una concepción de los derechos en la que éstos no quedan reducidos a facultades negativas, de exclusión, sino que prima también su vertiente positiva[15], que 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 son tratados si-

---

[13] Vid. sobre las características de estos derechos, J. BALLESTEROS, *Postmodernidad: decadencia o resistencia*. Tecnos, Madrid, 1989, pp. 56 y ss.

[14] 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. Es cierto que el juez goza de cierta discrecionalidad para decidir si es más valiosa la intimidad o el bien jurídico atacado y conocido mediante la acción ilegal, pero en la mayoría de las ocasiones termina venciendo la privacidad sobre la posibilidad de hacer justicia ante la existencia objetiva de acciones graves y manifiestamente delictivas. En el caso de nuestro ordenamiento, también carecen de valor las pruebas obtenidas mediante una clara violación de los derechos y libertades fundamentales, salvo que se haya roto el nexo causal entre el ilícito y un conocimiento posterior de los hechos por otros medios. Esta forma de proceder evidentemente desalienta cualquier intento de conseguir pruebas mediante medios ilícitos, pero deja impunes delitos graves de los que se tiene constancia cierta. Quizá otra solución podría consistir en castigar esos delitos descubiertos ilícitamente, pero establecer también sanciones graves para quienes obtuvieran esas pruebas mediante acciones ilegales, y no zanjar la cuestión con una anulación de la prueba.

[15] Vid. F. CARPINTERO, *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.

guiendo 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 el instrumento aprobado en Niza en diciembre de 2000 y conocido como *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», de modo que deben ser tratados «de modo leal, 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»[16].

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[17], etc. Además, por su naturaleza, podríamos decir que el secreto

---

[16] Esta disparidad de concepción es lo que provoca actualmente la falta de acuerdo, por ejemplo, para una normativa común del comercio electrónico entre europeos y norteamericanos.

[17] 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».

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[18], salvo que haya una causa justificada para permitir lo contrario. Habría que matizar que el simple hecho de intervenir una comunicación no implica forzosamente que podamos llegar a lo íntimo porque dependerá de su contenido, pero es un medio idóneo para conseguirlo[19].

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»[20]. 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

---

[18] 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, FJ 3º).

[19] Así lo ha vuelto a declarar la STC 70/2002, en el FJ 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».

[20] E. GARZÓN VALDÉS, *Privacidad y publicidad*, en «Doxa» 21-1 (1998), p. 226.

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[21]. Estas precisiones nos permiten un análisis o estudio, por separado, de los derechos afectados por las nuevas tecnologías, 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.

II. El derecho a la intimidad

Al establecer Yepes Stork las notas que definen a la persona, afirmaba que la primera de ellas era la intimidad, como grado máximo de la inmanencia o *apertura hacia dentro* que corresponde a cualquier ser humano[22]. 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 eso «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

---

[21] Cfr. E. Garzón Valdés, *Privacidad y publicidad*, cit., p. 227.

[22] «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 centro 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 intimidad creativa, capaz de crecer» y que cuando se muestra al exterior supone una «manifestación de la intimidad». R. Yepes Stork, *Fundamentos de Antropología*. Eunsa, Pamplona, 1996, pp. 76-77.

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»[23]. Si arrebatáramos la intimidad a una persona, estaríamos atacando directamente su dignidad, lo más vulnerable del ser.

Si bien es cierto que la persona vive en sociedad, rodeado de otras muchas personas ante las que debe dar cuenta de innumerables actuaciones, al mismo tiempo tiene también la necesidad de volverse hacia su interior y «meterse dentro de sí, atender a su propia intimidad»[24]. No solemos adoptar nuestras decisiones de un modo irreflexivo, instintivamente, sino que suelen ser el resultado de un proceso racional interno en el que han intervenido sentimientos, forma de pensar, deseos, anhelos, ... que normalmente no deseamos revelar a los demás. Es más, en numerosas ocasiones podríamos comportarnos de un modo distinto si no pudieramos 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, nos permite desarrollar una personalidad propia que tendrá enorme reflejo en nuestro comportamiento externo. Es decir, la intimidad no se agota en la interioridad humana, sino que también «adquiere virtualidad cuando el hombre pasa a la acción», de modo que éste no sólo debe ser soberano de su interior, sino también de sus acciones. Esta soberanía no puede consis-

---

[23] R. YEPES STORK, *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 R. SPAEMANN, *Personas. Acerca de la distinción entre «algo» y «alguien»*. Eunsa, Pamplona, 2000.

[24] T. DE DOMINGO, *El conflicto entre las libertades de expresión e información y los derechos al honor y la intimidad...,* cit., p. 315. Partiendo de este pensamiento orteguiano, entiende la intimidad como un «rasgo ontológico de la persona» de gran trascendencia jurídica, pues resultará importantísimo para el desarrollo de la personalidad (cfr. op. cit., p. 317).

tir simplemente en no encontrar impedimentos a la hora de llevar a cabo las acciones, sino que «comprende también la exclusión de la mirada y control ajenos en su realización», puesto que esa mirada ajena puede condicionarnos en el modo de comportamiento[25]. 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»[26]. No han faltado quienes, llevando hasta el extremo esta reivindicación, como es el caso de E. Garzón, dan 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 sería lícito actuar de acuerdo con lo «políticamente correcto», aunque no responda exactamente a la verdad de lo que sentimos y pensamos[27].

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, y que principios tan importantes como el de «seguridad jurídica», por ejemplo, pueden ceder en favor de la intimidad.

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 con-

---

[25] T. DE DOMINGO, *El conflicto entre las libertades...*, cit., pp. 318-320.

[26] L. GARCÍA SAN MIGUEL (ed.), *Estudios sobre el derecho a la intimidad*. Tecnos, Madrid, 1992, p. 18.

