

La Sala Segunda del Tribunal Constitucional, compuesta por don Eugeni Gay Montalvo, Presidente, doña Elisa Pérez Vera, don Ramón Rodríguez Arribas, don Francisco Hernando Santiago, don Luis Ignacio Ortega Álvarez y don Francisco Pérez de los Cobos Orihuel, Magistrados, ha pronunciado

EN NOMBRE DEL REY

la siguiente

SENTENCIA

En el recurso de amparo núm. 5928-2009, promovido por don Carlos Trabajo Rueda, representado por el Procurador de los Tribunales don Joaquín Pérez de Rada González de Castejón y asistido por el abogado don Diego Silva Merchante, contra la Sentencia de la Sección Primera de la Audiencia Provincial de Sevilla de 7 de mayo de 2008, dictada en Procedimiento Abreviado núm. 254/2007, que condenó al recurrente como autor de un delito de corrupción de menores a la pena de cuatro años de prisión e inhabilitación especial para el derecho de sufragio pasivo durante el tiempo de la condena, y contra la Sentencia de la Sala de lo Penal del Tribunal Supremo, de 18 de febrero de 2009, dictada en recurso de Casación núm. 1396/2008, que confirmó la condena impuesta. Ha intervenido el Ministerio Fiscal. Ha sido Ponente el Magistrado don Eugeni Gay Montalvo, quien expresa el parecer de la Sala.

I. Antecedentes

1. Mediante escrito registrado en este Tribunal con fecha de 24 de junio de 2009, el Procurador de los Tribunales don Joaquín Pérez de Rada González de Castejón, en nombre de

don Carlos Trabajo Rueda, interpuso recurso de amparo contra las resoluciones reseñadas en el encabezamiento.

2. Los hechos de los que trae causa la demanda de amparo, relevantes para la resolución del caso son, en síntesis, los siguientes:

a) La Sentencia de la Audiencia Provincial de Sevilla ya referenciada condenó al recurrente como autor de un delito de corrupción de menores del art. 189.1 b) CP a la pena de cuatro años de prisión e inhabilitación especial para el derecho de sufragio pasivo durante el tiempo de la condena. Los hechos probados relatan lo siguiente:

“Entre los meses de noviembre y diciembre de 2007, el acusado Carlos Trabajo Rueda (mayor de edad y sin antecedentes penales) ha tenido en su ordenador personal portátil numerosos ficheros de fotografías y videos mostrando a menores de edad – muchos de los cuales no alcanzan los trece años – solos o acompañados de otros menores, desnudos en actitudes y prácticas explícitamente sexuales.”

Así, en la carpeta ‘Mis documentos/mis imágenes’ el acusado conservaba 17 videos y más de 3.000 fotografías de contenido pedófilo, y en la carpeta ‘eMule/Incoming’ almacenaba más de 140 vídeos y más de 150 fotografías de pornografía infantil.

Los ficheros que representaban tales imágenes fueron obtenidos por el acusado, mediante el sistema de intercambio de archivos en Internet conocido como ‘Peer to peer’, utilizando el mencionado programa eMule, por el que se comparten imágenes mediante su descarga y distribución simultánea. Por este sistema, el acusado -que tenía configurado el programa eMule para poner a disposición de cualquier otro usuario de la red todos los archivos contenidos en el disco duro de su ordenador- distribuyó material pornográfico de menores (muchos de ellos, menores de trece años) en una cantidad equivalente a unos 96 Giga bytes.

Frente a la alegada lesión del derecho a la intimidad, planteada por el recurrente como cuestión previa, la Audiencia Provincial responde lo siguiente:

“Las presentes actuaciones dimanaron de la denuncia formulada por el testigo [...] Según la misma (fs. 15-16) -coincidente con su declaración en el plenario-, el acusado se personó en su establecimiento (APP Informática) entregándole su ordenador portátil con el encargo de cambiar la grabadora, que no funcionaba. Una vez efectuada la reparación y para comprobar el correcto funcionamiento de las piezas sustituidas, el testigo -como al parecer es práctica habitual- escogió al azar diversos archivos de gran tamaño (fotografías, videos o música) para grabarlos y reproducirlos en el ordenador, visualizándose entonces las imágenes pornográficas que contenía. El testigo puso entonces tal circunstancia en conocimiento de la Policía Nacional, que procedió a la intervención del portátil y al examen de su contenido, sin solicitar autorización judicial al efecto.

Pues bien, el Tribunal no considera que la actuación de [...] y de la Policía Nacional vulnerara el derecho a la intimidad del inculcado atendiendo a dos razones:

1. El testigo especificó en juicio que, al recibir el encargo, preguntó a don Carlos Trabajo Rueda si el ordenador tenía contraseña, a lo que el cliente le respondió que no, sin establecerle limitación alguna en el uso del ordenador y acceso a los ficheros que almacenaba.

En consecuencia, pese a conocer que el técnico accedería al disco duro del ordenador (pues para ello le solicitó la contraseña), el acusado consintió en ello sin objetar nada ni realizar ninguna otra prevención o reserva que permita concluir que pretendía mantener al margen del conocimiento ajeno determinada información, datos o archivos.

2. En ello abunda precisamente el hecho de que, como señaló el perito funcionario policial núm. 101.182 corroborando así la conclusión del informe pericial documentado (f. 120), el acusado tenía configurado el programa eMule de manera que todos los archivos del disco estuvieran a disposición de cualquier otro usuario de la aplicación.

En definitiva, difícilmente puede invocarse el derecho a la intimidad cuando los propios actos del acusado indican paladinamente que no tenía intención ni voluntad

alguna de preservar para su esfera íntima, exclusiva y personal ninguno de los ficheros que conservaba en su ordenador, pues a ellos tenía acceso cualquier persona que se conectara en Internet a la misma red de intercambio”.

b) La Sentencia del Tribunal Supremo desestimó el recurso de casación interpuesto. Respecto del motivo que denunciaba la vulneración del derecho a la intimidad, responde la Sala Segunda en los siguientes términos:

“Mas lo ocurrido es que sí existió la autorización de Carlos. En efecto, declara, hasta en el juicio oral, el dueño del establecimiento, acompañando una hoja de trabajo que dice ‘cambiar grabadora DVD-no lee muchos DVD’, que Carlos le llevó el ordenador portátil para que se lo reparara, porque funcionaba mal la grabadora, y no le puso límite alguno para entrar en el ordenador; uno de los técnicos procedió al cambio de la grabadora y se trató de probar, como es habitual, el correcto funcionamiento de las piezas, para lo que el técnico fue a la carpeta de ‘mis documentos/mis imágenes’ y, de repente, se pudo ver en miniatura lo que parecían fotografías de pornografía infantil..., no fue necesario el empleo de contraseña alguna y Carlos le había dicho que no la había; y llevó el ordenador a la Policía... Es decir, no hubo injerencia inconsentida para disponer de un elemento de prueba, sino la voluntaria puesta por el afectado, de ese elemento, a disposición de un número abierto de receptores.

