EL DERECHO A LA PRIVACIDAD FRENTE AL USO JUSTIFICADO DE LOS SISTEMAS DE VIGILANCIA*

Guillermo Vicente y Guerrero
Universidad de Zaragoza

SUMARIO: 1. *La necesidad de criterios de proporcionalidad para una justa ponderación de bienes jurídicos en conflicto.* 2. *Privacidad, intimidad y protección de datos. Una línea de distinción problemática.* 3. *Fuentes de compilación de datos según su valor.* 4. *Datos obtenidos a través de medios de vigilancia individual y colectiva.* 5. *Datos obtenidos mediante sistemas de vigilancia conocida y clandestina.* 6. *Conclusiones.*

1. LA NECESIDAD DE CRITERIOS DE PROPORCIONALIDAD PARA UNA JUSTA PONDERACIÓN DE BIENES JURÍDICOS EN CONFLICTO

N la actualidad, nos encontramos en un momento del proceso histórico en el que el desarrollo tecnológico está superando amplia y peligrosamente al desarrollo normativo en la carrera de la modernidad.

En otras palabras, una considerable cantidad de aspectos surtidos como consecuencia directa de las nuevas tecnologías se encuentran hoy por hoy

* Este trabajo ha sido realizado mediante una estancia de investigación en el Research Center of Computers and Law de Oslo. Debo agradecer sinceramente la gran amabilidad y excelente disposición de todos los investigadores del centro.

carentes de la mínima regulación legal que asegure su adecuación a las necesidades sociales y a los principios básicos que rigen la convivencia en los países occidentales [1].

Uno de los ámbitos en los que la revolución tecnológica está incidiendo con más fuerza es el de la información. En el mundo de hoy, información es poder, y su obtención y utilización se han convertido en una de las metas esenciales de los principales actores de la escena social.

Súbitamente, estas ansias informativas han comenzado a socavar las garantías de intimidad y privacidad de los individuos. Como afirma el profesor Perez Luño, cada vez se está haciendo más necesario el compromiso de un acuerdo social entre el Estado y los ciudadanos por el que se limiten la utilización de los datos personales [2].

En similares términos se expresa el profesor Cascajo Castro, quien incide en la necesidad de un pacto social informático entre los distintos agentes sociales que suponga un freno al empleo abusivo de los datos por parte de los poderes públicos [3].

Sin embargo, dicho pacto social está lejos de poder ser alcanzado. Entre los aspectos más huérfanos de regulación y que a la vez más problemas plantean, tanto de índole jurídica como moral, destaca la utilización de sistemas de vigilancia y el consiguiente empleo de los datos obtenidos como fruto de ese tipo de actividades.

¿Hasta qué punto podemos decir que es lícita la utilización de estos sistemas? ¿Cabe la posibilidad de trasvasar los datos conseguidos hacia ámbitos, finalidades o aplicaciones distintas a las previstas inicialmente durante su proceso de recolección?

---

[1] Sin embargo, para algunos filósofos del derecho, uno de los rasgos distintivos de la justicia es su facilidad para ser aplicada a nuevas situaciones. «Another characteristic of the principle of the justice, which has some connection with its lack of precision, is that it has a wide and comparatively undefined area of application. It can therefore easily be transferred to new situations», Torstein Eckhoff, *Justice. Its determinants in social interaction*, Rotterdam Unisersity Press, Rotterdam, 1974.

[2] «Las sociedades actuales precisan de un equilibrio entre el flujo de informaciones... Ese equilibrio precisa de un pacto social informático por el que el ciudadano consiente en ceder al Estado datos personales, a cambio del compromiso estatal de que los mismos se utilizarán con las debidas garantías». Antonio Enrique PEREZ LUÑO, «La LORTAD y los derechos fundamentales». *Revista derechos y libertades*, núm. 1, Instituto Bartolomé de las Casas, Madrid, 1993, p. 424.

[3] «Se precisa un pacto social informático, quedando los poderes públicos obligados a utilizar los datos únicamente para los supuestos para los que éstos fueron inicialmente cedidos». Extracto de la ponencia «Problemática actual de los Derechos Humanos», leída por el profesor José Luis Cascajo Castro en la Jornada Nacional sobre Derechos Humanos, organizada en Zaragoza por el Centro de Estudios Políticos y Constitucionales Lucas Mallada el día 18 de noviembre de 1994.

El propósito de este artículo es intentar demostrar que en el aparente conflicto entre privacidad y vigilancia, lo realmente trascendente no es el sistema empleado para la obtención de los datos, sino el rango del valor o bien jurídico protegido que entra en colisión con el derecho a la privacidad de la persona objeto de la vigilancia.

Si tras una necesaria ponderación de bienes jurídicos, el rango del valor en juego resulta superior al de la privacidad, la información obtenida debería poder ser utilizada como prueba ante un tribunal, en aras de lo que tendría que ser la principal meta de los sistemas legales: la realización de la justicia concreta en los casos particulares.

Esto no quiere decir que todo sea lícito a la hora de descubrir la verdad real, la verdad material. Cierto es que dicha verdad no puede ser conseguida a cualquier precio, sino que su obtención debe limitarse en función de las exigencias establecidas en el ordenamiento jurídico. Pero no toda infracción de las normas procesales que regulan la obtención y práctica de las pruebas conducen a la nulidad de las mismas, deberán ser criterios de justicia y proporcionalidad los que, tras la ponderación de intereses, decidan si la información obtenida puede ser presentada como prueba válida ante un tribunal.

La proporcionalidad, criterio indisolublemente unido al valor justicia, deberá en todo caso exigir una correlación entre la viabilidad de la medida, su duración y las circustancias del caso particular, especialmente la naturaleza del delito que se pretende combatir mediante la vigilancia, su gravedad y la propia trascendencia social del mismo[4].

En nuestra opinión, el Derecho considerado de modo estricto y su consecuente formalismo son hoy insuficientes, y cada vez se está haciendo más necesario introducir concepciones morales y de justicia.

2. INTIMIDAD, PRIVACIDAD Y PROTECCIÓN DE DATOS, UNA LÍNEA DE DIFERENCIACIÓN DIFUSA

Para comenzar, es necesario abordar un problema previo que se nos plantea: la distinción entre privacidad, intimidad y protección de datos, una

[4] Debe igualmente evaluarse la posibilidad de descubrir el presunto delito por otros medios que puedan resultar menos traumáticos individual y socialmente considerados.

cuestión de gran importancia y que a la vez ha generado una tremenda controversia.

El punto de separación a veces se presenta difuso. De esta misma opinión ya se mostraba Hans-Peter Gassman, ex director de la Organización para cooperación económica y desarrollo de París, al manifestar que todavía en muchos países la protección de los datos es usada como un sinónimo de protección de la privacidad [5].

Para el Tribunal Europeo de Derechos Humanos el concepto de privacidad no puede ser definido de forma exhaustiva, debiendo entenderse desde una perspectiva amplia [6], ya que se incurriría en un error manifiesto si se limitara a una esfera de intimidad personal de la que se excluyera absolutamente el mundo exterior.

El profesor Ruiz Miguel afirma, sin embargo, que es posible deducir de las sentencias dictadas por dicho Tribunal [7] una diferencia destacable entre las nociones de privacidad e intimidad: el mayor ámbito de alcance de aquélla con respecto a ésta, distinguiendo distintos niveles de intimidad dentro de la privacidad [8].

No obstante, otros autores se atreven a exponer una línea clara de diferenciación. Así, el profesor Jon Bing, el autor de mayor prestigio en temas de informática jurídica en Escandinavia, entiende la privacidad como una protección general contra toda invasión indebida contra la persona (sus cartas, su domicilio, sus llamadas telefónicas...), mientras que la protección de datos es algo más limitado y se refiere al control moderno de los archivos informatizados [9].

La doctrina italiana, encabezada por el profesor Vittorio Frosini, define a su vez la privacidad como el retiro temporal de un sujeto que se separa de la

---

[5] «The disiding line between privacy protection and data security has become thinner. Sometimes the term data protection is also used to cover data secutity, especially in those countries where data protection is used as a synonym of privacy protection». HANS-PETER GASSMANN, *Transnational Data and Communications Report*, Washington, noviembre 1989, p. 20.

[6] STEDH Niemitz. A 251-B, núm. 36.

[7] Ver especialmente STEDH Costello-Roberts, A 247-C, núm. 36, que hace referencia a ciertas actividades desempeñadas por miembros de profesiones liberales que pueden considerarse dentro del ámbito de la privacidad.

[8] «De esta última afirmación es posible deducir que el TEDH distingue entre intimidad y vida privada, o que al menos diferencia diversos grados de intimidad dentro de la vida privada, que sería un concepto de cierta amplitud y de un alcance mayor del que tendría el concepto de intimidad», CARLOS RUIZ MIGUEL, *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, Civitas, Madrid, 1991, pp. 34-35.

[9] Ver JON BING. *Privacy and surveillance systemsi*, The International Computer Lawyer, Septiembre, 1993, p. 18.

sociedad voluntariamente a través de todo tipo de medios psicológicos o físicos.