[27] Cfr. E. GARZÓN VALDÉS, *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).

traposición a la mayor concreción de la intimidad que encontramos en los textos jurídicos internos de cada Estado, como es el caso de nuestra Constitución. El art. 12 de la *Declaración Universal de los 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»[28]. Dado que la *Declaración* era tan sólo eso, una declaración, se hacía preciso establecer mecanismos de garantía que pudieran proteger de verdad y con eficacia tanto la intimidad como el resto de derechos que no podían ser negados a ningún ser humano; 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 llamativa 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 un 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 diverso origen y ámbito de aplicación, vinieron a lo largo de los años a incidir sobre la importancia que tiene —para el desarrollo de la persona— la protección de la intimidad, como fueron el *Pacto de San José de Costa Rica* de 1970 (art. 11), el *Convenio 108 Para la*

[28] 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 de 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 su domicilio y de su correspondencia».

protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal de 1981[29], la *Declaración del Parlamento Europeo sobre Derechos y Libertades Fundamentales* de 1989 (art. 6), la *Convención de los Derechos del Niño* de 1990 (art. 16), 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 asemeja 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 que dejen de tener una estrecha conexión.

Este paso de distinguir de forma clara los diversos derechos que conforman la vida privada lo dieron definitivamente los textos constitucionales, que abandonaban esta expresión para dar cabida a la de «intimidad», haciéndose cargo también de las posibles consecuencias que podrían 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»[30]. Esta fórmula, más o menos general, permite incluir en ese ámbito no sólo los datos, sucesos, acciones,

---

[29] 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.

[30] STC 231/1988, FJ 3º; esta idea ha sido reiterada en las SSTC 179/1991, FJ 3º, 20/1992, FJ 3º, 57/1994, FJ 5º, 143/1994, FJ 6º, etc.

etc., que se produzcan en la intimidad[31], sino también aquellos que, aún siendo públicos y notorios, o bien han sido difundidos más allá del ámbito en que tenía sentido su conocimiento, o bien pueden dar acceso a la intimidad si se ponen en conexión con otros datos. El segundo supuesto se enmarcaría concretamente en lo que se ha denominado «teoría mosaico»: un dato conocido públicamente, pero aislado, puede ser que no nos diga nada, pero puesto en conexión con otros datos también públicos nos puede dar el perfil íntimo de una persona. Las nuevas tecnologías permiten la obtención de estos datos, su almacenamiento, su combinación, etc., hasta podernos indicar, por ejemplo, si conviene a un empresario contratar a determinado trabajador o si a una aseguradora le compensa mantener a determinados asegurados, etc.

Por tanto, hay que distinguir netamente entre la facultad de excluir del conocimiento de los datos y la de controlarlos. En el primer caso nos encontraríamos ante el derecho a la intimidad, cuya función es proteger frente a cualquier 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»[32]. 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 derechos del afectado»[33].

---

[31] 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. Cfr. T. DE DOMINGO, *El conflicto entre las libertades...*, cit., pp. 330-334.

[32] STC 144/1999, de 22 de julio, FJ 8º.

[33] STC 292/2000, de 30 de noviembre, FJ 6º.

En esta línea, uno de los mayores peligros hoy día para nuestra intimidad es el rastreo de nuestros hábitos de navegación, que realizan determinadas compañías. Hace poco más de un año Netscape era demandada por obtener información sin consentimiento de los usuarios mediante su SmartDownload, programa que se activaba automáticamente cuando el usuario descargaba archivos de la red y transmitía a Netscape la información, lo que le permitía crear un perfil de descargas para usuarios. También DoubleClick fue 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 vienen precedido por la violación de otro derecho, el de la autodeterminación informativa, pues se ha llegado a conocer nuestra intimidad mediante la recolección de datos personales sin nuestro consentimiento y su posterior tratamiento. El hecho de que se haya denunciado y perseguido no ha animado al sector privado a erradicar estas prácticas, como hemos tenido oportunidad de comprobar recientemente con las actividades de la compañía norteamericana Comcast, tercera operadora de cable que el pasado mes de febrero reconocía que había registrado toda la actividad en Internet del millón de 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[34].

Con mayor precisión se puede determinar que constituye un atentado contra la intimidad el acceso no consentido o el robo de datos personales contenidos en nuestro propio

[34] Ante el revuelo causado entre sus usuarios por la publicación de la noticia, Comcast se comprometió inmediatamente a eliminar los datos no necesarios y abandonar la recogida.

ordenador o en aquellos sistemas que cuentan con nuestra autorización[35], sistemas que tendrían que responder del daño sufrido si no llegaron a adoptar las medidas de seguridad necesarias[36].

Otro tipo de atentados, cada vez más frecuentes, se producen en el ámbito laboral a causa del control —por parte del empresario— bien del ordenador que la empresa ha puesto a disposición del trabajador para desempeñar sus tareas, bien del uso de Internet que el trabajador pueda realizar durante su horario laboral[37]. En lo que se refiere a la primera cuestión, el art. 18 del Estatuto de los Trabajadores permite el registro sobre la persona del trabajador, así como el registro de sus taquillas y efectos personales; pero ésta no es una facultad absoluta, sino que se necesita una razón para llevarla a cabo, que puede ser la protección del patrimonio empresarial y la de los demás trabajadores. No hay obstáculo para entender que un ordenador

---

[35] Fue significativo el robo de datos de los participantes en el *Foro Económico Mundial de Davos*. A principios de febrero de 2001 fueron sustraídos del servidor de la Cumbre de Davos sobre la globalización los datos de los asistentes (número de pasaporte, de tarjetas de créditos, de teléfonos, direcciones, etc.) y enviados posteriormente al diario suizo *Sonntagzeitung*. Entre los asistentes afectados (unos 27.000) figuraban Clinton, Simón Peres, Madeleine Albright, Li Peng, Gianni Agnelli, Bill Gates, etc.