Pero es más, el informe policial establece que el ordenador tenía instalado el programa eMule de intercambio de ficheros tipo ‘peer to peer’; con el cual programa se accede a los contenidos que tienen compartidos todos los equipos conectados a Internet que estén utilizando eMule y, a su vez, se comparten las carpetas que se determinen del equipo propio; en la carpeta de descarga por defecto llamada “Incoming” se almacenan los ficheros descargados; se pueden determinar las carpetas a compartir con los demás usuarios, pero hay algo común a todos, la carpeta de descarga siempre es compartida; en el contenido de la carpeta de descarga y compartida “Incoming” se encontraban los archivos con las imágenes a que afecta este proceso.

Con todo ello ha de concluirse la existencia de dos factores interconectados: a) Carlos no había dispuesto un ámbito de privacidad respecto al contenido pornográfico

infantil del ordenador; b) no fue necesaria, en el presente caso, gestión alguna para desvelar la identidad de Carlos, como usuario del ordenador y de su contenido.

No existía, en el supuesto que nos ocupa, protección incluíble en el art. 18.1 o en el art. 18.3 CE; ni hubo injerencia contraria a los derechos reconocidos en esos preceptos.”

3. La demanda de amparo se fundamenta en la vulneración del derecho a la intimidad (art. 18.1 CE) y de los derechos a un proceso con todas las garantías y a la presunción de inocencia (art. 24.2 CE). Considera el recurrente vulnerado su derecho a la intimidad porque tanto el dueño de la tienda donde llevó a reparar el ordenador como los policías nacionales que accedieron al ordenador actuaron sin previa autorización judicial. Alega que la Policía al recibir la denuncia debía haber solicitado autorización del Juez. Por otra parte, tampoco existían motivos de urgencia que legitimaran una actuación policial inmediata. De igual modo que, tanto para acceder al contenido de la correspondencia -salvo las que incorporan una declaración de contenido-, como para acceder a los registros de llamadas de un teléfono móvil es necesaria autorización judicial que debe exigirse para acceder al contenido de un ordenador personal. Además, discrepa asimismo de la argumentación de los órganos judiciales pues no cabe afirmar un consentimiento siquiera tácito a la divulgación de la información contenida en el ordenador. Por más que hubiera manifestado que carecía de contraseña, el ordenador fue entregado en la tienda únicamente para la reparación de la grabadora y no para el acceso a los documentos. Y tampoco puede justificarse tal consentimiento en el hecho de que compartía los archivos a través del programa eMule, pues ese dato sólo se obtiene a posteriori una vez que ya se ha accedido al contenido del equipo.

En segundo lugar entiende vulnerado el derecho a un proceso con todas las garantías (art. 24.2 CE), por haberse utilizado prueba ilícita para fundar la condena dada la lesión del derecho a la intimidad; además, la totalidad de las pruebas en que se basa la condena se derivan directa o indirectamente del hallazgo de los archivos obtenido con vulneración del art. 18.1 CE, por lo que resulta lesionado también el derecho a la presunción de inocencia (art. 24.2 CE). Especifica al respecto que tampoco puede servir a tal fin la declaración del propio recurrente, puesto que en el acto del juicio oral se acogió a su derecho a no declarar y la acusación no solicitó la lectura de sus declaraciones prestadas ante el Juez de instrucción.

4. La Sala Segunda de este Tribunal, por providencia de 22 de julio de 2010, acordó admitir a trámite la demanda de amparo y, en aplicación de lo dispuesto en el art. 51 LOTC, dirigir atentas comunicaciones a los órganos judiciales competentes para la remisión de certificación o fotocopia adverada de las actuaciones y emplazamiento a quienes hubieran sido parte en el procedimiento, a excepción del demandante de amparo, para que, si lo desearan, pudiesen comparecer en el plazo de diez días en el presente proceso de amparo.

Igualmente se acordó formar la correspondiente pieza separada de suspensión, en la que, tras los trámites oportunos, se dictó por la Sala Segunda de este Tribunal el Auto de 4 de octubre de 2010, acordando acceder la suspensión de la pena privativa de libertad de cuatro años de prisión y la accesoria de inhabilitación especial para el derecho de sufragio pasivo durante el tiempo de la condena.

5. Por diligencia de ordenación de la Secretaría de Justicia de la Sala Segunda de 18 de octubre de 2010 se acordó dar vista de las actuaciones recibidas al Ministerio Fiscal por plazo común de veinte días para presentar las alegaciones que estimase pertinentes, de conformidad con el art. 52.1 LOTC.

6. El Ministerio Fiscal, en escrito registrado el 24 de noviembre de 2010, interesó el otorgamiento del amparo por vulneración del derecho a la intimidad (art. 18.1 CE) y del derecho a un proceso con todas las garantías (art. 24.2 CE).

Después de exponer la doctrina constitucional sobre el derecho a la intimidad, manifiesta que el ordenador es un elemento idóneo para albergar datos personales contenidos en los archivos informáticos y, con ello, para ejercer el derecho a la intimidad, por lo que para su acceso resulta preciso el consentimiento del titular o, en su caso, la existencia de razones de necesidad y urgencia y un juicio positivo de proporcionalidad. Respecto al acceso del encargado de la tienda a la carpeta “mis documentos”, discrepa el Ministerio Público de los argumentos esgrimidos por las resoluciones judiciales recurridas, pues considera que ni hubo un consentimiento expreso por parte del demandante de amparo, ni cabe afirmar la realización de actos concluyentes e inequívocos de los que quepa inferir un consentimiento tácito. Por ello, el acceso a los archivos del ordenador por parte del encargado de la tienda vulneró el derecho a la intimidad.

En relación a la actuación de la policía judicial, asevera el Ministerio Fiscal, tras citar lo que afirmamos en la STC 70/2002, de 25 de abril, que una vez entregado el ordenador junto con la formulación de la denuncia, la policía habría podido solicitar el consentimiento del recurrente, quien se hallaba ya identificado, o bien haber recabado autorización judicial. En ausencia de tales requisitos habilitantes, el acceso al contenido del ordenador únicamente podría considerarse legítimo cuando existiesen razones de necesidad de una intervención policial inmediata para la prevención y averiguación del delito, el descubrimiento del delincuente y la obtención de pruebas incriminatorias, y sólo cuando la intervención se realizara desde el respeto al principio de proporcionalidad; circunstancias de urgencia y necesidad que no concurren en el caso concreto. Por otra parte, no cabe justificar la actuación policial con el argumento de que el denunciante ya había accedido a los mismos, ni tampoco en que el recurrente tuviera configurado un programa de intercambio de archivos con acceso a terceros. En relación con esta última circunstancia, asevera el Ministerio Público que ese hecho no permite abrigar una suerte de autorización genérica para el acceso por cualesquiera personas al contenido de su ordenador, debiendo tenerse en cuenta, asimismo, que el conocimiento de la existencia del programa informático de intercambio de archivos se obtiene sólo una vez se ha accedido al ordenador.