Por intimidad entiende aquella fase de la privacidad en la que el sujeto se encuentra situado en un grupo reducido en el que caben una serie de relaciones como las derivadas de la esfera familiar o conyugal [10].

En Gran Bretaña, ya a comienzos de la década de los setenta, se establece mediante el llamado «Informe Younger sobre la intimidad» [11] una interesante diferenciación entre intimidad física e intimidad informativa.

En concreto la intimidad física supondría la plena libertad del individuo frente a toda intromisión sobre su persona, familia o domicilio, mientras que la intimidad informativa se definiría como aquel derecho de que goza el sujeto para poder delimitar por sí mismo el flujo de informaciones sobre sí mismo que está dispuesto a comunicar a otros.

Es sin embargo destacable la ausencia de referencias tanto en la doctrina como en la propia jurisprudencia británica del concepto de privacidad, llegándose incluso a rechazar de plano por algunos de sus más prestigiosos autores [12].

Todo lo contrario ocurre con la doctrina estadounidense, que desde la publicación del pionero libro de Alan F. Westin *Privacy and Freedom* [13] a finales de la década de los sesenta la proliferación de estudios sobre intimidad y privacidad se han sucedido constantemente.

Imprescindibles referencias son los trabajos de Samuel D. Warren y de Louis D. Brandeis [14], en los que analizan el derecho a la privacidad frente a la amenaza de la prensa y su capacidad de lesionar la vida privada de los sujetos.

La noción de privacidad derivada de la línea doctrinal mayoritaria [15] entiende este derecho como control de las informaciones que nos conciernen a nosotros mismos, por encima incluso de aquellos que lo entienden como ausencia de información sobre nosotros por parte del resto de los individuos.

---

[10] Debemos recordar aquí la interesante diferenciación en fases que realiza Frosini al distinguir cuatro etapas dentro de la privacidad: soledad (imposibilidad física de contactos materiales), intimidad (pequeñas relaciones en grupos reducidos de carácter familiar), anonimato (exposición al contacto con personas no deseadas) y reserva (creación psicológica de obstáculos para evitar intrusiones). Ver VITTORIO FROSINI, *Il diritto nella società tecnologica*, Giuffrè, Milán, 1981

[11] Publicado en Inglaterra en julio de 1972, supuso un importante avance, extendiéndose con rapidez su influencia entre los países de cultura anglosajona.

[12] Ver P. STEIN y J. SHAND, *Legal Values in Western Soeiety*, Edimburgh University Press, Edimburgo, 1978.

[13] Alan F. WESTIN, *Privacy and Freedom*, Atheneum, Nueva York, 1967

[14] En especial «The right to privacy», *Harvard Law Review*. 15 de diciembre de 1980, pp 193 y ss.

[15] Ver en este sentido CHARLES FRIED, «Privacy», *YLJ*, núm. 77, 1968.

Por su parte la doctrina alemana distingue entre la *Intimsphäre*, la *Privatsphäre* y la *Individualsphäre*. La *Intimsphäre* se refiere a la esfera de lo secreto, a todas aquellas noticias y sucesos que el sujeto desea que no sean objeto de comunicación exterior. La *Privatsphäre* incide en todas aquellas facetas íntimas que están integradas en la vida familiar y conyugal del individuo. La *Individualsphäre* equivale a los aspectos que comprenden la peculiaridad del individuo (como pueden ser la propia imagen o el honor).

En España la polémica, aunque relativamente reciente, está provocando una abundante literatura. El profesor Albaladejo entiende la intimidad como el poder que tiene el individuo sobre las actividades que se consideran integradas dentro de su círculo íntimo, por lo que puede verse libre de intromisiones y publicidades no deseadas [16].

Otros autores, sin embargo, se muestran reacios a definir intimidad y privacidad, prefiriendo hacer una enumeración de contenidos posibles [17], lo que tiene inconvenientes tan grandes como su necesaria variación en el tiempo o la incapacidad del legislador para poder tipificarlos todos, por lo que en principio me parece inaceptable esta solución [18].

El profesor Pablo Lucas Murillo de la Cueva identifica la defensa de la personalidad como el bien jurídico a proteger, si bien se equivoca a mi entender al identificar el concepto de intimidad con la noción anglosajona de *privacy* [19], concepto que cubre un mayor ámbito que el de la intimidad y que para nosotros correspondería a la privacidad [20].

La Ley Orgánica 1/1982, de 5 de mayo, de Protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, tipifica en su artículo 7 como ilícito civil la intromisión a la intimidad, enumerando los cuatro tipos de intromisiones ilegítimas que pueden atentar contra el derecho a la

---

[16] «Poder concedido a la persona sobre el conjunto de actividades que forman su círculo íntimo, personal y familiar, poder que le permite excluir a los extraños de entrometerse en él y de darle una publicidad que no desee el interesado.» JOSÉ LUIS ALBALADEJO, *Derecho Civil*, t. I, vol 2.º, Barcelona, 1985, p. 65.

[17] Ver LUIS MARÍA FARIÑAS MANTONI, *El derecho a la intimidad*, Madrid, 1983.

[18] No obstante la enumeración de tipos es práctica común y deseable en el derecho penal, lo que no es óbice para que nos mostremos en desacuerdo con su utilización fuera de ámbitos estrictamente penales.

[19] «En general, las aproximaciones que se han hecho y continúan haciéndose sobre la protección del individuo frente a los peligros dimanantes de la informática parten del concepto de la intimidad o *privacy*. Ahora bien, está claro que dicho concepto puede ser entendido con mayor o menor amplitud según el contexto en el que sea considerado.» PABLO LUCAS MURILLO DE LA CUEVA, «La protección de los datos personales ante el uso de la informática», *Revista de la Facultad de Derecho de la Universidad Complutense*, núm. 15, Madrid, 1989, pp. 604.

[20] Si bien hay que destacar el hecho de que este término, el de privacidad, todavía no se encuentra en nuestro diccionario de la lengua.

intimidad [21], derecho que no se encuentra definido en ninguna parte de esta desafortunada ley [22].

Por su parte, el Tribunal Constitucional en el fundamento jurídico tercero del Auto 342/1986 destaca la considerable extensión que ha experimentado la protección al derecho a la intimidad equiparándolo de nuevo erróneamente al derecho a la privacidad.

De indudable interés resultan sin embargo las aportaciones del profesor O'Callaghan Muñoz, quien destaca el hecho de que el concepto de intimidad debe ser definido doctrinalmente pese a su falta de claridad, provocada sin duda por el hecho de que si la intimidad se centra en un círculo íntimo de la persona, este concepto variará según sea la actividad a la que se dedique el sujeto en cuestión [23].

Es por ello que si tomamos en consideración la proyección pública de las actividades de los individuos, el círculo de intimidad de dichos sujetos va decreciendo proporcionalmente conforme aumenta el grado de proyección de sus actividades públicas, porque a la generalidad de las personas afectadas por las actuaciones públicas no se les puede poner el freno de la intimidad de las personas públicas, ya que pueden verse muy negativamente perjudicados.

Ha sido la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal [24] la que ha entrado de lleno en el asunto diferenciando intimidad y privacidad, entendiendo por la primera las facetas más reservadas del ser humano (domicilio, comunicaciones...) y definiendo la segunda como aquellas facetas de la vida humana que

---

[21] «Tendrán la consideración de intromisiones ilegítimas: 1. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas... La utilización de dichos aparatos... 3. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de las cartas, memorias u otros escritos personales de carácter íntimo... 4. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela...»

[22] En mi opinión, se perdió una gran ocasión de avanzar con esta ley que se limita a enunciar los tipos de violación o atentado contra el derecho a la intimidad.

[23] «... si el concepto de intimidad se centra en la idea de círculo íntimo, que es preservado por el derecho a la intimidad, este concepto varía según la persona y, no tanto en sí misma, sino en razón de su profesión o cargo...». XAVIER O'CALLAGHAM MUÑOZ. «Derecho al honor, a la intimidad y a la propia imagen», en el volumen colectivo *XII Jornadas de estudio, Los Derechos Fundamentales y Libertades Públicas (I)*, vol. I, Ministerio de Justicia, Madrid, 1992, p. 577.

[24] Ley Orgánica 5/1992, de 29 de octubre, publicada en el «BOE» núm. 262, de 31 de octubre de 1992.

consideradas individualmente carecen de importancia, pero que coherentemente unidas pueden reflejar un retrato de la personalidad del individuo que éste está legitimado a ocultar [25].

La situación se presenta compleja, entendiéndose como hemos visto de manera diferente los mismos conceptos dependiendo del país que se trate. Este es uno de los principales problemas que es necesario denunciar: la falta de uniformidad entre los distintos países.

En cualquier caso, esta falta de uniformidad podemos disculparla en parte por las diferentes tradiciones legislativas de las distintas naciones, por las siempre inevitables diferencias terminológicas y de lenguajes y por el distinto grado de tecnología entre unas sociedades y otras [26].