[36] Este fue el caso de Telefónica, que dejó al descubierto durante una hora del día 8 de marzo de 2001 los datos personales de clientes que habían contratado su servicio ADSL. Bastaba con teclear una dirección IP para acceder a un fichero en el que figuraban nombres, direcciones, números de teléfono y dirección IP del usuario (incumplía así el mandato del art. 9 LOPD sobre medidas de seguridad). A finales de ese mismo mes, era sancionada Terra por la APD con una multa de veinte millones de pesetas por otro hecho similar: la circulación en el mes de agosto de un fichero con los nombres y contraseñas de tres mil usuarios de su servicio.

[37] Me refiero exclusivamente a los hábitos de navegación, no al uso del correo electrónico, que examinaremos más adelante. Vid. J. GARCÍA y A. L. DE VAL, *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; J. LUJÁN, *Uso y control en la empresa de los medios informáticos de comunicación*, en *Aranzadi Social* 3 (2001); J. R. MERCADER, *Derechos fundamentales de los trabajadores y nuevas tecnologías*, en *Relaciones Laborales* 10 (2001); J. ESCRIBANO, *El derecho a la intimidad del trabajador. A propósito de la STC 186/2000, de 10 de julio*, en *Relaciones Laborales* 10 (2001).

debe ser asimilado a una taquilla o a cualquier otro instrumento de trabajo, de modo que podría ser inspeccionado. La cuestión es que, tal como exige el ET, debe existir también una causa que lo justifique y realizarlo en presencia de un representante de los trabajadores. El incumplimiento de estos requisitos supone que de ser llevado a efecto, estaríamos ante un atentado contra la intimidad, como estimó en Málaga la Sala de lo Social del Tribunal Superior de Justicia de Andalucía en su Sentencia 389/2000, de 25 de febrero. En este caso se 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[38].

La segunda posibilidad de atentar contra la intimidad está motivada por el control de los hábitos de navegación del trabajador por parte del empresario que ha puesto a su disposición una conexión para desempeñar su trabajo, pero por ahora no ha sido considerado como tal por los tribunales. Tal fue el caso resuelto por el Juzgado de lo Social nº 23 de Madrid, en su Sentencia de 6 de abril de 1998, confirmada posteriormente por la Sentencia 721/1998, de 16 de octubre, del Tribunal Superior de Justicia de Madrid. Lucent Technologies Network System España había despedido a uno de sus empleados en enero por sus conexiones desde el puesto de trabajo a páginas de ocio, diarios, sexo, etc., durante los meses de octubre, noviembre y diciembre de 1997, aportando la empresa datos sobre días, horas y duración de las conexiones[39]. En este

---

[38] 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».

[39] También consta como hecho probado el uso del ordenador con fines particulares completamente ajenos a la empresa, almacenando en el disco duro co-

caso concreto no se cuestionaba en ningún momento que la intimidad del trabajador hubiera resultado lesionada por la grabación de sus conexiones y su posterior revelación, sino que lo que se valoraba era la existencia de perjuicio para la red de la empresa y la no atención por parte del trabajador de las indicaciones expresas sobre el uso de internet establecidas por la misma. Efectivamente, resulta probado para los magistrados que Lucent había manifestado expresamente «su intención de sancionar disciplinariamente las navegaciones irregulares» un año antes, y dan por sentado que el modo de evitarlas es mediante unas medidas de control a través de los proxis[40].

A mi juicio, se debe establecer una diferencia entre el control del ordenador propiamente y el control del uso de Internet. En el primer caso concuerdo con los tribunales en que el ordenador es asemejable a una taquilla, por lo que el trabajador debe saber —sin necesidad de ser advertido previamente— que puede ser objeto de una inspección cuando exista una causa para ello, y que tal inspección nunca podrá suponer un atentado contra la intimidad si se realiza en su presencia y la de un representante sindical. Sin embargo, creo que en el segundo caso, en el con-

---

rrespondencia, ofertas, pedidos, etc., de negocios mercantiles en los que participaba el trabajador despedido. Esto implicaba el que se hubiera practicado un registro del ordenador de éste que el Tribunal no cuestiona en ningún momento, considerando en su Fundamento de Derecho 2º que el uso indebido es motivo suficiente para el despido.

[40] Un caso similar se produjo con el despido de una empleada por parte del laboratorio Dermofarm el 5 de abril de 2000. El Juzgado de lo Social nº 17 de Barcelona ordenaba su readmisión, pero el Tribunal Superior de Justicia de Cataluña estimaba en julio de 2001 el recurso del laboratorio por entender que quedaba acreditado que la empleada había realizado conexiones completamente ajenas a sus cometidos laborales (páginas de ocio). También en este caso quedó fuera de duda la licitud de control por parte del empresario, y que había una justificación por infringir la empleada el deber de lealtad laboral y la buena fe contractual: «es evidente que la trabajadora usó material informático de la empresa sin su autorización, abusando de este modo de la confianza depositada en ella, pues confundió lo propio con lo ajeno»; las conexiones denunciadas constituyen «una forma lúdica de ocupar el tiempo de trabajo que, a la vez que extraña a las exigencias de buena fe en que debe desarrollarse, resulta incompatible con la estricta finalidad laboral asignada a la herramienta informática de que se trata».

trol de la navegación, sí que debe ser advertido el trabajador de que se va a practicar un control de lo que haga, pues aquí ya no se trata de examinar un bien ajeno cedido para un uso determinado (una taquilla, una herramienta, etc., que pudiera entenderse comprendida en el art. 18 ET), sino una actividad que el trabajador puede creer reservada, ajena a cualquier mirada extraña y amparada por el derecho a la intimidad laboral[41]: sólo si se ha hecho saber al trabajador previamente que no existe tal reserva, sería lícito el control. Además, se precisa también una razón justificadora para materializar el control[42], de modo que debe quedar al margen la mera «curiosidad» del empresario o directivo.