A continuación, se plantea el Ministerio Fiscal si la vulneración del derecho a la intimidad (art. 18.1 CE) conllevaría, además, la lesión del derecho a un proceso con todas las garantías (art. 24.2 CE), por haberse valorado prueba obtenida con vulneración de derechos fundamentales. Las pruebas practicadas en el juicio oral y valoradas por los órganos judiciales han sido, además del hallazgo de los archivos pedófilos, el testimonio del testigo dueño de la tienda de informática y el del policía instructor del atestado, quien además depuso como perito del informe pericial que se aportó como prueba documental pericial. El hallazgo de los archivos proviene directamente de la medida lesiva del derecho fundamental, pero para determinar si las restantes pruebas derivadas adquieren también ese carácter, es preciso analizar si son jurídicamente independientes (STC 81/1998, de 2 de abril). Por lo que respecta a la testifical del policía, considera el Fiscal que es materialmente inescindible de la prueba originaria, por no ser sino mera reproducción vía testimonio del acto de injerencia en el derecho fundamental; a igual conclusión llega respecto de la prueba pericial, hallándose también en conexión de antijuridicidad con el hallazgo ilícito de los archivos pedófilos. Distinta suerte ha de correr, no obstante, la prueba testifical del encargado del establecimiento, atendiendo a la menor entidad de la lesión del derecho a la intimidad -al no ser intencional- del que tal prueba proviene.

Pudiendo considerarse lícita la citada declaración testifical del encargado de la tienda, y habiéndose valorado conjuntamente con otras que sí deben ser consideradas ilícitas y deben, por ello, ser expulsadas del ordenamiento, concluye el Ministerio Fiscal que desde las competencias atribuidas al Tribunal Constitucional no puede éste efectuar un pronunciamiento sobre la entidad probatoria de dicha prueba a los efectos de su relevancia para la presunción de inocencia, por lo que lo procedente sería declarar la vulneración del derecho a la intimidad (art. 18.1 CE) y el derecho a un proceso con todas las garantías (art. 24.2 CE); anular las resoluciones recurridas y retrotraer el procedimiento al momento anterior a dictarse la Sentencia de la Audiencia Provincial, para que sean los órganos judiciales quienes valoren la suficiencia de la prueba carente del vicio de ilicitud.

El recurrente, mediante escrito de 22 de noviembre de 2010, reiteró los argumentos expuestos en su demanda de amparo, solicitando la anulación de las Sentencias recurridas.

7. Por Providencia de fecha 3 de noviembre de 2011, se señaló para deliberación y fallo de la Sentencia el día 7 del mismo mes y año.

II. Fundamentos jurídicos

1. Se dirige la presente demanda de amparo contra la Sentencia de la Audiencia Provincial de Sevilla de 7 de mayo de 2008 que condenó al recurrente como autor de un delito de corrupción de menores en su modalidad de distribución de pornografía infantil [art. 189.1 b) CP], y contra la Sentencia del Tribunal Supremo de 18 de febrero de 2009 que confirmó la condena impuesta. Se plantea en la misma la vulneración del derecho a la intimidad (art. 18.1 CE), del derecho a un proceso con todas las garantías (art. 24.2 CE) y del derecho a la presunción de inocencia (art. 24.2 CE), por haberse fundado la condena en prueba de cargo obtenida con vulneración del primer derecho fundamental invocado, al haber accedido tanto el denunciante de los hechos, como después la Policía, a determinados archivos del ordenador del demandante de amparo sin su consentimiento y sin autorización judicial, y no existiendo, por lo demás, razones de urgencia. El Ministerio Fiscal solicita igualmente el otorgamiento del amparo por las razones que se han expuesto en los antecedentes de esta resolución.

2. Para dar respuesta a la cuestión nuclear que se plantea en la demanda es preciso, en primer lugar, exponer la doctrina que este Tribunal ha desarrollado en relación con el derecho fundamental a la intimidad (art. 18.1 CE).

Según hemos venido manifestando, el derecho a la intimidad personal, en cuanto derivación de la dignidad de la persona (art. 10.1 CE), implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana (SSTC 207/1996, de 16 de diciembre, FJ 3; 186/2000, de 10 de julio, FJ 5; 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 4; 159/2009, de 29 de junio, FJ 3). De forma que "lo que el art. 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio" (SSTC 127/2003, de 30 de junio, FJ 7; 89/2006, de 27 de marzo, FJ 5). Del precepto constitucional citado se deduce que el derecho a la intimidad confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido (SSTC 196/2004, de 15 de noviembre, FJ2; 206/2007, de 24 de septiembre, FJ 5; 70/2009, de 23 de marzo, FJ 2).

No obstante lo anterior, hemos afirmado que el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno (SSTC 83/2002, de 22 de abril, FJ 5; 196/2006, de 3 de julio, FJ 5), aunque este consentimiento puede ser revocado en cualquier momento (STC 159/2009, de 29 de junio, FJ 3). Ahora bien, se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto "aún autorizada, subverta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida" (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; 70/2009, de 23 de marzo, FJ 2). En lo relativo a la forma de prestación del consentimiento, hemos manifestado que este no precisa ser expreso, admitiéndose también un consentimiento tácito. Así, en la STC 196/2004, de 15 de noviembre, en que se analizaba si un reconocimiento médico realizado a un trabajador había afectado a su intimidad personal, reconocimos no sólo la eficacia del consentimiento prestado

verbalmente, sino además la del derivado de la realización de actos concluyentes que expresen dicha voluntad (FJ 9). También llegamos a esta conclusión en las SSTC 22/1984, de 17 de febrero y 209/2007, de 24 de septiembre, en supuestos referentes al derecho a la inviolabilidad del domicilio del art. 18.2 CE, manifestando en la primera que este consentimiento no necesita ser “expreso” (FJ 3) y en la segunda que, salvo casos excepcionales, la mera falta de oposición a la intromisión domiciliar no podrá entenderse como un consentimiento tácito (FJ 5).

Por otra parte, tampoco podrá considerarse ilegítima aquella injerencia o intromisión en el derecho a la intimidad que encuentra su fundamento en la necesidad de preservar el ámbito de protección de otros derechos fundamentales u otros bienes jurídicos constitucionalmente protegidos (STC 159/2009 de 29 de junio, FJ 3). A esto se refiere nuestra doctrina cuando alude al carácter no ilimitado o absoluto de los derechos fundamentales, de forma que el derecho a la intimidad personal, como cualquier otro derecho, puede verse sometido a restricciones (SSTC 98/2000, de 10 de abril, FJ 5; 156/2001, de 2 de julio, FJ 4; 70/2009, de 23 de marzo, FJ 3). Así, aunque el art. 18.1 CE no prevé expresamente la posibilidad de un sacrificio legítimo del derecho a la intimidad -a diferencia de lo que ocurre en otros supuestos, como respecto de los derechos reconocidos en los arts. 18.2 y 3 CE-, su ámbito de protección puede ceder en aquellos casos en los que se constata la existencia de un interés constitucionalmente prevalente al interés de la persona en mantener la privacidad de determinada información. Precisando esta doctrina, recordábamos en la STC 70/2002, de 3 de abril, FJ 10, (resumiendo lo dicho en la STC 207/1996, de 16 de diciembre, FJ 4) que los requisitos que proporcionan una justificación constitucional objetiva y razonable a la injerencia en el derecho a la intimidad son los siguientes: la existencia de un fin constitucionalmente legítimo; que la medida limitativa del derecho esté prevista en la ley (principio de legalidad); que como regla general se acuerde mediante una resolución judicial motivada (si bien reconociendo que debido a la falta de reserva constitucional a favor del Juez, la Ley puede autorizar a la policía judicial para la práctica de inspecciones, reconocimientos e incluso de intervenciones corporales leves, siempre y cuando se respeten los principios de proporcionalidad y razonabilidad) y, finalmente, la estricta observancia del principio de proporcionalidad, concretado, a su vez, en las tres siguientes condiciones: “si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o

equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)” (STC 89/2006, de 27 de marzo, FJ 3).