Sin embargo, es destacable la buena disposición que en los últimos años está demostrando el Consejo de Europa [27], consciente del desarrollo cada vez mayor de los servicios de carácter público y de la progresiva tecnificación de las distintas sociedades de los Estados miembros que lo integran, lo que provoca una creciente demanda de datos de carácter personal cuya obtención atenta a veces frontalmente contra los derechos a la intimidad y a la privacidad.

Pero el Consejo de Europa es igualmente consciente de que la fórmula más adecuada para intentar resolver todos estos problemas debe tomar en consideración la necesidad de una auténtica colaboración permanente entre los distintos gobiernos de los Estados miembros [28].

---

[25] La Ley Orgánica española 5/1992 considera la privacidad como el objeto esencial de protección en su regulación sobre el tratamiento automatizado de los datos personales. Según ésta, la intimidad se encontraría protegida por las previsiones del artículo 18 de la Constitución.

[26] En este sentido, JACQUES FAUVET, ex presidente de la Comisión nacional de informática de Francia, hace ya varios años que realizaba constantes llamamientos a la cooperación entre países en estas materias. «Such trends make international cooperation and the exchange of information between commissions necesary now more than ever before...», *Transnational data and Communications Report.*, Washington, noviembre 1989, p. 17.

[27] Especialmente elogiables fueron sus trabajos y negociaciones en la Convención para la protección de los individuos de cara al tratamiento automático de datos de carácter personal, conocida como Convención 108, que trataremos en el epígrafe quinto de este mismo artículo.

[28] De la misma opinión, entre otros, se muestra EGBERT J. AUSEMS, secretario del Consejo de Europa para la protección de las personas frente al tratamiento automatizado de los datos personales. «Asimismo, para el Consejo de Europa la protección de datos de carácter personal aparece como una de las actividades en las que la cooperación intergubernamental permanente es necesaria.» Ver «La protección de las personas frente al tratamiento automatizado de los datos personales en el marco del Convenio 108 del Consejo de Europa», conferencia pronunciada en las jornadas sobre Informática Judicial y Protección de Datos Personales los días 7 y 8 de octubre de 1993 en San Sebastián y publicada por el Departamento de Justicia del Gobierno Vasco en el volumen colectivo *Informatica Judicial y Protección de Datos Personales*, Vitoria, 1994, p. 27.

Visto todo lo anterior, y ante la necesidad de clarificar, nos vemos obligados a adoptar aquí nuestras propias definiciones de protección de datos, de intimidad y de privacidad.

Entenderemos en este artículo por protección de datos toda actividad que tenga como objetivo la salvaguarda de datos personales almacenados en archivos informatizados.

La privacidad será para nosotros todas aquellas facetas de la vida de la persona (independientemente de su posible importancia o valor) que todo individuo tenga derecho a mantener reservadas.

Por último, entenderemos por intimidad las facetas de la vida humana que proporcionan datos de especial valor o consideración sobre la persona (por ejemplo datos concernientes a la ideología, a las creencias religiosas o a la salud).

3. FUENTES DE RECOLECCIÓN DE DATOS ATENDIENDO AL VALOR DE LOS MISMOS.

La diferenciación que he realizado en el apartado anterior distinguiendo intimidad y privacidad por el valor de los datos que ambas protegen es de una considerable importancia.

Los datos sin valor tomados individualmente encuentran en la privacidad el medio de protección más idóneo. Son datos sin una importancia intrínseca y su tratamiento y almacenamiento informatizado es sencillo. A menudo suelen ser utilizados como modelos.

Los datos con valor son susceptibles de múltiples clasificaciones. Nosotros adoptaremos en este artículo una propia distinguiendo tres tipos bien diferenciados: los datos sensibles, los datos con valor de mercado y los datos obtenidos mediante sistemas de vigilancia.

Los datos sensibles surgieron fruto de la polémica iniciada en la década de los setenta sobre la existencia de una serie de datos personales que debían ser objeto de una protección específica como consecuencia de su especial vulnerabilidad. La doctrina fue dándose cuenta de que la utilización incontrolada de determinados datos podía desembocar en decisiones especialmente desfavorables para los distintos sujetos.

Pronto en los países escandinavos, Gran Bretaña y Francia comenzaron a arbitrarse normas de protección especial para una serie restringida de datos de

una naturaleza determinada: datos relativos a las creencias religiosas, a la ideología, a la raza, a las opiniones políticas, a la vida sexual y a la salud.

El Convenio 108 del Consejo de Europa [29] recoge la protección de dichos datos de naturaleza especial en su artículo 6, en el que concede la posibilidad de obtener y registrar estos datos en aquellos casos en los que el Derecho interno ofrezca las garantías adecuadas. Es por ello que las diferentes legislaciones nacionales de los Estados miembros se diversifican a la hora de reconocer dichas garantías.

En su artículo 7, el Convenio 108 realiza una diferenciación en mi opinión desafortunada, al distinguir dentro de los datos sensibles lo que podríamos llamar dos niveles de sensibilidad: un primer nivel compuesto por los datos personales altamente sensibles (que estarían integrados por los datos referentes a las creencias religiosas y a la ideología), y un segundo nivel compuesto por los datos personales referentes al origen racial, a la vida sexual y a la salud.

En nuestro país, la Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal secunda esta diferenciación, estableciendo en su exposición de motivos que los datos personales referentes a las creencias religiosas y a la ideología únicamente estarán disponibles con el consentimiento expreso y por escrito del afectado [30], mientras que los datos personales que afecten a la raza, a la salud y a la vida sexual sólo podrán ser obtenidos mediante dicha aceptación por parte del sujeto afectado o a través de una habilitación legal expresa [31].

Esta distinción, sin duda influenciada por el artículo citado del Convenio 108, no se basa en ningún criterio lógico, sin estar en absoluto claro que en la sociedad occidental actual los datos referentes a las creencias religiosas de los individuos necesiten una mayor protección que los datos referidos al origen racial o a la vida sexual [32].

---

[29] Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Este Convenio fue ratificado por España tres años más tarde, el 7 de enero de 1984, publicándose en el «BOE» de 15 de noviembre de 1985.

[30] Contra los datos relativos a creencias religiosas e ideología no pueden realizarse ningún tipo de invasiones, ya que se chocaría frontalmente contra lo dispuesto por el articulo 16 de nuestra Constitución.

[31] Lo que abre peligrosamente el campo a posibles excepciones en aras de un mal entendido interés general.

[32] De la misma opinión se confiesa el Magistrado de la Sala Segunda del Tribunal Supremo José Antonio Martín Pallín, quien afirma textualmente: «... no se debe de ninguna de las maneras el primar a los datos de ideología, religión y creencias sobre los de origen racial y los de hábitos o vida sexual». JOSÉ ANTONIO MARTÍN PALLÍN, «La Ley Orgánica de Regulación del tratamiento automatizado de datos de carácter personal. Una visión crítica», en el volumen colectivo *Informática Judicial y protección de Datos Personales*, *op. cit.*, p. 88.

Los únicos datos que personalmente opino que sí que son susceptibles de una regulación específica atendiendo a su especial naturaleza son los referentes a la salud, ya que pueden darse circunstancias en las que estos datos sean indispensables para resolver un caso urgente o para establecer un tratamiento médico.

En definitiva, podríamos definir los datos sensibles como aquellos que necesitan una protección especial, encontrando en la intimidad el cauce de protección más favorable. Son datos de verdadera importancia. y hacen referencia a las creencias religiosas, a la raza, a la ideología, a la vida sexual, a la salud y a las posibles condenas penales.

No obstante, estos últimos, los datos referentes a posibles condenas criminales anteriores, inexplicablemente no se encuentran contenidos en nuestra LORTAD con la consideración de datos sensibles, lo que personalmente considero una grave omisión. Estos datos sí que son recogidos en otras regulaciones europeas, siendo reveladora su inclusión dentro del artículo 6 del Convenio 108 del Consejo de Europa [33].

Los datos con valor de mercado son aquellos obtenidos mediante encuestas, estadísticas y prospecciones de mercado. Actualmente, el poder y la fuerza de las empresas suelen encontrar como canon de medición la calidad y cantidad de sus informaciones. Son datos de un gran valor para las distintas empresas del sector, pero para el resto de los ciudadanos no dejan de ser meras informaciones sin valor.

El mayor problema que plantean la recolección y utilización de estos datos es la tendencia cada vez más acusada a generar prácticas abusivas encaminadas a obtener los datos por cualquier medio posible aunque puedan en determinados momentos infringir claramente la privacidad de los ciudadanos.

Se ha llegado incluso a un punto en el que los individuos están viéndose contaminados constantemente por un cúmulo de datos de inequívoca intención consumista a los que no se pueden enfrentar [34].

Para intentar regular en la medida de lo posible esta situación, la LORTAD establece que todas aquellas empresas cuyas actividades se dediquen fundamen-

---

[33] Dicho artículo concede a los datos referentes a condenas criminales anteriores el mismo trato que al resto de datos personales sensibles, remitiendo el artículo 2.3 c) la regulación de dichos datos a los correspondientes artículos del Código penal y al Real Decreto 202/1983, de 28 de julio.