III. 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[43]. Las SSTC 290/2000 y 292/2000, de 30 de noviembre, que resol-

---

[41] El Tribunal Constitucional, en su Sentencia 98/2000, de 10 de abril, es claro al admitir que una 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 concreto, en su FJ 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.»

[42] Una cosa es que quede registrada en el proxi cualquier conexión realizada por los trabajadores y otra muy distinta es la revisión efectiva de dichas conexiones por alguien en concreto.

[43] 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. Mª. J. Romero, *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; S. Rodríguez, *La intimidad del trabajador en el uso de diagnósticos médicos informatizados*, en *Revista Española de Derecho del Trabajo* 101 (2000), pp. 287-299.

vieron los recursos presentados contra la LORTAD y la LOPD, supusieron un paso definitivo en su consolidación detallada, aunque todavía podrá establecerse un marco más acorde a los nuevos avances tecnológicos cuando sea aprobada definitivamente la *Ley sobre la Sociedad de la Información y el Comercio Electrónico*.

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[44].

La Sentencia 290/2000 resolvía en realidad una cuestión de competencias, pero dejó fuera de dudas el ámbito de aplicación definitivo de 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 ser 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[45], si el Estado tenía competencias para atribuir a la Agencia de Protección de Datos y al Registro General de Datos Personales —como órgano integrado de aquella— las funciones que le otorgaba sobre ficheros de

---

[44] 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.

[45] En su FJ 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».

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 —y por tanto 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[46]. 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 (se refiere a 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»[47]. Por su parte, la Sentencia 292/2000 —como decía más arriba— tiene especial 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.

Si pretendemos fijar el origen 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

---

[46] Es rotundo en su FJ 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».

[47] Sentencia ult. cit., FJ 14º. Sin embargo, no hay inconveniente en que las Comunidades Autónomas tengan sus propias APD. Por ejemplo, Cataluña ha creado la suya mediante la Ley 2/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos (BOE nº 115, de 14 de mayo de 2002).

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[48]. 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, ...»[49]. 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 dos Directivas importantes, a las que habría que añadir una tercera que se aprobará en breve plazo y que, aun estando referida a las comunicaciones electrónicas, también contiene referencias a la protección de datos personales. 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 respecta al tratamiento

---

[48] B. RODRÍGUEZ, *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 (cfr. pp. 15-17).

[49] STC 254/1993, de 20 de julio, FJ 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*».

de los datos personales y a su libre circulación, dos años más tarde era aprobada la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. 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* 11/1998, de 24 de abril, *General de Telecomunicaciones*. Entre las normas de rango inferior, muy numerosas, tiene especial relevancia el *Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal*, aprobado por el RD 994/1999, de 11 de junio.

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[50]. 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[51]. Por ello, fue normal la preocupación que suscitó en ciertos círculos norteamericanos el

---

[50] STC 292/2000, FJ 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».

[51] 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.

lanzamiento de *Passport* por parte de Microsoft hace unos meses. El *Electronic Privacy Information Center* y otras organizaciones pro defensa de la privacidad presentaron el 26 de julio del pasado año 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 recoge información personal de los consumidores —como las contraseñas e información de las tarjetas de crédito— y las almacena en una base de datos para que el usuario no tenga que reescribirlas continuamente al realizar sus compras por Internet —se introduce automáticamente—, supone una gran comodidad para los usuarios, pero al concentrar toda la información personal de cada usuario deja abierta una puerta al tratamiento abusivo de los mismos, lo que suponía para los defensores de la privacidad una causa de alarma[52]. *Microsoft* acudió en agosto 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. A día de hoy sigue funcionando con total normalidad, aunque a finales de mayo se inició por parte de las autoridades comunitarias una investigación con el objetivo de comprobar si respeta o no las Directivas europeas sobre protección de datos. La Comisión se comprometió a presentar un informe detallado antes de que finalice el año 2002.

Para evitar que pueda resultar afectada la intimidad de este modo, las normas coinciden en establecer una serie de principios que deben regir bien en el momento de recoger

[52] 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.

los datos, bien en el momento de su tratamiento[53]. 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). Apunta H. Campuzano que todos estos principios han informado tanto las Directivas citadas como las normas nacionales, pero incurriendo en el error de proteger fundamentalmente frente a los abusos por parte del sector público y pasando de puntillas por el ámbito del sector privado[54]. Las normas deberían prever mecanismos para hacerlos efectivos en todo momento tanto frente a la Administración pública como frente a cualquier particular.

Ya vimos 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

---

[53] Cfr. H. CAMPUZANO, *Vida privada y datos personales*, cit., pp. 83-84.

[54] Op. cit., pp. 89-94. Sirva de ejemplo el caso ya citado de Comcast, en el que poco a poco se fueron recogiendo datos de los usuarios con el riesgo de elaboración de un perfil como consumidor. Más grave puede ser el procesamiento de datos genéticos, de salud, de antecedentes, etc., a efectos de considerar si puede ser rentable para la empresa realizar un contrato de seguro, o laboral, etc.

puestos en relación con otros revelan 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[55]. 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[56]. 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.

¿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 De-

---

[55] Por ejemplo, el Reglamento relativo al servicio universal de telecomunicaciones (aprobado por RD 1736/1998, de 31 de julio) establece la posibilidad de que una línea llamante no sea identificada en el aparato receptor; de este modo podemos evitar la captación de nuestro número de teléfono cuando no deseamos facilitarlo. Esta posibilidad queda excluida por el propio Reglamento cuando se llama a servicios de urgencia, medida aplicable de oficio en algunos casos según la Resolución de 30 de octubre de 2001, de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, sobre condiciones para la eliminación de marcas de supresión de identificación de la línea llamante.