Por lo que se refiere a la concurrencia de un fin constitucionalmente legítimo que puede permitir la injerencia en el derecho a la intimidad, este Tribunal ha venido sosteniendo que reviste esta naturaleza “el interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal” (SSTC 25/2005, de 14 de febrero, FJ 6; 206/2007, de 24 de septiembre, FJ 6). En efecto, “la persecución y castigo del delito constituye un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana, bienes igualmente reconocidos en los arts. 10.1 y 104.1 CE” [SSTC 127/2000, de 16 de mayo, FJ 3 a); 292/2000, de 30 de noviembre, FJ 9]. También hemos precisado que “reviste relevancia e interés público la información sobre los resultados positivos o negativos que alcanzan en sus investigaciones las fuerzas y cuerpos de seguridad, especialmente si los delitos cometidos entrañan una cierta gravedad o han causado un impacto considerable en la opinión pública, extendiéndose aquella relevancia o interés a cuantos datos o hechos novedosos puedan ir descubriéndose por las más diversas vías, en el curso de las investigaciones dirigidas al esclarecimiento de su autoría, causas y circunstancias del hecho delictivo” (STC 14/2003, de 28 de enero, FJ 11).

De lo anterior, se deduce que el legislador ha de habilitar las potestades o instrumentos jurídicos que sean adecuados para que, dentro del respeto debido a los principios y valores constitucionales, las fuerzas y cuerpos de seguridad del Estado cumplan con esta función de averiguación del delito. Como reseñamos en la STC 70/2002, de 3 de abril, FJ 10, “Por lo que respecta a la habilitación legal en virtud de la cual la policía judicial puede practicar la injerencia en el derecho a la intimidad del detenido, en el momento de la detención, las normas aplicables son, en primer lugar el art. 282 LECrim, que establece como obligaciones de la policía judicial la de ‘averiguar los delitos públicos que se cometieron en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro poniéndolos a disposición de la Autoridad Judicial’. En la misma línea, el art. 11.1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado, establece como funciones de éstos, entre otras, f) ‘prevenir la comisión de actos delictivos’; g) ‘investigar los delitos para descubrir y detener a los presuntos

culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del Juez o Tribunal competente y elaborar los informes técnicos y periciales procedentes'. Por último, el art. 14 de la Ley Orgánica 1/1992, de 21 de febrero, sobre protección de la seguridad ciudadana, establece que las autoridades competentes podrán disponer las actuaciones policiales estrictamente necesarias para asegurar la consecución de las finalidades previstas en el art. 1 de esta Ley, finalidades entre las que se encuentra la prevención de la comisión de delitos". Según la citada Sentencia (mismo FJ) existe, por tanto, "una habilitación legal específica que faculta a la policía para recoger los efectos, instrumentos y pruebas del delito y ponerlos a disposición judicial y para practicar las diligencias necesarias para la averiguación del delito y el descubrimiento del delincuente. Entre esas diligencias (que la Ley no enumera casuísticamente, pero que limita adjetivándolas y orientándolas a un fin) podrá encontrarse la de examinar o acceder al contenido de esos instrumentos o efectos, y en concreto, de documentos o papeles que se le ocupen al detenido, realizando un primer análisis de los mismos, siempre que -como exige el propio texto legal- ello sea necesario (estrictamente necesario, conforme al art. 14 de la Ley Orgánica 1/1992), estricta necesidad que habrá de valorarse atendidas las circunstancias del caso y que ha de entenderse como la exigencia legal de una estricta observancia de los requisitos dimanantes del principio de proporcionalidad. Así interpretada la norma, puede afirmarse que la habilitación legal existente cumple en principio con las exigencias de certeza y seguridad jurídica dimanantes del principio de legalidad, sin perjuicio de una mayor concreción en eventuales reformas legislativas".

En relación a la necesidad de autorización judicial, el criterio general, conforme a nuestra jurisprudencia, es que sólo pueden llevarse a cabo injerencias en el ámbito de este derecho fundamental mediante la preceptiva resolución judicial motivada que se adecue al principio de proporcionalidad (SSTC 207/1996, de 16 de diciembre, FJ4; 25/2005, de 14 de febrero, FJ 6; 233/2005, de 26 de septiembre, FJ 4). Esta regla no se aplica, también según nuestra doctrina, en los supuestos en que concurran motivos justificados para la intervención policial inmediata, que ha de respetar también el principio de proporcionalidad. De manera significativa hemos resaltado en la STC 70/2002, de 3 de abril, que "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” [FJ 10 b).3]. Bien entendido que “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 al 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” [FJ 10 b).5]. En esta línea en la STC 206/2007, de 24 de septiembre, FJ 8, afirmábamos que “la regla general es que sólo mediante una resolución judicial motivada se pueden adoptar tales medidas y que, de adoptarse sin consentimiento del afectado y sin autorización judicial, han de acreditarse razones de urgencia y necesidad que hagan imprescindible la intervención inmediata y respetarse estrictamente los principios de proporcionalidad y razonabilidad”. En esta Sentencia razonábamos que no había existido una autorización judicial previa para la injerencia acaecida en el derecho a la intimidad (en este caso un análisis de sangre interesado por la Guardia Civil), entendiéndose como relevante el hecho de que tampoco por los órganos judiciales se había efectuado posteriormente una “ponderación de los intereses en conflicto teniendo en cuenta el derecho fundamental en juego que les condujera a considerar justificada -a la vista de las circunstancias del caso- la actuación policial sin previa autorización judicial” (mismo FJ).

3. Una vez expuesta la doctrina relevante para efectuar el enjuiciamiento que nos ocupa, el siguiente paso de nuestro análisis debe dirigirse a determinar si un ordenador personal puede ser un medio idóneo para el ejercicio de la intimidad personal, resultando entonces necesario para acceder a su contenido el consentimiento de su titular o que se den los presupuestos que legalmente habilitan la intromisión, de acuerdo con los parámetros constitucionales antes desarrollados.