[34] El profesor PÉREZ LUÑO destaca el hecho de esta tremenda contaminación informativa, señalando textualmente: «... el ciudadano normal es el que acepta gustoso la contaminación de su vida privada por los intereses consumistas de los mercaderes de publicidad. El ciudadano insólito será aquel que se obstine en salvaguardar su derecho fundamental a la intimidad y se autoconfina en un aislamiento parangonable al sufrido por Robinson en su isla solitaria», *op. cit.*, p. 417.

talmente al reparto de documentos, recopilación de direcciones, publicidad o venta directa podrán utilizar los datos de los ciudadanos exclusivamente cuando figuren en documentos que sean accesibles al público, cuando hayan sido facilitados por los afectados o cuando éstos hayan dado su consentimiento [35].

El problema surge al continuar esta ley manifestando que corresponde a los interesados darse de baja de los correspondientes ficheros a su simple solicitud [36].

Esta solución creo que es de todo punto inadmisible, ya que en realidad la ley está invirtiendo la carga de la prueba, obligando a los individuos que no quieran ver incluidos sus nombres y direcciones en las listas de las empresas comerciales a borrarse de las mismas, en vez de ser las propias empresas las que prueben el consentimiento de los individuos cuyos datos aparecen reflejados en sus listas comerciales.

El tercer tipo de datos con un posible valor son los obtenidos mediante sistemas de vigilancia. Los datos conseguidos a través de estos medios van a ser objeto de nuestro estudio en este artículo, dejando los sensibles y los de mercado para trabajos posteriores [37].

Distinguiremos medios de obtención de datos a través de procesos de control individual y colectivo por un lado y sistemas de recolección de datos mediante procesos de vigilancia conocida y clandestina por otro lado.

4. DATOS OBTENIDOS MEDIANTE SISTEMAS DE VIGILANCIA INDIVIDUAL Y COLECTIVA

Como ya señalé al principio del trabajo, el objeto principal de éste reside en intentar demostrar que la vigilancia no puede ser justificada según el medio empleado para llevarla a cabo, sino única y exclusivamente a través de una ponderación de bienes jurídicos que sirva para calibrar si el rango del valor protegido por la vigilancia es superior al rango que ostenta la propia privacidad [38].

---

[35] Ver artículo 9.1 de la LORTAD, en el que se regulan los ficheros con fines de publicidad.

[36] «Los afectados tendrán derecho a conocer el origen de sus datos de carácter personal, así como a ser dados de baja de forma inmediata del fichero automatizado, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud», artículo 9.2 de la LORTAD.

[37] Interesantes reflexiones sobre todos estos aspectos pueden encontrarse en JON BING, «Data protection in a time of changes», *Information Law Series*, 1994, pp. 247-259.

[38] Nótese pues que el ámbito de estudio de este trabajo se va a centrar en el concepto de privacidad y en su presumible conflicto con la utilización de sistemas de vigilancia, dejando a un lado, una vez realizada su distinción, las nociones de intimidad y de protección de datos.

Esto no quiere decir, por supuesto, que el fin justifique los medios, pero sí que existen medios para lograr una información cuya finalidad sea proteger un bien jurídico superior a la privacidad que deben ser admitidos, aun cuando por dichos sistemas pueda socavarse la privacidad de la persona vigilada.

Para ello nos basaremos en una serie de casos reales juzgados por los tribunales de Estados Unidos, Noruega, Alemania y Suecia, países en los que ya existe una importante tradición judicial en este tipo de materias. Como muestra de la actividad de los tribunales españoles comentaremos aquí el famoso «caso Naseiro», una de las sentencias pioneras en nuestro país sobre estos problemáticos temas.

Para demostrar que la utilización de los datos obtenidos por estos sistemas puede ser correcta, e incluso servir de prueba ante un Tribunal, dependiendo del rango del valor defendido y no del sistema de vigilancia empleado, vamos a presentar en cada caso un ejemplo en el que estaría justificado el uso de esos datos y un ejemplo en el que no.

Comenzaremos con la posible utilización de datos obtenidos como fruto de medios de vigilancia individual. Estos sistemas pueden ser caracterizados como aquellos que se emplean para confirmar una sospecha que se ha conseguido mediante el uso de otros medios anteriores y distintos.

Un caso en el que la vigilancia individual fue deplorable y debió ser rechazada, cosa que no ocurrió, se dió en 1990 en los Estados Unidos en el caso USA *v.* Mitchell [39].

En éste, miles de personas rellenaron un formulario para una empresa publicitaria sobre sus tendencias sexuales, sin ser informados previamente de que dicha empresa era en realidad de propiedad estatal.

Con posterioridad, todos los datos de la encuesta fueron puestos a disposición del Gobierno, quien advirtió que uno de los entrevistados había manifestado sus tendencias hacia la pornografía infantil. Al estar penadas estas prácticas en la legislación americana, el Gobierno decidió enviar por correo toda una serie de fotografías de niños desnudos al domicilio particular de la persona encuestada.

Tras el envío de esas fotografías, la policía efectuó un registro con la única finalidad de encontrar pruebas sobre las tendencias sexuales de aquel individuo. Como no encontraron otras evidencias, esas fotografías fueron utilizadas más tarde como el medio de prueba para llevar a juicio a esa persona [40].

---

[39] USA *v.* Nritchell, 88-5063. 59 USA Law Week 2263 (1 octubre 1990).

[40] Para más información sobre este escandaloso caso, ver Privacy Journal, noviembre 1990.

Independientemente de lo deplorable de las desviaciones sexuales de ese sujeto, resulta claro que el uso que se hizo de esas fotos no estaba en absoluto justificada. El valor que se pretendía salvaguardar, la decencia, la mera rectitud sexual (puesto que en ningún momento se produjo corrupción de menores), no estaba por encima de la privacidad de tal individuo. Pese a ello, las fotografías fueron admitidas como prueba por el Tribunal de primera instancia.

Sin embargo, un caso en el que la utilización de datos obtenidos a través de sistemas de vigilancia individual fue completamente correcta a mi entender tuvo lugar en la ciudad alemana de Hamburgo.

La policía germana había conseguido mediante toda una serie de investigaciones previas los lugares en que se daba cita uno de los terroristas más peligrosos del país, Rudolph Clemens Wagner[41].

Este terrorista fue sometido a una auténtica vigilancia constante, socavando repetidamente por parte de la policía su derecho a la intimidad y a la privacidad. Unos días más tarde, mediante dicho control, la policía consiguió las pruebas necesarias para ser llevado ante los Tribunales.

En este caso, la vigilancia y el posterior empleo de los datos obtenidos como medio de prueba frente a un Tribunal estaban perfectamente justificados, ya que el valor protegido, la seguridad nacional, es de rango inequívocamente superior al de la privacidad de un delincuente.

En cuanto a la vigilancia colectiva, ésta puede ser definida como aquella que recae sobre una serie de sujetos que no han sido identificados con anterioridad, de lo que se deriva, a diferencia de los casos anteriores, la inexistencia de datos previos en la construcción de la sospecha.

Un muy interesante ejemplo en el que dicha vigilancia estuvo plenamente justificada lo podemos encontrar en USA *v.* Sokolow, asunto de gran importancia que llegó hasta la Corte Suprema de los Estados Unidos[42].

En éste, las computadoras dieron un perfil del típico traficante de drogas. Dicho perfil fue utilizado para detener a un cierto número de personas en un aeropuerto norteamericano, con tan buena suerte de que una de las detenciones identificó a un importante traficante de drogas.

El asunto llegó hasta el Tribunal Supremo, que por una mayoría de 7-2 confirmó la legalidad de la redada. En este caso, de nuevo la salud pública es un valor que ocupa un puesto más alto en la jerarquía que el de la privacidad.

---

[41] Ver K. V. Russell (editor), *Yearbook of Law, Computers and Technology*, Londres, 1991. pp. 164-177.

[42] USA *v.* Sokolow. 87-1295 (4 de abril).

El Tribunal Supremo norteamericano argumentó, no obstante, que la vigilancia y posterior redada estuvieron basadas no en perfiles informáticos, sino en observaciones personales que aumentaron considerablemente lo razonable de la sospecha [43].

Sin embargo, como muestra de vigilancia colectiva injustificada podemos citar el incidente de la Swedish Kungsbacka, en el que unas computadoras identificaron en Estocolmo a una cantidad elevada de personas (alrededor del millar), como culpables de fraude a la seguridad social sueca.

Estos ordenadores, propiedad de la Administración sueca, se basaron en una serie de datos incompatibles que con posterioridad se demostraron erróneos.

El caso se complicó todavía más al existir en el país escandinavo una norma que dice que nadie puede ser acusado basándose únicamente en pruebas informatizadas.

Después de las investigaciones pertinentes, sólo un número no superior a la decena fueron definitivamente condenados como causantes de fraude, absolviéndose al resto tras un minucioso estudio de todos sus datos privados y personales, lo que originó unas tremendas polémicas al ser considerado por la población sueca la actuación de la Administración como una flagrante socavación de su derecho a la privacidad [44].