[56] STC 292/2000, FJ 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.

recho, 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 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[57]. 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[58]. El 28 de enero de 2002 se aprobó la Posición Común nº 26/2002 sobre esta nueva Directiva[59], con la

---

[57] Sentencia ult. cit., FJ 17º.

[58] 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.

[59] Publicada en el DOCE C 113, de 14.05.2002, pp. 39-53.

aprobación por el Consejo de un buen número de enmiendas realizadas por el Parlamento Europeo. 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»[60].

La trascendencia de este derecho se puso de manifiesto, por ejemplo, con el aumento de los mensajes electrónicos no solicitados (*spam*)[61], que destaparon el tráfico de datos existente sin que los usuarios tuvieran conocimiento. Estas conductas, cada vez más extendidas, son constitutivas de verdaderos atentados difíciles de evitar[62] y su fin más común suele ser la venta a otras compañías bien de datos de clientes propios, bien 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. 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

---

[60] Sobre qué debe entenderse por «protección adecuada» y quién decide cuándo un tercer país ofrece tal protección, cfr. H. CAMPUZANO, *Vida privada y datos personales*, cit., pp. 111-129.

[61] El rechazo masivo supuso un cambio en el Proyecto de Ley de Servicios de la Sociedad de la Información, aprobado por el Pleno del Congreso a principios de mayo. En la primera versión del Anteproyecto se permitía el *spam* publicitario siempre que se indicara visiblemente que se trataba de publicidad; en el nuevo texto se precisará el consentimiento de los receptores y quedará prohibido el *spam*; la medida elimina esta práctica desde territorio español, aunque nada podrá hacerse contra los mensajes enviados desde el extranjero (salvo la utilización de un filtro).

[62] Un informe reciente de Jupiter MMX afirma que en 2001 los internautas recibieron una media de 571 mensajes comerciales no solicitados, estimando que podrían llegar a 1.500 diarios en 2006. La propia FTC norteamericana recibe cada día 10.000 *e.mails* reenviados por usuarios que los recibieron sin haber prestado su consentimiento. Hasta el momento, 19 Estados han impuesto leyes contra el *spam*, pero los intentos de legislar a nivel nacional se han topado con la oposición de los empresas de marketing directo. Ahora se encuentra en curso la *Controlling the Assault of Non-Solicited Pornography and Marketing* (CanSpam Act), que puede convertirse en la primera ley federal anti-spam, con sanciones de hasta medio millón de dólares y un año de prisión.

contra, prohibiendo a las compañías vender o alquilar los datos de clientes cuando para su obtención se habían comprometido a no hacerlo. 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.

Uno de los medios utilizados para conseguir los datos personales consiste en 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 es el caso de Francia, que recientemente ha modificado su legislación para autorizar las *cookies* únicamente si el usuario «ha recibido previamente una información clara y completa sobre las finalidades del tratamiento y los medios de los que dispone para oponerse a él»[63]. 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[64].

Por lo que respecta a nuestro país, entre los números publicados por la Agencia de Protección de Datos referidos al año 2001 destaca que de las 700 denuncias recibidas, 210 estaban relacionadas con el uso abusivo de In-

---

[63] 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.

[64] 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. J. A. UREÑA, *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.

ternet, fundamentalmente con el comercio electrónico online y con la e-banca. Las sanciones impuestas a las administraciones públicas y a los particulares por la APD, rondaron los 12 millones de euros, cifra similar a la del año 2000[65]. Recientemente, a mediados de mayo, se hacía pública la resolución de la APD contra la Universidad de Castilla-La Mancha por vulneración del art. 9 LOPD. La Agencia consideraba responsable a la Universidad de haber puesto en peligro la intimidad de su personal docente al acumular sus datos de navegación en un fichero que no estaba lo suficientemente protegido. El acceso a las páginas web visitadas por el profesorado era posible para personas con conocimientos informáticos, que podrían haber elaborado con estos datos el perfil de navegación de cada uno de ellos[66].

IV. El derecho al secreto de las comunicaciones

Como derecho tuvo un reconocimiento en los textos constitucionales muy anterior al derecho a la intimidad, quedando recogido 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)[67]. 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

[65] En cuanto a los cambios necesarios para controlar el uso fraudulento de datos en Internet, quizás se pueda avanzar un poco más en este terreno cuando se apruebe definitivamente la *Ley sobre la Sociedad de la Información y el Comercio Electrónico*, cuyo proyecto fue aprobado por la Cámara de Diputados a principios del mes de mayo.

[66] Los hechos habían sido denunciados por el sindicato CSI-CSIF en diciembre de 2000. Sobre el proceso seguido contra Telefónica por cláusulas abusivas sobre cesión de datos, cfr. J. A. Ureña, op. cit., pp. 142-145, donde comenta la Sentencia de 29 de noviembre de 1999.

[67] Cfr. L. Rebollo, *El derecho fundamental a la intimidad*, cit., pp. 58-60.

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»[68]. La reciente STC 70/2002, de 3 de abril, ha realizado 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, pero al menos dio a entender que no es ajeno a los avances en este terreno.

El derecho al secreto de las comunicaciones es, quizás, el que más atención ha requerido en los últimos meses, debido sobre todo a la notoriedad que algunos litigios —de carácter nacional e internacional— han alcanzado en la prensa. El primero de ellos 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[69]. 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 mismo 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[70]. La Sala

---

[68] B. RODRÍGUEZ, *El secreto de las comunicaciones*..., cit., p. 67.

[69] Vid. M. CORREA, *Libertad sindical y libertad informática en la empresa*, en *Revista de Derecho Social* 2 (1998); I. MARÍN, *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).