A tal fin conviene empezar recordando que este Tribunal ha reseñado, ya en su STC 110/1984, de 26 de noviembre, que “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. Lo ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado 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” (FJ 3). En el mismo sentido, en la STC 119/2001, de 24 de mayo, afirmábamos que “estos derechos han adquirido también una dimensión positiva en relación con el libre desarrollo de la personalidad, orientada a la plena efectividad de estos derechos fundamentales. En efecto, habida cuenta de que nuestro texto constitucional no consagra derechos meramente teóricos o ilusorios, sino reales y efectivos [...], se hace imprescindible asegurar su protección no sólo frente a las injerencias ya mencionadas, sino también frente a los riesgos que puedan surgir en una sociedad tecnológicamente avanzada. A esta nueva realidad ha sido sensible la jurisprudencia del Tribunal Europeo de Derechos Humanos, como se refleja en las Sentencias de 21 de febrero de 1990, caso Powell y Rayner contra Reino Unido; de 9 de diciembre de 1994, caso López Ostra contra Reino de España, y de 19 de febrero de 1998, caso Guerra y otros contra Italia” (FJ 5).

En armonía con lo anterior, este Tribunal ha venido describiendo casuísticamente una serie de supuestos, en que, con independencia de las libertades tradicionales antes mencionadas, ha podido sobrevenir una injerencia no admisible en el ámbito de la vida privada e íntima de la persona. Así, hemos afirmado que “el derecho a la intimidad comprende la información relativa a la salud física y psíquica de las personas, quedando afectado en aquellos casos en los que sin consentimiento del paciente se accede a datos relativos a su salud o a informes relativos a la misma” (SSTC 70/2009, de 23 de marzo, FJ 2 y 159/2009, de 29 de junio, FJ 3). También hemos dicho que “no hay dudas de que, en principio, los datos relativos a la situación económica de una persona entran dentro de la intimidad constitucionalmente protegida” (STC 233/1999, de 16 de diciembre, FJ 7), que “en las declaraciones del IRPF se ponen de manifiesto datos que pertenecen a la intimidad constitucionalmente tutelada de los sujetos pasivos” (STC 47/2001, de 15 de febrero, FJ 8), y que “la información concerniente al gasto en que incurre un obligado tributario, no sólo forma parte de dicho ámbito, sino que a través de su investigación o indagación puede penetrarse en

la zona más estricta de la vida privada o, lo que es lo mismo, en los aspectos más básicos de la autodeterminación personal del individuo”. (STC 233/2005, de 26 de septiembre, FJ 4). Por otra parte, en la STC 70/2002, de 3 de abril, en que un guardia civil había intervenido a un detenido una agenda personal y un documento que se encontraba en su interior, sostuvimos que “con independencia de la relevancia que ello pudiera tener a los fines de la investigación penal y, por tanto, de su posible justificación, debemos afirmar que la apertura de una agenda, su examen y la lectura de los papeles que se encontraban en su interior supone una intromisión en la esfera privada de la persona a la que tales efectos pertenecen, esto es, en el ámbito protegido por el derecho a la intimidad, tal como nuestra jurisprudencia lo define” (FJ 10). Finalmente, cabe recordar que en la STC 14/2003, de 28 de enero, FJ 6, afirmamos que la reseña fotográfica de un detenido, obtenida durante su permanencia en dependencias policiales, “ha de configurarse como un dato de carácter personal”, respecto del cual los miembros de las fuerzas y cuerpos de seguridad del Estado “están obligados en principio al deber de secreto profesional”.

Si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) – por lo que sus funciones podrían equipararse a los de una agenda electrónica-, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o

recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o “email”, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información.

4. En este mismo sentido diversas disposiciones tomadas a nivel europeo se han ocupado de esta materia. Así procede citar en primer lugar el Convenio núm. 108 del Consejo de Europa sobre protección de los datos informatizados de carácter personal (1981), vinculante para España, y las Recomendaciones del Comité de Ministros que lo desarrollan, en particular, la Recomendación sobre datos personales utilizados en el sector policial (1987) y la Recomendación sobre privacidad en Internet (1999). El preámbulo de esta última Recomendación - R(99) 5, de 23 de febrero de 1999 - pone de relieve que "el desarrollo de las tecnologías y la generalización de la recogida y del tratamiento de datos personales en las 'autopistas de la información' suponen riesgos para la intimidad de las personas naturales" y que "las comunicaciones con ayuda de las nuevas tecnologías de la información están también sujetas al respeto de los derechos humanos y de las libertades fundamentales, en concreto al respeto a la intimidad y del secreto de las comunicaciones, tal y como se garantizan en el artículo 8 de la Convención Europea de los Derechos Humanos". Además, recuerda esta Recomendación que "el uso de Internet supone una responsabilidad en cada acción e implica riesgos para la intimidad" (Introducción), por cuanto cada visita a un sitio de Internet deja una serie de "rastros electrónicos" que pueden utilizarse para establecer "un perfil de su persona y sus intereses" (apartado II, 2), subrayando también que la dirección de correo electrónico constituye "un dato de carácter personal que otras personas pueden querer utilizar para diferentes fines" (apartado II, 6).

En este mismo orden de cosas debe citarse la acción normativa desarrollada por la Unión Europea, entre la que destaca a los efectos del presente asunto, además de la consagración del derecho a la protección de los datos personales realizada por el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos

personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, cuyo considerando núm. 6 resalta que “Internet esta revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas. 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”. Además, recuerda en su considerando núm. 24 que “los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales”, advirtiendo que “los denominados programas espías (Spyware), web bugs, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intromisión en la intimidad de dichos usuarios”.

También cabe citar las Resoluciones del Parlamento Europeo de 17 de septiembre de 1996 y de 17 de diciembre de 1998, ambas sobre el respeto de los derechos humanos en la Unión Europea, la primera en cuanto dispone en su apartado 53 que "el respeto de la vida privada y familiar, de la reputación, del domicilio y de las comunicaciones privadas, tanto de las personas físicas como jurídicas, así como la protección de datos de carácter personal son derechos fundamentales básicos respecto de los cuales los Estados miembros deben ejercer una especial protección, habida cuenta de la incidencia negativa que sobre los mismos tienen las nuevas tecnologías y que sólo la armonización de las legislaciones nacionales en la materia, confiriendo una alta protección, es susceptible de responder a este desafío", y la segunda, al subrayar en su apartado 23 que "el derecho al respeto de la vida privada y familiar, del domicilio y de la correspondencia, así como a la protección de los datos de carácter personal, representan derechos fundamentales que los Estados tienen la obligación de proteger y que, por consiguiente, toda medida de vigilancia óptica, acústica o informática deberá adoptarse dentro de su más estricto respeto y acompañada en todos los casos de garantías judiciales".