5. DATOS OBTENIDOS MEDIANTE SISTEMAS DE VIGILANCIA CONOCIDA Y CLANDESTINA

Durante el apartado anterior he intentado mostrar que tanto los sistemas de vigilancia individualizada como los de colectiva se justifican según el rango del valor que defienden en su conflicto frente a la privacidad, siempre que la realización de la vigilancia no socave otros valores fundamentales superiores al «status» del bien jurídico protegido.

Este mismo esquema voy a seguir a continuación para referirme a los sistemas de vigilancia conocida y clandestina.

Los procesos de vigilancia conocida son aquellos que el sujeto objeto de la vigilancia o bien conoce o bien debería conocer, por estar dicho conocimiento dentro de unos cauces lógicos y razonables.

---

[43] Ver Privacy Journal, abril de 1989.

[44] Este desafortunado suceso puede encontrarse dentro de las memorias del entonces director de la Agencia de Protección de Datos sueca, JAN FREESE. *Den maktfullkomliga oformogan*, Wahlstrom och Widstrand, Estocolmo, 1987.

Un significativo ejemplo de vigilancia conocida justificable acaeció en la ciudad noruega de Stavanger [45].

Un ladrón entró en una casa cogiendo gran cantidad de objetos valiosos y dándose a la fuga robando además el coche que utilizó para escapar. Sin embargo, cometió la imprudencia de conducir a excesiva velocidad y a causa de ello fue fotografiado por dispositivos de control de tráfico, apareciendo en la fotografía el ladrón conduciendo un coche que no era suyo con parte de los objetos robados en los asientos traseros.

El delincuente, pese a no conocer el lugar de localización exacta del sistema automático de vigilancia, sí debía estar enterado del peligro que corría al respecto si se excedía conduciendo a demasiada velocidad.

No obstante, el Parlamento noruego en la sesión 1986-1987 había dado un decreto regulando el control de tráfico por medio de sistemas automáticos, explicitando que las fotos resultantes no podrían usarse nada más que para infracciones de tráfico.

Durante el consiguiente juicio contra el ladrón, el fiscal presentó la foto conseguida como consecuencia de la infracción de tráfico, y ésta fue aceptada como prueba del delito.

La defensa recurrió, pero la Corte Suprema noruega ratificó la foto como prueba, aun desoyendo las instrucciones del decreto, ya que por encima de éste se encontraban las leyes criminales procesales.

El Tribunal Supremo no entró en el fondo del asunto, pero esto ya lo había hecho el Tribunal inferior, considerando acertadamente que la justicia social ante un caso de delito flagrante contra la propiedad se encontraba por encima de la privacidad del delincuente.

Nuevamente pues, vuelve a plantearse la dicotomía entre seguridad jurídica y justicia. Afortunadamente, en este caso, los tribunales optaron por la segunda [46].

Sin embargo, un claro ejemplo en el que la vigilancia es conocida pero injustificada se produjo en los Estados Unidos en 1982, en el caso Schowengerdt *v.* General Dynamics [47].

---

[45] El caso fue publicado en Norsk Retstidende 1990, 1008, y es discutido en JON BING, *Privacy and surveillance systems, op. cit.*

[46] De la misma opinión favorable a primar las concepciones de justicia sobre la propia seguridad jurídica se muestra Vilhem Aubert: «The veredicts, would raise expectations with respect to the outcome in new cases, which could not be fulfilled without violating considerations of concrete justice». VILHEM AUBERT, «The structure of legal thinking», Legal Essays. A tribute to Frede Castberg, Universitetsforlaget, Oslo, 1963, pp. 41 y ss.

[47] Schowengerdt *v.* General Dynamics, 823 F 2d 1328 (9 th Cir. 30 de julio de 1987).

La polémica fue realmente grande a lo largo del juicio. En principio, se preveía que la línea jurisprudencial sobre el derecho a la privacidad iniciada por el Tribunal Warren en Griswold *v.* Connecticut [48] y en Lovina *v.* Virginia [49] iba a influir poderosamente en el veredicto del Tribunal, mas como a continuación veremos se produjo el efecto contrario.

Los hechos son los siguientes: un marino homosexual se sintió objeto de una vigilancia estrecha debido a suposiciones sobre sus tendencias sexuales. Dicha vigilancia llegó al extremo de contratar la propia Marina a un agente especial para que consiguiera pruebas suficientes sobre las inclinaciones sexuales del marino.

El agente no sólo no ejerció una presión intimidatoria sino que incluso le incautó en el escritorio de su oficina correspondencia y fotografías privadas.

El Tribunal cometió, en mi opinión, el tremendo error de declarar que el sujeto no tenía derecho a la privacidad en su oficina, porque el escritorio pertenecía a la Marina [50].

Independientemente de lo desacertado de esta desafortunada sentencia, influenciada tal vez por la legislación de los Estados Unidos referente a la prohibición de reclutar en las filas de la Marina a homosexuales [51], resulta obvio que la privacidad de las personas se encuentra muy por encima del interés de los dirigentes de las empresas e instituciones en conocer las inclinaciones sexuales de sus empleados.

A continuación vamos a abordar la, a mi juicio, más problemática esfera: la utilización justificada de datos obtenidos mediante sistemas de vigilancia clandestina, esto es, aquella que es realizada sin el conocimiento de la persona objeto de dicha vigilancia.

En la actualidad, este tipo de vigilancia se suele realizar a través de sistemas electrónicos, siendo el instrumento más utilizado la cámara de vídeo, la cual plantea como veremos a continuación innumerables problemas fundamentalmente relacionados con las grabaciones de los empresarios en el lugar de trabajo controlando a sus empleados.

---

[48] Griswold *v.* Connecticut, 381 US 479 (1965). Esta sentencia puede afirmarse que inicia el derecho a la privacidad en los Estados Unidos, al autorizar la utilización y venta de anticonceptivos.

[49] Loving *v.* Virginia, 388 US 1 (1967). En esta sentencia el Tribunal anuló la ley vigente por entonces que prohibía los matrimonios entre cónyuges de distinta raza.

[50] Este caso puede ser consultado en *Privacy Journal.*, noviembre de 1987.

[51] Una orden de la Marina norteamericana dispone que «todo miembro del cuerpo de Marina que pida, acepte o entable relaciones homosexuales será inmediatamente separado del servicio. Su actitud en un ambiente militar reduce el espíritu de combate, la seguridad y la moralidad».

Esta práctica, que en principio puede parecer escandalosa, está siendo cada vez más generalizada en los países altamente industrializados. Como denuncia Gerard G. Montigny, consejero de la Agencia de Protección de Datos de Noruega, los monitores de vigilancia en los lugares de trabajo son una realidad para cientos de miles de trabajadores.

Para Montigny, estos sistemas de vigilancia electrónica clandestina se realizan bajo el disfraz de la seguridad, y se incluyen medios visuales, telefónicos, computarizados y de acceso a monitores de control [52].

Debido a la gravedad del problema, el propio Comité de Ministros del Consejo de Europa adoptó en 1989 una importante Recomendación [53] sobre la protección de los datos personales utilizados con fines de empleo, aplicada a la recolección y uso del procesamiento automático de datos personales en los lugares de trabajo, tanto en el sector público como en el sector privado [54].

Ya en el preámbulo de dicha Recomendación se destaca el hecho de que el empleo de métodos por parte de los empresarios para la obtención de datos de sus empleados debe ser regulado a través de unos principios cuya finalidad última sea minimizar en la medida de lo posible los riesgos que tales métodos puedan implicar para los derechos y libertades de los trabajadores, poniendo especial interés en el derecho al respeto de la vida privada.

De especialmente acertada cabe catalogar la redacción del artículo 2 de dicha Recomendación, sobre el respeto de la vida privada y de la dignidad humana de los trabajadores, que afirma que deberá preservarse la posibilidad de mantener relaciones individuales o colectivas en los lugares de trabajo durante la obtención y posterior utilización de los datos personales de los trabajadores con fines de empleo [55], con las únicas excepciones de aquellos casos

---

[52] «Computers collect and analyze personal data, in such areas as key stroke counts, information use and tracking, hours worked, file access, work patterns and electronic mail», GERARD G. MONTIGNY. *Privacy 2000. Information technology and privacy*, Oslo, 1993, p. 18.

[53] Recomendación núm. R (89) 2. Adoptada por el Comité de Ministros el 18 de enero de 1989, durante la 423 reunión de los Delegados de los Ministros. Debe ser sin embargo destacado que la polémica presidió la reunión, e incluso el Delegado de Irlanda, en aplicación del artículo 10.2.c) del Reglamento interior de las reuniones de los Delegados de los Ministros, se reservó el derecho de su Gobierno a restringir el ámbito de la recomendación a datos exclusivamente automatizados, excluyendo de su ámbito de aplicación a los empleados domésticos y a las empresas familiares cuyo personal esté compuesto exclusivamente por miembros de la familia.