[70] 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 banca-

de lo Social del Tribunal Supremo decidió casar y 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[71]. Pero sí que reconoció en ella que la empresa no tiene obligación de facilitar los medios materiales de comunicación a los sindicatos y trabajadores, salvo que se hubiera pactado expresamente.

Un segundo tipo de litigio, que cobra cada día más fuerza, es el entablado por empresarios y trabajadores por el uso del correo electrónico para uso personal desde el puesto de trabajo. El de mayor trascendencia social se produjo en otra entidad bancaria, en este caso el *Deutsche Bank*, que despidió a un trabajador y amonestó a otros después de varias advertencias de uso indebido del correo electrónico. La Sala de lo Social del Tribunal Superior de Justicia de Cataluña, en su Sentencia 9382/2000, de 14 de noviembre, declaraba el despido procedente y en ningún momento se puso en tela de juicio durante el proceso la legitimidad del control empresarial, pues no había sido denunciada tal práctica por el demandante[72].

---

ria 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 encomendadas. 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».

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

[72] Tras la STSJC el trabajador sancionado interpuso recurso de casación ante el TS —en el que solicitaba unificación de doctrina— y querella contra los directivos de la entidad bancaria, a quienes imputaba la comisión del delito tipificado en el art. 197 del Código penal. Un Auto del Tribunal Supremo de 5 de enero de 2002 declaraba la inadmisión del recurso de casación; el proceso penal sigue su curso.

Un tercer caso, de carácter internacional y de importancia considerable, fue el de la famosa red *Echelon*, que volvió a reavivarse tras la confirmación de su existencia en 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, recomendaba en su exposición a los gobiernos, empresas y ciudadanos la utilización de sistemas de cifrado seguro[73]. Así como los dos casos anteriores pueden ser más discutibles, por existir razones a favor y en contra de cierto control, en este caso nunca estaría justificada una interceptación. 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[74]. 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.

A nivel nacional también hemos tenido un proceso por espionaje hasta hace escasos meses, el conocido como caso *Bitel*. La denuncia que inició este caso fue presentada en el 2000 por el Pacto de Progreso que gobierna en Baleares

---

[73] 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— afirmaba 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, y subrayaba en el informe —en relación con el respeto a la vida privada— que interceptar las comunicaciones suponía una clara injerencia en el ámbito privado de la persona, y sólo debía estar permitido cuando se tratara de garantizar la seguridad nacional, recomendando a los Parlamentos de cada nación que contaran con una comisión especial que controlara y examinara las actividades de los servicios de inteligencia.

[74] 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 los poderes de 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.

y acusaba al Ministro de Medio Ambiente, Jaume Matas, de espiar a través de otra persona el correo electrónico del ex-presidente de la Comisión Insular de Urbanismo, Francecs Quetglas. La acusación sostenía que cuando Matas presidía el Govern balear exhibió un documento interno de la Comisión de Urbanismo que le había llegado irregularmente a una dirección electrónica que gestionaba un subordinado. Transcurrido más de un año, en febrero de 2002, la Junta de Fiscales de Baleares enviaba un escrito al Fiscal General del Estado en el que se solicitaba por unanimidad la imputación del Ministro de Medio Ambiente, pero dos semanas más tarde el titular del Juzgado de Instrucción nº 9 de Palma acordaba el archivo de las diligencias al apreciar que no había indicios racionales de criminalidad contra ninguna de las personas que aparecían imputadas en la causa —la secretaria de Matas y un funcionario de Presidencia—, ni tampoco indicios que permitieran elevar las actuaciones a la Sala Segunda del Supremo para que se recibiera declaración, en calidad de imputado, al ex presidente del Govern balear[75].

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[76], pues lo que se pretende

---

[75] A juicio del magistrado, si bien era cierto que se habían reenviado correos electrónicos del socialista Francesc Quetglas a la polémica dirección electrónica, «no existen indicios racionales de que el hecho cierto y contrastado del redireccionamiento indebido hubiese sido intencionado y con la finalidad de descubrir los secretos de Francisco Quetglas o vulnerar su intimidad». Tampoco había indicios de que «aprovechándose de que se había producido el redireccionamiento mencionado, alguno de los imputados en la causa o el anterior presidente del Govern balear se hubieran apoderado de los mensajes de correo electrónico del señor Quetglas». El magistrado, atendiendo a los distintos informes periciales y a la información de la Policía Judicial, dio mayor credibilidad a la posibilidad de que el redireccionamiento fuera producto de un error debido al programa informático utilizado por la empresa, que ofrecía «una alta probabilidad de incurrir en error».

[76] Esta idea es repetida constantemente a lo largo de la obra de B. RODRÍGUEZ, *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

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[77]; combina, pues, el carácter formal y el material para realizar un juicio de valor[78]. Con

---

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).

[77] 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». *La garantía constitucional del secreto de las comunicaciones*, en «Revista Española de Derecho Constitucional» 20 (1987), p. 41.

[78] Así, podemos leer en la STC 70/2002, de 3 de abril, FJ 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 judicial *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».

ello se sitúa en una postura 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[79]. 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.

En lo que atañe a los litigios citados anteriormente, comenzaré por recoger el parecer del Tribunal Constitucional —mantenido invariablemente desde su Sentencia 114/1984, de 29 de noviembre— sobre el derecho al secreto de las comunicaciones: «rectamente entendido, el derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto»[80]. Estas

---

[79] Cfr. B. RODRÍGUEZ, *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, FJ 3º, 57/1994, de 28 de febrero, FJ 6º, 49/1996, de 26 de marzo, FJ 3º, 54/1996, de 26 de marzo, FJ 7º. En el mismo sentido y más recientes, cfr. SSTC 299/2000, de 11 de noviembre, y 17/2001, de 29 de enero).