El Tribunal de Justicia de la Unión Europea ha reafirmado también la importancia del derecho a la protección de los datos personales como un elemento a tomar en consideración

no sólo en el momento de transponer una Directiva sino también cuando las autoridades estatales y los órganos judiciales nacionales procedan a su aplicación (entre otras, Sentencia del Tribunal de Justicia (Gran Sala) de 29 de enero de 2008, asunto C-275/06, Productores de Música de España (Promusicae) c. Telefónica de España SAU, apartados 61-70). Por su parte, el Tribunal Europeo de Derechos Humanos ha venido asumiendo una interpretación extensiva del concepto “vida privada” del art. 8 del Convenio Europeo de Derechos Humanos y de las Libertades Fundamentales. Así, su Sentencia de 16 de febrero de 2000, dictada en el caso Amman contra Suiza, considera que “el término ‘vida privada’ no se debe interpretar de forma restrictiva”, de forma que éste “engloba el derecho del individuo de crear y desarrollar relaciones con sus semejantes”, sin que “ninguna razón de principio permita excluir las actividades profesionales o comerciales” (§ 65). De manera específica, la STEDH de 3 de abril de 2007, caso Copland contra el Reino Unido, considera en su § 41 que están incluidos en el ámbito de protección del art. 8 del Convenio Europeo, por cuanto pueden contener datos sensibles que afecten a la intimidad, tanto “los correos electrónicos enviados desde el lugar del trabajo” como “la información derivada del seguimiento del uso personal de Internet”. En este caso, precisa el Tribunal, a la demandante no se le advirtió de que podría ser objeto de un seguimiento, por lo que podía razonablemente esperar que se reconociera el carácter privado “en lo que respecta al correo electrónico y la navegación por Internet”. (§ 42). Por su parte, la STEDH de 22 de mayo de 2008, caso Iliya Stefanov contra Bulgaria, consideró que el registro de la oficina de un abogado, incluyendo los datos electrónicos, equivale a una injerencia en su “vida privada”, lesiva por ello del art. 8 del Convenio. (§ 34). No obstante reconocer el Tribunal que concurría en este caso un objetivo legítimo (investigación penal por delito de extorsión) y que existía una previa autorización judicial, siendo así que “los registros del PC y las incautaciones deben, por regla general, llevarse a cabo en virtud de una orden judicial” (§ 39), razona que la expresada orden se había elaborado en términos excesivamente amplios, ejecutándose además de manera desproporcionada por la Policía, por lo que se había afectado al secreto profesional, por cuanto “retiró todo el equipo del solicitante, incluyendo sus accesorios, así como todos los disquetes que se encontraban en su oficina”, resultando que durante el tiempo que permaneció este material en su poder “ningún tipo de garantías existen para asegurar que durante el periodo intermedio el contenido completo del disco duro y los discos no fueron inspeccionados o copiados” (§ 42). De lo expuesto, parece desprenderse que cualquier injerencia en el contenido de un ordenador personal –ya sea por vía de acceso remoto a través de medios técnicos, ya, como en el presente caso, por vía manual- deberá

venir legitimada en principio por el consentimiento de su titular, o bien por la concurrencia de los presupuestos habilitantes antes citados.

Tal conclusión, por otra parte, parece desprenderse, si bien de manera indirecta, del contenido de la Sentencia de este Tribunal Constitucional 34/2009, de 9 de febrero, en la que apreciamos que no se había infringido por el órgano judicial el principio de legalidad penal al haber condenado el demandante por un delito de descubrimiento y revelación de secretos, cuyo bien jurídico protegido es la intimidad, resultando como hechos probados que este había accedido al ordenador de una compañera de trabajo y había procedido a la lectura de sus mensajes de correo electrónico. En particular, reseñábamos que “Desde la estricta perspectiva de control que corresponde a este Tribunal en modo alguno cabe tildar a la vista del tipo penal previsto del art. 197.1 y 2 CP de aplicación analógica o *in malam* parte, carente de razonabilidad por apartarse de su tenor literal o por utilización de pautas extravagantes o criterios no aceptados por la comunidad jurídica la llevada a cabo por la Audiencia Provincial, al considerar documentos personales e íntimos la libreta de direcciones y de teléfonos de la denunciante, accediendo por este medio a la dirección de su correo electrónico y subsumir en aquel tipo penal el acceso a dichos documentos sin el consentimiento de su titular, obteniendo de esta forma datos de carácter personal de aquella y de sus compañeros, que es la conducta por la que ha sido condenado el recurrente de amparo” (FJ6). A la misma conclusión hemos llegado respecto del acceso a los datos almacenados en un teléfono móvil en la STC 230/2007, de 5 de noviembre, si bien declarando vulnerado en tal caso el art. 18.3 CE al haberse accedido por la Guardia Civil al registro de llamadas memorizado en el terminal intervenido al recurrente, confeccionando un listado de llamadas recibidas, enviadas y perdidas, sin su consentimiento ni autorización judicial (FJ 2).

5. Expuesto lo anterior, resulta conveniente analizar por separado las dos conductas que el demandante de amparo considera lesivas del derecho a la intimidad, comenzando por la del encargado del establecimiento de informática, consistente en acceder a la carpeta llamada “mis documentos / mis imágenes” de su ordenador personal, en la que encontró diversos archivos fotográficos de contenido pedófilo que motivaron la interposición de la denuncia.

Según se desprende de los antecedentes, el recurrente acudió al establecimiento de informática que regentaba el denunciante y le hizo entrega de su ordenador portátil con el

encargo de cambiar la grabadora que no funcionaba. Consta también acreditado que al recibir el encargo el titular del establecimiento preguntó al recurrente si el ordenador tenía contraseña de acceso, respondiendo éste negativamente y sin manifestar limitación alguna en el uso del ordenador y acceso a los ficheros que almacenaba. Una vez efectuada la reparación y para comprobar el correcto funcionamiento de las piezas sustituidas el encargado escogió al azar diversos archivos para proceder a su grabación y posterior reproducción en el ordenador, lo que, al parecer, suele ser práctica habitual en estos casos, visualizando entonces las imágenes pornográficas de los menores que contenía. El testigo puso entonces tal circunstancia en conocimiento de la Policía Nacional que procedió a la intervención del portátil.

Como hemos afirmado anteriormente, corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno, por lo que el consentimiento del titular del derecho fundamental legitimará la inmisión en el ámbito de la intimidad e impedirá, por tanto, considerarlo vulnerado. En lo relativo a la forma de este consentimiento hemos puesto de relieve que puede manifestarse de forma expresa, prestándose entonces verbalmente, o bien tácita. En este caso la conducta analizada no es por sí misma reveladora de una declaración de voluntad, sino que de dicha conducta se infiere que debió concurrir tal voluntad. Por ello, se conceptúan estas declaraciones como tácitas, porque resultan, no de expresiones, sino de hechos (actos concluyentes), siendo preciso, para conocer su verdadero significado, acudir a conjeturas o presunciones.