[54] Necesario es sin embargo recordar el carácter no legalmente vinculante de estas Recomendaciones, dirigidas a todos los Estados miembros, incidiendo únicamente en la obligación moral de dichos Estados en considerar de buena fe la conveniencia de su aplicación.

[55] «El respeto de la vida privada y de la dignidad humana del trabajador, en particular la posibilidad de mantener relaciones sociales y colectivas en el lugar de trabajo, debería preservarse durante la reco-

extraordinarios en los que entren en juego datos que sean necesarios para la protección de la seguridad del Estado y para la represión de las infracciones penales.

La expresión «con fines de empleo» está tomada en un sentido amplio, incluyendo todas aquellas relaciones entre el empresario y sus empleados que tengan por objeto el reclutamiento de los trabajadores, la planificación y organización de las actividades y la realización del contrato de trabajo.

Dicho acuerdo introdujo, pues, el principio de respeto a la privacidad y dignidad humana de los trabajadores y un número de prácticas acerca de datos personales que deben ser antes aceptadas por los empleados [56].

El propio Consejo de Europa, a través del Convenio 108, interpreta el concepto de dato en un sentido amplio, abarcando toda modalidad de información que comprenda representaciones alfabéticas, numéricas o gráficas que sean susceptibles de registro y transmisión.

Es por ello posible entender por dato no únicamente la información alfabética o numérica sino también las imágenes. Por tanto, las filmaciones e imágenes obtenidas a través de pantallas de control son asimiladas como auténticos datos, siendo reguladas por las disposiciones de dicho Convenio.

En Noruega, la polémica ha llevado a actuar al propio ministro de Justicia. Según datos que me han sido facilitados amablemente por la Agencia de Protección de Datos de Oslo [57], este Ministerio ha creado en 1993 una nueva sección en la Ley de Registros de Datos Personales [58] la cual autoriza a la Agencia a regular el uso de las grabaciones de vídeo incluyendo cuestiones de seguridad de los datos y derechos de acceso a las grabaciones.

Al mismo tiempo, una enmienda al Código penal acaba de ser introducida. Dicha enmienda impone un deber de aceptación mediante firma por parte de los trabajadores de la vigilancia por medio de cámaras de vídeo en sus lugarares de trabajo.

En Alemania, los problemas han sido resueltos parcialmente a través de una categoría jurídica nueva: *el concepto de autodeterminación informativa,*

---

gida y utilización de datos de carácter personal con fines de empleo». Artículo 2 de la Recomendación núm. R (89) 2.

[56] Esta Recomendación puede ser consultada en castellano en el volumen *Recomendaciones y Resoluciones del Comité de Ministros del Consejo de Europa en materia jurídica*, Secretaria General Técnica, Madnd, 1992. pp. 559-567.

[57] Debo agradecer sinceramente la amabilidad de todo el personal de la Agencia de Protección de Datos de Noruega y su exquisito comportamiento en todo momento.

[58] Act. núm. 48 de 9 de junio de 1978.

consagrada constitucionalmente por el Tribunal Constitucional Federal alemán en su decisiva sentencia de 15 de diciembre de 1983 relativa a la ley del censo de población de 1982[59].

Esta sentencia anulaba en parte dicha ley, estableciendo una total protección a la persona contra la recolección, almacenamiento, empleo y transmisión ilimitada de los datos concernientes al individuo.

Incide la sentencia en el consentimiento del sujeto, sin limitar el mismo a la recogida de datos, lo que obliga en cualquiera de las fases u operaciones que componen el tratamiento de los datos a conseguir el consentimiento del afectado.

Por todo ello la jurisprudencia germana interpreta que es el propio sujeto el que goza de la facultad de decidir cuándo y dentro de qué límites considera aceptable que se revelen datos de su propia privacidad, lo que desemboca en la obligación por parte de los empresarios de recabar de sus empleados el correspondiente permiso antes de utilizar dichos sistemas de vigilancia visual.

El Tribunal Constitucional alemán afirma, por otro lado, que un orden social y un orden jurídico que provocara que los individuos no pudieran saber qué, quién, cuándo y por qué se tienen datos personales sobre ellos serían incompatibles con el derecho a la autodeterminación informativa.

En España, los primeros casos[60] sobre vigilancia a través de sistemas automatizados han provocado un importante debate, siendo constatable la influencia de dicho principio de autodeterminación informativa tanto en la LORTAD como en las sentencias de nuestro Tribunal Constitucional, regulándose la obtención de datos por el libre consentimiento del sujeto.

Ha sido precisamente este Tribunal quien ha establecido el ámbito de protección, concretado en el derecho a la intimidad vinculado a la facultad de autodeterminación del sujeto y a su propia dignidad como ser humano[61].

Nuestro Tribunal entiende dicha facultad de autodeterminación como la posibilidad que se le brinda a todo ciudadano de decidir aquellos aspectos de su vida privada que quiere mantener ocultos y aquellas facetas que consiente que puedan ser transmitidas a terceros.

---

[59] Hay traducción castellana realizada por Mariano Daranas publicada en el «Boletin de Jurisprudencia Constitucional», núm. 33, Cortes Generales. 1984, pp. 126 y ss

[60] Baste citar aqui como ejemplo los hechos acaecidos en agosto de 1994 en Lugo, donde las cámaras de televisión instaladas para controlar el tráfico urbano de vehículos de dicha ciudad fueron empleadas para grabar a una pareja haciendo el amor en una habitación de una vivienda. La colocación y utilización de esas cámaras de televisión controladoras del tráfico provocaron la denuncia del Grupo de Convergencia Galega, por un presunto delito de violación de la intimidad que personalmente me parece irrefutable.

[61] Sentencia de 17 de octubre de 1991 del Tribunal Constitucional.

Sin embargo, vuelve la LORTAD a caer en el peligroso mundo de las excepciones, al regular su artículo 6 que no será preciso el consentimiento de la persona afectada cuando la recopilación de datos de carácter personal sea necesaria para el mantenimiento o cumplimiento de relaciones contractuales [62].

No es necesario señalar el grado de arbitrariedad que nuestra ley está indirectamente legitimando, pudiendo entenderse en sentido amplio la noción de necesidad de obtención de datos personales al no estar regulados por escrito dichos supuestos de necesidad.

Esto provoca la introducción de un nuevo problema, conocido por la ley francesa en su artículo 44 como desviación de finalidad (*détournement de finalité*), constituyendo un delito penado en el vecino país con pena de privación de libertad.

Sin embargo la LORTAD ha ignorado por completo en su artículo 43 este supuesto, recogiéndose únicamente en su artículo 43.3.*b*) la obtención de datos personales para incluir en ficheros automatizados con finalidades distintas de las que deberían constituir el objeto legítimo de la empresa recolectora de los datos, sin mencionar en ninguna parte de la ley como parte del supuesto de hecho el uso ulterior de los datos personales obtenidos.

Esta indudable laguna resulta todavía más incomprensible si procedemos a la lectura del articulado del Convenio de Schengen, que en su artículo 102.5 establece que toda utilización de los datos del Sistema de Información Schengen para finalidades distintas a las indicadas en los artículos 95 a 100 de dicho Convenio será considerada como desviación de finalidad.

La única solución que me parece válida para resolver esta laguna es acudir a lo dispuesto por el artículo 43.3.*d*), que define como infracción grave el hecho de tratar de forma automatizada los datos o usarlos posteriormente con conculcación de los principios señalados por la ley y acudir con posterioridad al artículo 4.2, que afirma que los datos no podrán ser empleados para finalidades distintas de aquellas para las que hubieran sido recogidos [63].

---

[62] «No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato». Artículo 6.2 de la LORTAD.

[63] Manuel Heredero Higueras, Subdirector general adjunto de cooperación jurídica internacional del Ministerio de Justicia, se manifiesta en similares términos, incidiendo en la utilización del artículo 4.2 como único medio para tratar de resolver el problema. MANUEL HEREDERO HIGUERAS, «La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal», *Boletín de Información del Ministerio de Justicia*, núm. 1669, 25 de abril de 1993.

En los Estados Unidos, la discusión ha alcanzado las proporciones más grandes. Según trabajos realizados por Simson Garfinkel [64], una impresionante mayoría de entrevistados en una encuesta en Boston afirman que ellos estan siendo electrónicamente controlados por monitores en sus lugares de trabajo.

Resumiendo los datos de la encuesta, el 81 por 100 de los entrevistados reconocen que sus supervisores escuchan las conversaciones telefónicas entre empleados y clientes. El 85 por 100 afirman que ellos son objeto de control por parte de sus responsables a través de monitores de vídeo. El 47 por 100 declaran que conocieron de la existencia de esa vigilancia porque la dirección de su empresa les informó de la misma. El resto se enteraron por conversaciones con otros compañeros de profesión o tras sufrir medidas disciplinarias como consecuencia de la visionalización de las grabaciones.

Otra encuesta realizada en Massachusetts ofrece el mismo panorama desesperanzador. Los trabajadores odian el uso de monitores de vídeo como sistema de control, especialmente al considerar que éstos suelen ser utilizados injustamente como medio de espionaje [65].