[80] STC 114/1984, de 29 de noviembre, FJ 7º. También lo recoge literalmente la STC 70/2002, FJ 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

dos apreciaciones convierten en dudosa la legitimidad del BBVA para discriminar los mensajes sindicales dirigidos a sus empleados. Es cierto que los medios pertenecen a la empresa y cumplen un fin determinado, pero se hace necesario compaginar el uso empresarial de los medios con la libertad de las comunicaciones. 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 pudiera producirse un colapso de la red, que es lo que pretende evitar la empresa. 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. Como bien manifestó 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»[81], pero 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» con que lo venía realizando antes de ocasionar los problemas[82]. Sin embargo, el Tribunal Supremo se sitúa en una posición estricta de justicia formal: no hay precepto legal que reconozca tal derecho, no existe acuerdo entre las partes al respecto (ni si-

---

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)...»

[81] SAN 17/2001, de 6 de febrero de 2001, FJ 4º.

[82] Loc. cit., FJ 5º.

quiera tácito, como podría ser el uso pacífico previo) y tampoco existe autorización unilateral del empresario, por lo que CC.OO debe cesar en el uso de la red del banco mientras no cambie una de las tres posibilidades[83]. Los últimos convenios colectivos suelen hacer ya mención expresa de estas cuestiones, bien para conceder acceso en condiciones determinadas, bien para denegarlo[84].

Tal como lo hemos planteado hasta ahora, hemos visto la relación con la libertad de comunicaciones, pero ¿afectaría la interceptación de los mensajes por parte del BBVA también al derecho al secreto de las comunicaciones? El secreto amparado por este derecho no sólo afecta al contenido, «sino también a las circunstancias que las rodean, como puede ser la identidad de los interlocutores o el momento en que se realizan»[85]. Incluso si una de las partes hubiera dado su consentimiento expreso y concreto para la interceptación de un mensaje, sólo quedaría desprotegido por tal consentimiento el contenido, pero no las circunstancias de la comunicación que rodean al otro interlocutor y que seguirían quedando bajo el control de éste. En el

---

[83] En los FJ 2º y 3º 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 FJ 4º 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».

[84] Por ejemplo, el *I Convenio Colectivo Getronics Grupo CP S.L.*, en su Sección 10ª reconoce 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) concede acceso a la red en su art. 55, pero establece expresamente que «Los representantes de los trabajadores no utilizarán como medio de comunicación el envío de correos electrónicos a grupos de empleados».

[85] B. RODRÍGUEZ, *El secreto de las comunicaciones*..., cit., p. 68. Queda al margen de este secreto quien presta el servicio proveedor, que suele guardar una copia secreta de los mensajes para un nuevo envío en el caso de que hubiera fallado el sistema. Pero si ese servicio intentara averiguar el contenido del mensaje, sí que constituiría una injerencia ilícita (cfr. p. 74).

caso que nos ocupa, la interceptación realizada con filtros por parte del banco permite rechazar los mensajes sin acceder a su contenido, y aunque se llega a saber quién es el remitente y que el contenido es sindical, quedaría amparada la conducta por la facultad de control en el entorno laboral que corresponde al empresario.

Más complicaciones podría presentar la interceptación, por parte de la empresa, de los mensajes electrónicos de sus empleados (recibidos o enviados) desde sus puestos de trabajo y en horario laboral, pues su contenido puede estar referido a cuestiones íntimas sin relación alguna con el entorno laboral[86]. Desde que fuera aprobada en el Reino Unido la *Regulation of Investigatory Powers Act 2000,* que permitía —con ciertos límites— a las empresas británicas controlar el uso del correo electrónico desde los puestos de trabajo, la práctica de estas medidas en España levantó suspicacias tras los primeros despidos supuestamente por esta causa, como ocurrió con el empleado del *Deutsche Bank*. En este supuesto se produce un conflicto entre el derecho a la intimidad de los empleados y el de propiedad y dirección empresarial, similar al analizado anteriormente en el control del uso de Internet, aunque en éste entra también en liza el derecho al secreto de las comunicaciones.

Debemos partir de la premisa de que, al igual que ocurre con los representantes sindicales, el trabajador tampoco tiene reconocido en nuestro ordenamiento un derecho a usar de forma privada los medios tecnológicos que la empresa pone a su disposición para el desempeño de su cometido laboral, aunque tampoco impide esta posibilidad.

---

[86] MªB. CARDONA, *Correo electrónico de los empleados. Transgresión de la buena fe contractual*, en *Aranzadi Social*, T. III (2000); J. J. DE VAL ARNAL, *El correo electrónico en el trabajo y el derecho a la intimidad del trabajador*, en *Aranzadi Social*, T. III (2000); J. A. SANFULGENCIO, *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); J. I. GARCÍA, *Sobre el uso y abuso del teléfono, del 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).

La solución a este debate tendrá que venir, como aconsejan la Audiencia Nacional y el Tribunal Supremo en sus sentencias sobre el conflicto entre CC.OO y el BBVA, de la mano de una nueva regulación legal que se enfrente a estos problemas recientes, pero mientras tanto debe ser la negociación colectiva o los empleados y empresarios, en particular, los que tengan que pactar unas medidas concretas[87]. Algunas compañías disponen de normas internas sobre el uso privado de los ordenadores y de Internet, pero, de no tenerlas, sería lógico pensar que queda excluido este uso por diversas razones: coste de la utilización a cargo del empresario, utilización en tiempo de trabajo, posibilidad de transmitir información confidencial de la empresa, de transmisión de virus informáticos, de utilización de programas sin licencia, de vulneración de derechos de propiedad intelectual, de menoscabar la imagen de la empresa a través de mensajes inadecuados, etc. La trascendencia del conflicto es tal que los últimos convenios colectivos suelen contener alguna referencia expresa, como el ya citado *Convenio Mapfre, Grupo Asegurador 2002-2004*, que en su artículo 57 establece que «1º. Los empleados deben utilizar de forma adecuada los medios que la empresa les proporciona para el desarrollo de su trabajo y muy especialmente los tecnológicos. 2º. Respetando el derecho a la intimidad de las comunicaciones, existen procedimientos que permiten conocer *si dichos medios se utilizan para fines distintos a los laborales, lo que en su caso podría dar origen a las sanciones previstas en la normativa vigente*»[88].