En el presente caso, más allá del tradicional marco conceptual de la forma de la prestación del consentimiento a que se ha hecho referencia, es preciso analizar las características de la declaración de voluntad en realidad emitida por el propietario del ordenador personal. Éste, es verdad, como dice el Fiscal, no autorizó de forma expresa al encargado de la tienda de informática a acceder al contenido de sus archivos o ficheros donde se encontraban las fotografías y videos de contenido pedófilo, ni tampoco tácitamente porque nos encontramos ante una manifestación de voluntad efectuada por su parte, por lo que no es necesario acudir a conjeturas o presunciones sobre los hechos para su interpretación. Dicho lo anterior, lo que sí se aprecia claramente en el recurrente es la concurrencia de una declaración expresiva de su voluntad de hacer entrega a dicho encargado de su portátil, poniéndolo a su disposición, para que éste procediera a su reparación (en concreto, para cambiar la grabadora que no funcionaba). Para ello le informa, incluso, como hemos visto, que no precisa de contraseña alguna de acceso. Las razones que hayan podido llevar al recurrente a adoptar esta

actitud, ya sean debidas a negligencia, descuido o desconocimiento del carácter ilícito de los referidos archivos (en este sentido, se observa en las actuaciones que una de las alegaciones de su línea defensiva fue invocar precisamente un supuesto error de prohibición) escapan, evidentemente, al análisis que debe realizarse en este Tribunal Constitucional. Así las cosas, durante el desempeño de la función encomendada, el responsable del establecimiento informático descubrió casualmente el material pedófilo, en particular cuando, una vez reparado el ordenador, procedía a comprobar su correcto funcionamiento. A tal fin, escogió al azar diversos archivos para llevar a cabo su grabación y posterior reproducción, lo que le permitiría conocer el correcto funcionamiento de las piezas sustituidas, práctica que, según se acreditó durante el juicio, constituye el protocolo habitual en estos casos. De lo expuesto, se deduce que dicho responsable no se extralimitó del mandato recibido estando amparado su proceder, que ha llevado al descubrimiento del material ilícito, por la propia autorización expresa del ahora demandante. Avala esta conclusión la circunstancia de que este encargado limitara su actuación a la carpeta “mis documentos” del usuario, mínimo necesario para realizar la referida prueba de grabación, sin pretender adentrarse en otras carpetas respecto de las que, por hallarse más ocultas o por expresarlo así el título asignado a las mismas, pudiera presumirse un mayor revestimiento de protección y reserva. Seguidamente, una vez producido el hallazgo, este se limitó a cumplir con la obligación que le viene legalmente impuesta a todo ciudadano consistente en denunciar ante las autoridades competentes la posible perpetración de un delito público del que ha tenido conocimiento (arts. 259 y ss. L.E.Crim).

En consecuencia, podemos descartar que la conducta desarrollada por el denunciante vulnerara el derecho a la intimidad del recurrente (art. 18.1 CE), por haber sufrido este una supuesta intromisión indebida en su esfera íntima. [...]

6. Procede seguidamente analizar la legitimación de la actuación policial, una vez que el propietario de la tienda de informática presentó la denuncia e hizo entrega del ordenador, al haber procedido a revisar su contenido sin autorización judicial.

Según consta en las actuaciones, dicho responsable, en efecto, compareció en fecha 18 de diciembre de 2007 en el Grupo de delitos tecnológicos y contra la propiedad industrial de la Brigada Provincial de Policía Judicial de Sevilla, donde informó a los agentes del material pedófilo que había descubierto casualmente al acceder a la carpeta “mis documentos / mis imágenes”, haciendo entrega en dicho acto del portátil. También facilitó los datos

identificativos del cliente e, incluso, le reconoció fotográficamente en una composición que le fue exhibida a tal fin. Por la Policía se procedió entonces a encender el ordenador entregado, accediendo ésta, no sólo a la carpeta “mis documentos”, sino también a la carpeta denominada “Incoming”, perteneciente al programa de intercambio de archivos “eMule”. Poco después de la diligencia de acceso al ordenador, al día siguiente, se procede a la detención del denunciado, quien es oído en manifestación en las dependencias policiales. Concluido el atestado, en el que obra una diligencia de remisión del ordenador al Grupo de Pericias Informáticas de dicha Brigada Provincial para que se realizara un análisis más exhaustivo de su contenido, el detenido es puesto a disposición judicial el 20 de diciembre del mismo año. En la misma fecha el Juez de Instrucción en funciones de guardia dictó Auto incoando diligencias previas, realizando como primera actuación procesal la de oír en declaración al agente policial que había intervenido como instructor del referido atestado, quien dio las explicaciones necesarias.

Con estos antecedentes, lo primero que cabe afirmar es que la autorización que el recurrente prestó para el acceso a su ordenador al propietario del establecimiento de informática, en la forma expuesta, no puede extenderse al posterior acceso a los archivos por parte de la Policía. Tal como hemos afirmado anteriormente, el derecho a la intimidad personal se vulnera también cuando, aun autorizada su intromisión en un primer momento, se subvierten después los términos y el alcance para el que se otorgó. Como hemos visto, en el presente caso el alcance de la autorización dada se circunscribía a la manipulación por parte de dicho profesional del portátil para que procediera a la reparación del equipo informático, lo que no puede erigirse en legitimación para una intervención posterior realizada por personas distintas y motivada por otros fines. Lo contrario significaría asignar a un acto concreto de autorización una eficacia genérica *erga omnes* y temporalmente indeterminada, argumento que, sin duda, se revela contrario a los márgenes de disponibilidad de los derechos fundamentales, basados en la voluntad de su titular y cuyo alcance sólo a él corresponde delimitar. Esta conclusión aparece, además, avalada por la circunstancia de que los funcionarios policiales no se limitaron, una vez incautado el ordenador, a acceder, tal como había efectuado el denunciante, a la carpeta "mis documentos" del usuario, sino que ampliaron su análisis supervisando en particular la carpeta "eMule/Incoming", como hemos dicho.

Conviene reseñar en este momento que fue el hallazgo de este último programa, que estaba configurado de forma que los archivos pedófilos depositados en el ordenador pudieran ser descargados por otras personas a través de Internet, lo que ha fundado la condena del recurrente por la modalidad específica de distribución de material pornográfico infantil del art. 189.1 b) CP. En este sentido, tampoco el hecho de que el recurrente permitiera, a través del programa "eMule" este acceso de otros usuarios a sus archivos, puede erigirse en una suerte de autorización genérica frente a posteriores y distintas injerencias en el ámbito reservado de su intimidad, a pesar de que ha sido éste el argumento utilizado aquí tanto por la Audiencia Provincial de Sevilla como por la Sala Segunda del Tribunal Supremo. En efecto, además de que el acceso a los expresados archivos sólo es factible para los usuarios que tengan instalada su misma aplicación, es lo cierto que la Policía tan solo tiene conocimiento de la utilización del referido programa cuando accede al ordenador, siendo así que, conforme hemos expuesto, las circunstancias que permiten afirmar la existencia del presupuesto habilitante para penetrar en la esfera de la intimidad del titular del derecho deben evaluarse y apreciarse *ex ante*, sin que dicho acceso pueda justificarse *ex post* a partir de hechos sólo descubiertos después y como consecuencia del mismo.