David F. Linowes, en su interesante libro *Privacy in America* [66], llega a una inquietante conclusión señalando que en la actualidad es completamente falso todo tipo de confidencialidad incluso de las propias grabaciones y de los datos extraíbles de éstas.

En este problemático contexto, presentamos ahora dos ilustrativos ejemplos de vigilancia clandestina, uno por medio de monitores de vídeo y otro a través de escuchas telefónicas.

Queremos resaltar de nuevo que la solución es para nosotros clara: únicamente podrán utilizarse los datos obtenidos (en este caso grabaciones) en un juicio cuando los valores defendidos mediante la presentación de dichas pruebas sean de un rango superior al de la privacidad de las personas violadas, con la finalidad de anteponer ante todo la justicia individual del caso concreto.

Esta premisa no se cumple en el llamado «caso Naseiro», en el que la brigada de la policía judicial de Valencia efectuó una serie de escuchas telefónicas con la finalidad de obtener pruebas para llevar a juicio a unos individuos por un presunto delito de tráfico de drogas, y durante las interceptaciones telefónicas consiguieron indicios de pruebas de un delito de cohecho, relacionado con la financiación ilegal de partidos políticos.

---

[64] Ver *Privacy Journal*, Washington, junio de 1989.

[65] Resulta tremendamente preocupante que las dos terceras partes estuvieran de acuerdo con esta afirmación, «monitoring makes it hard to get up for a break, even to go to the bathroom».

[66] DAVID F. LINOWES, *Privacy in America*, Illinois, 1989.

El problema de las escuchas telefónicas ya había sido regulado con anterioridad en los artículos 8.2 y 10.2 del Convenio paya la protección de los derechos humanos y las libertades fundamentales [67]. No obstante debe destacarse que el artículo 8.1 de dicho tratado no menciona en ningún momento las escuchas telefónicas, si bien la jurisprudencia del Tribunal Europeo de Derechos Humanos estima que éstas deben ser englobadas dentro del concepto de vida privada y familiar y de correspondencia [68].

La sentencia española [69], como por otra parte ya se esperaba, siguió la línea jurisprudencial marcada por el Tribunal Europeo de Derechos Humanos en los casos Klass, Malone, Huvig y Kruslin, en los que se ofrecen unas directrices inequívocas de rigurosa defensa del derecho a la intimidad, considerando la interceptación telefónica como una de las injerencias más graves a la intimidad de las personas.

Esta tesis del Tribunal Europeo de Derechos Humanos tenía ya un sólido apoyo en la Resolución del Comité de Ministros del Consejo de Europa de 5 de mayo de 1971, en la que se establecía que todas aquellas grabaciones magnetofónicas que se llevaran a cabo con desconocimiento de alguno de los participantes en la conversación constituirían una injerencia en la vida privada.

Las únicas injerencias permitidas a la autoridad pública (de nuevo nos encontramos ante un importante número de excepciones) son aquellas que estando previstas por la ley constituyan una medida necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás [70].

Ahora bien, para que la injerencia en el ejercicio del derecho recogido por el artículo 8.1 del Convenio resulte compatible con éste es completamente necesario que cumpla tres requisitos [71]: estar prevista por la ley (lo que requiere la previsibilidad de la ley, la accesibilidad de la misma y la existencia de una base legal suficiente en Derecho interno), atender a un fin legítimo y ser nece-

---

[67] Firmado en Roma el 4 de noviembre de 1950.

[68] Caso Klass, S. 6-9-1978, A 28, núm. 41; caso Malone, S. 2-8-1984, A 82, núm. 64; caso Huvig, S. 24-4-1990, A 176-B, núms. 25 y 32; caso Kruslin, S. 24-4-1990, A 176-A, núms. 33 y 36.

[69] Sentencia del Tribunal Supremo de 18 de junio de 1992 (A. 6102).

[70] Ver artículo 8.2 CEDH. Sin embargo, es conveniente contrastarlo con el artículo 10.2 CEDH, ya que su catálogo de excepciones no es exactamente coincidente, al añadir este último la integridad territorial, el impedir la transmisión de informaciones confidenciales, la protección de la reputación ajena y el garantizar la imparcialidad y autoridad del poder judicial.

[71] Para el estudio de los requisitos necesarios para la legalidad de estas injerencias ver CARLOS RUIZ MIGUEL, *op. cit.*, pp. 89-113.

saria en una sociedad democrática, si bien las nociones de estos últimos no han sido diferenciadas claramente [72].

Relacionando los ámbitos de expansión de dicho artículo 8 del Convenio con el artículo 18 de nuestra propia Constitución, deben ser destacadas indudablemente las contribuciones del TEDH en la regulación específica de las escuchas telefónicas, al limitar su utilización de una forma minuciosa y al exigir toda una serie de requisitos tanto institucionales como legales, ampliando de forma inequívoca el marco de protección establecido por nuestro artículo 18.3.

Por otro lado, la regulación del artículo 18 queda mejorada al tener en consideración el ámbito de protección establecido por el TEDH, al englobar dicho tribunal en el derecho a la privacidad aspectos de difícil relación con la informática no recogidos en nuestro texto constitucional.

La Ley Orgánica 4/1988, de 25 de mayo, de reforma de la Ley de Enjuiciamiento Criminal, introduce al dar nueva redacción al artículo 579 de la misma la noción de *indicios racionales de criminalidad*, considerando que tan sólo cuando dichos indicios sean suficientes el juez estará legitimado para ordenar la obtención de la prueba mediante sistemas de vigilancia cuya utilización sería en principio ilegítima.

Estos indicios son datos externos que permiten descubrir o atisbar, tras su examen judicial, la responsabilidad criminal del individuo en relación con el hecho presumible objeto de la investigación.

Ahora bien, creo necesario añadir que el término *indicio* tomado en el sentido querido por la Ley de Enjuiciamiento Criminal sólo debería aplicarse en aquellos supuestos en los que ya existieran dichos datos que pudieran inducir a una razonable sospecha, lo que es distinto a aquellos casos en los que la prueba es inducida como fenómeno que permite descubrir la existencia de otro delito no percibido con anterioridad.

La sentencia española, realmente acertada en mi opinión, recurre a la resolución del problema mediante la ponderación de intereses, afirmando que sólo cabe hablar de prueba *prohibida* cuando se lesionan los derechos proclamados por la Constitución como fundamentales.

Efectivamente, estas intervenciones telefónicas vulneran el derecho fundamental proclamado en el artículo 18.3 de la Constitución, y por ello el Tribunal declara radicalmente nula la prueba de intervención de conversaciones telefónicas por ser realizada con vulneración del derecho fundamental a la pri-

[72] Ver caso De Wilde, S. A 12, núm. 93; caso Golder, S. A 18, núm. 45; caso Handyside. S. A 24 núms. 48-57.

vacidad, y añadimos nosotros por encontrarse este bien jurídico por encima del derecho del Estado a investigar mediante estos sistemas los comportamientos de los ciudadanos constitutivos de infracciones penales que atenten contra valores de inferior rango a la misma privacidad.

El último caso que vamos a presentar aquí, como paradigma de vigilancia colectiva justificada, ocurrió en Noruega y es conocido internacionalmente como el «snack bar case».

Como ya ocurriera anteriormente en el supuesto Schowengerdt *v.* General Dynamics, de nuevo nuestra opinión va a ser contraria a la de los Tribunales que juzgaron el caso [73].

Un empresario tenía la certeza de que le robaban altas cantidades de dinero a diario. Su establecimiento poseía una cámara de vídeo en el lugar de descanso de sus empleados para que éstos pudieran ver si entraban a la tienda clientes

Como las pérdidas que sufría por el robo eran cuantiosas, el empresario únicamente tenía dos opciones: o despedir a todos sus trabajadores o intentar descubrir al ladrón por sí mismo.

Al optar por la segunda solución, decidió desviar un poco la inclinación de la cámara de tal modo que enfocara la caja registradora, introduciendo una cinta de vídeo sin que sus trabajadores lo supieran. Así, descubrió fácilmente cuál de sus empleados era realmente el ladrón.

La cinta de vídeo se presentó como evidencia en el juicio, pero fue rechazada, al aducir el tribunal que el caso suponía un serio infringimiento de la integridad personal incidiendo en la tensión que sin duda provoca tener una cámara de vídeo en el lugar de trabajo.

De esta forma, el tribunal noruego hacía caso omiso a la Recomendación núm. R (89) 2 del Comité de Ministros del Consejo de Europa ya citada con anterioridad, señalando en su artículo 1.5 que toda información recogida por el empresario con fines de empleo sobre sus empleados podrá ser utilizada si es considerado necesario para proteger la seguridad del Estado o como medio de represión de las infracciones penales (lo que indudablemente se da en el caso que nos ocupa).