Aunque se ha aducido que con un control empresarial resultarían afectados varios derechos del trabajador —derecho a la intimidad, al secreto y libertad de comunicaciones y libertad de expresión—, lo cierto es que la doctrina mayoritaria entiende que las medidas de control serían lí-

---

[87] SAN 17/2001, de 6 de febrero, FJ 4º: «todo ello es revelador de la necesidad de ordenar, bien por Convenio Colectivo, Acuerdo de Empresa, *ratione materiae* o norma de la jerarquía legal que corresponda, el derecho de los Sindicatos y trabajadores a la utilización de la red de la Empresa por correo electrónico para transmitir información sindical».

[88] La cursiva es mía.

citas cuando existiera una política clara de la empresa, estableciéndose un código de conducta conocido por los trabajadores y unas reglas accesibles a éstos[89]. Además, las medidas adoptadas por el empresario —que restringen derechos fundamentales— deben cumplir unos requisitos como son, en primer lugar, la idoneidad de tal medida para conseguir el objetivo propuesto, en segundo lugar la necesariedad de la misma sin que se pueda utilizar otra menos restrictiva y, por último, se exige también un equilibrio entre los perjuicios ocasionados y el bien que se produce para el interés general[90]. Por tanto, hay que descartar *a priori* que sea lícita cualquier medida de control: sólo podrán aplicarse aquellas medidas que permitan al empresario conocer el uso indebido del correo electrónico sin tener que llegar al conocimiento del contenido, aunque éste podría ser lícito en determinadas ocasiones, pues no todas la posibilidades de uso del correo electrónico desde la empresa deben tener la misma consideración.

Habría que distinguir, por tanto, entre el uso para fines particulares de mi dirección desde el trabajo («minombre@miservidor.es»), el uso de mi dirección particular pero creada para el trabajo (minombre@empresa.es) y el uso

---

[89] En febrero de 2001 iBrujula.com reproducía un comunicado de Telefónica a sus empleados sobre esta cuestión: «Aviso: Telefónica de España informa sobre la utilización adecuada del correo electrónico. Últimamente se han venido observando diversos casos de utilización incorrecta del correo electrónico entre empleados de Telefónica de España. Esta nota pretende recordar a los usuarios la política de utilización de esta herramienta, así como del resto de los recursos, tanto físicos como electrónicos, que la empresa pone a disposición de toda la organización... La finalidad del correo electrónico es facilitar la comunicación y colaboración entre los diversos grupos de trabajo. Por tanto, debe ser utilizado para fines exclusivamente laborales en el ámbito de la empresa. Ni el correo, ni el resto de medios informáticos (Internet, ordenadores, impresoras, etc.) deben ser utilizados para fines privados o particulares. Esto incluye, entre otros, todos aquellos temas relacionados con el ocio, cualquier actividad profesional fuera del ámbito de Telefónica, o la difusión de opiniones personales en temas políticos o de actualidad. A la vista de los mencionados casos de utilización indebida del correo electrónico, ha de advertirse que la empresa no va a permitir este uso inadecuado y, que por ello, ha abierto el oportuno expediente con el fin de determinar las circunstancias en que se han producido y depurar, en su caso, las responsabilidades que procedan...».

[90] Cfr. STC 186/2000, de 10 de julio, FF.JJ. 6 y 7.

con fines exclusivamente profesionales («departamentodeempresa@empresa.es»). En el primer caso nos encontraríamos más bien ante un 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[91]; 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 caso 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 ejercerse en presencia de una tercera persona. Ahora bien, 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)[92], sino por el

---

[91] 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.

[92] Afirma el Tribunal Constitucional en su Sentencia 186/2000, de 10 de julio, FJ 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 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.

derecho al secreto de las comunicaciones (garantía formal) y por mermar la libertad de autodeterminación y la dignidad en el trabajo. Así lo reconoce, por ejemplo, el Tribunal Supremo francés, que en su Sentencia de 3 de octubre de 2001 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». Así dio la razón a un ingeniero de *Nikon France* despedido en 1995 y 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»[93].

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. 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, pero 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 tener la misma consideración que una taquilla, por lo que podrían ser abiertos en presencia de un representante sindical[94]. Así como el derecho a la intimidad en

---

[93] En idéntico sentido se manifestó el Tribunal de Trabajo de Bruselas en Sentencia de 2 de mayo de 2000.

[94] En el proceso que se sigue en el Juzgado de Instrucción núm. 2 de Barcelona tras la querella del trabajador despedido por el *Deutsche Bank*, el Mº Fiscal solicitó a finales de noviembre de 2001 el archivo de la misma al considerar que el acceso al contenido como medida de control del empresario no supone conduc-

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.

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 lo empleados que tengan acceso a la misma[95]. 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.

---

ta delictiva. La acusación mantiene que el control podría haberse efectuado sobre los datos de carácter formal y con ello hubiera sido suficiente, pero al accederse al contenido se cometió el delito tipificado en el art. 197 CP. Por su parte, la titular del Juzgado decidió continuar con el proceso contra cinco directivos basando sus razonamientos en una consideración estrictamente formal del derecho al secreto de las comunicaciones: todo acceso al contenido sin previa autorización judicial supone una vulneración del derecho.

[95] 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).