Debo además destacar que el tribunal olvidó la existencia de un valor superior al de la privacidad del ladrón: el de la justicia del caso concreto. El único medio del empresario para conocer la identidad del ladrón era realizar esa clandestina grabación, con esa única finalidad y durante el período de tiem-

[73] La sentencia fue publicada en Norsk Retstidende 1991:616, Lov & data 28/1991: 8-9.

po imprescindible. Todas las razones morales estaban a su favor y tengo que mostrarme en desacuerdo tanto con el rechazo de la prueba por parte del tribunal como con la doctrina noruega, que encabezada por el profesor Jon Bing se manifiesta a favor de la inadmisión de ésta, por considerar que en caso contrario, de haber sido admitida, podrían generalizarse este tipo de vigilancias clandestinas [74].

Sin embargo, la justicia del caso concreto debería estar por encima de la privacidad del delincuente. Según mi opinión, la más importante meta de los sistemas legales debe ser la realización de la justicia concreta en los casos individuales. Los tribunales no deberían caer en el error de sacrificar la justicia concreta para conseguir una mayor seguridad jurídica [75].

6. CONCLUSIONES

A lo largo de este artículo hemos tratado varias cuestiones que parece conveniente volver a destacar.

En primer lugar, el fuerte grado de discrecionalidad del que gozan los Tribunales a la hora de juzgar este tipo de supuestos. En muchos casos los jueces acuden a la técnica legislativa de claúsulas o principios generales, procedimiento que si bien es aconsejable para regular materias especialmente sujetas a las innovaciones del mundo de la tecnología, provoca una considerable cantidad de innegables dificultades.

En segundo lugar, muchos de los aspectos generados por la tecnología continúan actualmente carentes de una adecuada regulación legal. Así pues, en este campo, la discrecionalidad no es el único problema que se plantea frente a la seguridad jurídica [76].

---

[74] «... it would necessarilly lead to an undetermining of the protection on privacy... If evidence is permitted in such cases, it will increase the risk for extensive use of clandestine recording also in other cases». JON BING, *Privacy and surveillance systems, op. cit.*, p. 90.

[75] En parecidos términos se expresa uno de los más grandes pensadores del realismo jurídico escandinavo, el sociólogo del Derecho Vilhem Aubert. «It is possible, may likely, that the optimum combination of predictibility and justice has not been reached, and the courts could move toward more predictability without violating justice». VILHEM AUBERT, «The structure of legal thinking», *Legal Essays. A tribute to Frede Castberg*, Universitetsforlaget, Oslo, 1963, p. 45.

[76] Sin embargo, un cierto grado de discrecionalidad es instrumento necesario para el correcto funcionamiento de los sistemas de Derecho occidentales. La previsión de todas las posibles combinaciones de circunstancias éticamente relevantes en los casos interpuestos ante los Tribunales es imposible en la actualidad y probablemente siempre lo será.

En tercer lugar, todas estas lagunas legales deben ser atacadas mediante una doble estrategia: realizando una ordenación armonizadora de aquellas normas que continúan dispersas en nuestro Derecho y que tienen que ver con la intimidad, con la privacidad y con la protección de datos por un lado, y llevando a cabo una auténtica cooperación internacional con la ineludible finalidad de lograr un consenso común sobre los aspectos de mayor importancia por otro lado, ya que en la actualidad la necesidad de proteger la privacidad de los ciudadanos ha superado con creces la esfera estricta del Derecho interno para ser discutida como un presupuesto básico del orden jurídico internacional.

En cuarto lugar, debemos abogar por el auténtico papel que tendría que jugar el principio de proporcionalidad dentro de un verdadero sistema de Derecho. Este criterio, indisolublemente unido al valor justicia, debe resolver en aquellos casos en los que se planteen conflictos frente a la privacidad, mediante la ponderación de bienes jurídicos atendiendo a la naturaleza del delito que se pretende combatir, su gravedad y su propia trascendencia social.

Para concluir, recordar que pese al frenesí de la era tecnológica que nos está tocando vivir, todavía existen una serie de valores fundamentales, inherentes a la naturaleza humana, con una escala que debe ser respetada. No hacerlo conlleva exponerse a caer en una trampa demasiado peligrosa.

BIBLIOGRAFÍA

ÁLVAREZ-CIENFUEGOS, José María, «La informática en el ámbito de la Administración de Justicia», *Actualidad Informática de Aranzadi,* Madrid, núm. 4, 1 992, pp. 1 -4.

AUBERT, Vilhelm, «On the structure of legal thinking», *Legal Essays. A tribute to Frede Castberg*, Universitetsforlaget, Oslo, 1963, pp. 41-63.

AUBERT, Vilhelm, *Continuity and developement*, Norwegian University Press, Oslo, 1989.

AUSEMS, Egbert J., «La protección de las personas frente al tratamiento automatizado de los datos personales en el marco del Convenio 108 del Consejo de Europa», Departamento de Justicia del Gobierno Vasco, en el volumen colectivo *Informática Judicial y Protección de Datos Personales*, Vitoria, 1994.

BELTRÁN, Miguel. *Originalismo e interpretación. Dworkin v. Borlt: una polémica constitucional*, Civitas, Madrid, 1989.

BUENO ARÚS, Francisco, «El delito informático», *Actualidad Informática de Aranzadi*, Madrid, núm. 11, 1994. pp. 1-6.

BING, Jon, «Reflections on data protection policy for 1992». *Yearbook of Law, Computers and Technology,* Londres,1991, pp. 1 64177.

BING, Jon, «Privacy and surveillance systems», *The International Computer Lawyer,* septiembre 1993, pp. 17-23.

BING, Jon, «Data Protection in a time of changes». *Information Law Series,* 1994, pp. 247-259.

DAVARA RODRÍGUEZ, Miguel Ángel, «La informática jurídica y el derecho informático», *Actualidad Informática de Aranzadi*, Madrid,1991, núm. 1. pp. 1-6.

DWORKIN, Ronald, *Los derechos en serio,* Ariel, Barcelona,1989.

ECKHOFF, Torstein, «Justice and social utility». *Legal Essays. A tribute to Frede Castberg,* Universitetsforlaget, Oslo, 1963, pp. 74-93.

ECKHOFF, Torstein, *Justice. Its determinants in social interaction,* Rotterdam University Press, Rotterdam, 1974.

ELY, John H., *Democracy and distrust. A theory of judicial review,* Harvard University Press, Cambridge, 1980.

FARIÑAS MANTONI, Luis María, *El derecho a la intimidad,* Trivium, Madrid, 1983.

FROSINI, Vittorio, *Il diritto nella societa tecnologica,* Giuffre. Milán.1981.

FULLER, Lon L., *La moral del derecho,* México, 1961.

GALINDO AYUDA, Fernando, «Consecuencias de la entrada de España en la Comunidad Europea en el Derecho español de la informática», en el volumen colectivo, *Derecho español y Derecho comunitario europeo,* Fernando Mariño (ed.), Zaragoza, 1987, pp. 389-426.

HEREDERO HIGUERAS, Manuel, «La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal», *Boletín de Información del Ministerio de Justicia,* núm. 1669, 25 de abril de 1993.

LINOWES, David F., *Privacy in America,* Illinois, 1989.

LUCAS MURILLO DE LA CUEVA, Pablo, «La protección de los datos personales ante el uso de la informática», *Revista de la Facultad de Derecho de la Universidad Complutense*, núm. 15, Madrid, 1989, pp. 601-619.

LUCAS MURILLO DE LA CUEVA, Pablo, *El derecho a la autodeterminación informática,* Madrid, 1990.

MALT, Gert-Fredrik, «Methods for the solution of conflicts between rules in a system of positive law», *Coherence and conflict in law,* Amsterdam, 1991. pp. 201-226.

MARTÍN PALLÍN, José Antonio, «La Ley Orgánica de Regulación del tratamiento automatizado de datos de carácter personal. Una visión crítica», Departamento de Justicia del Gobierno Vasco en el volumen colectivo *Informática Judicial y Protección de Datos Personales*, Vitoria, 1994, pp. 77-94.

MONTIGNY, Gerard G., «Privacy 2000. Information technology and privacyf», Oslo. 1993. pp. 1-22.

OLIVECRONA, Karl. *El derecho como hecho,* Buenos Aires. 1959.

O'CALLAGHAM MUÑOZ, Xavier, «Derecho al honor, a la intimidad y a la propia imagen», en el volumen colectivo *XII Jornadas de estudio, Los Derechos Fundamentales y Libertades Públicas (I)*, vol. I, Ministerio de Justicia, Madrid, 1992, pp. 545-625.

PECES-BARBA, Gregorio, *Los valores fundamentales,* Tecnos, Madrid, 1984.

PECES-BARBA, Gregorio, *Derecho y derechos fundamentales*, Centro de Estudios Constitucionales, Madrid, 1993.

PÉREZ LUÑO, Antonio Enrique, *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 1991.

PÉREZ LUÑO, Antonio Enrique, *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid. 1989.

PÉREZ LUÑO, Antonio Enrique, «La LORTAD y los derechos fundamentales», *Revista derechos y libertades*, núm. 1, Instituto Bartolomé de las Casas, Madrid, 1993, pp. 405-424.

RUIZ MIGUEL, Carlos, *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, Civitas. Madrid, 1994.

WESTIN, Alan, *Privacy and Freedom*, Atheneum, Nueva York, 1967.