7. Descartada la existencia de una autorización por parte del recurrente que facultase a la policía para supervisar su ordenador personal, nos corresponde analizar si, en todo caso, su actuación ha podido estar motivada por la concurrencia de otros bienes jurídicos constitucionalmente protegidos, de forma que se aprecie una justificación objetiva y razonable para la injerencia en su derecho a la intimidad personal.

Puede afirmarse, sin necesidad de una mayor argumentación, que la conducta adoptada por la Policía perseguía un fin legítimo, por cuanto se enmarcaba dentro de las investigaciones que ésta realizaba dirigidas al esclarecimiento de un delito de pornografía infantil. Al propio tiempo existe la habilitación legal necesaria para la realización, por parte de los agentes intervinientes, de este tipo de pesquisas, pues, como hemos visto, se encuentran entre sus funciones las de practicar las diligencias necesarias para comprobar los delitos, descubrir sus autores y recoger los efectos, instrumentos o pruebas, pudiendo efectuar “un primer análisis” de los efectos intervenidos (en este sentido, se observa en el propio atestado policial cómo su instructor califica el informe realizado sobre el contenido del ordenador como “un análisis preliminar”, sin perjuicio de la pericial que luego se solicita al Grupo

especializado de Pericias Informáticas). Finalmente, si bien la intervención policial desplegada no contó con la previa autorización judicial, circunstancia ésta que ha llevado a considerar, tanto al recurrente como al Fiscal, que se había producido en este caso una vulneración del derecho a la intimidad personal, podemos afirmar que nos encontramos ante uno de los supuestos excepcionados de la regla general, que permite nuestra jurisprudencia, pues existen y pueden constatarse razones para entender que la actuación de la Policía era necesaria, resultando, además, la medida de investigación adoptada razonable en términos de proporcionalidad.

Dicho lo anterior, y con independencia de la necesidad de que el legislador regule esta materia con más precisión, avala esta última conclusión la circunstancia de que los funcionarios intervinientes actuaron ante la *notitia criminis* proporcionada por el propietario de una tienda de informática, quien se personó en las dependencias policiales informando acerca del material pedófilo que había encontrado en un ordenador personal. Con esta actuación, los expresados agentes pretendían, con la conveniente celeridad que requerían las circunstancias, comprobar la veracidad de lo ya descubierto por este ciudadano, así como constatar si existían elementos suficientes para la detención de la persona denunciada. Hemos de valorar, además, que la investigación se circunscribía de manera específica a un delito de distribución de pornografía infantil, lo que resulta relevante, no sólo por la modalidad delictiva y la dificultad de su persecución penal al utilizarse para su comisión las nuevas tecnologías e Internet, sino fundamentalmente en atención a la gravedad que estos hechos implican, derivada ésta de la pena que llevan aparejados por referirse a víctimas especialmente vulnerables.

En esta dirección, la Decisión del Consejo de la Unión Europea de 29 de mayo de 2000, relativa a la lucha contra la pornografía infantil en Internet, luego de advertir en su introducción que “la producción, tratamiento, posesión y difusión de material pornográfico infantil pueden representar una modalidad importante de la delincuencia internacional organizada, cuya envergadura dentro de la Unión Europea suscita cada vez mayor preocupación”, insta a los Estados miembros en su artículo 1 a que adopten las medidas necesarias para “garantizar una actuación rápida de las autoridades policiales” en cuanto reciban información sobre estos casos y para “animar a los usuarios de Internet a que comuniquen a las autoridades policiales, directa o indirectamente, sus sospechas sobre la difusión de material pornográfico en Internet, cuando encuentren material de este tipo”. Por su

parte, la Decisión Marco del mismo Consejo de 22 de diciembre de 2003, sobre la lucha contra la explotación sexual de los niños y la pornografía infantil, tras resaltar también en su parte introductoria que la pornografía infantil constituye “una violación de los derechos humanos y del derecho fundamental del niño a una educación y un desarrollo armonioso”, describe en su artículo 5 las especiales penas privativas de libertad y las circunstancias agravantes que los Estados miembros han de aplicar en este tipo de infracciones.

Por otra parte, adquiere especial relevancia en este caso la función que se encomienda a la Policía Judicial de asegurar las pruebas incriminatorias, debiendo destacarse que en estas infracciones, a diferencia de lo que generalmente ocurre con ocasión de otro tipo de intervenciones (p.ej. telefónicas o postales), el delito se comete en la red, por lo que el ordenador, no sólo es el medio a través del cual se conoce la infracción, sino fundamentalmente la pieza de convicción esencial y el objeto de prueba. En este supuesto, hay que tener en cuenta que la persona denunciada no estaba detenida cuando se practica la intervención, por lo que tampoco aparece como irrazonable intentar evitar la eventualidad de que mediante una conexión a distancia desde otra ubicación se procediese al borrado de los ficheros ilícitos de ese ordenador o que pudiera tener en la “nube” de Internet. En todo caso, también aparece como un interés digno de reseñar la conveniencia de que por parte de los funcionarios policiales se comprobara con la conveniente premura la posibilidad de que existiesen otros partícipes, máxime en este caso en que se utilizó una aplicación informática que permite el intercambio de archivos, o que, incluso, detrás del material pedófilo descubierto, pudieran esconderse unos abusos a menores que habrían de acreditarse.

A estas apreciaciones, habría de añadirse que la actuación policial respetó el principio de proporcionalidad, pues se trata de una medida idónea para la investigación del delito (del terminal informático se podían extraer -como así fue- pruebas incriminatorias y nuevos datos para la investigación), imprescindible en el caso concreto (no existían otras menos gravosas) y fue ejecutada de tal modo que el sacrificio del derecho fundamental a la intimidad no resultó desmedido en relación con la gravedad de los hechos y las evidencias existentes. En este punto, merece subrayarse que el órgano judicial no estuvo durante un espacio prolongado de tiempo al margen de la iniciativa adoptada por la Policía, pues ésta inmediatamente (a los dos días) dio cuenta al Juez de Instrucción, pudiendo entonces éste hacer la conveniente ponderación sobre si dicha diligencia estaba o no justificada, después de oír, como hemos visto, al instructor del atestado instruido.

De todo lo cual cabe concluir que, siendo la actuación policial constitucionalmente legítima, el sacrificio del derecho fundamental afectado estaba justificado por la presencia de otros intereses constitucionalmente relevantes, no pudiendo apreciarse vulneración alguna del derecho a la intimidad personal del recurrente.

8. Finalmente, se alega en la demanda la vulneración del derecho a un proceso con todas las garantías y a la presunción de inocencia (art. 24.2 CE), al haberse utilizado en el proceso por el órgano judicial para la condena la diligencia de apertura y examen por la Policía del ordenador personal, reputada prueba ilícita según lo expuesto por el recurrente, resultando que el resto de los elementos probatorios ponderados derivarían de esta actuación. Es decir, según se infiere de la demanda, las demás pruebas practicadas en el juicio oral proceden del hallazgo de los archivos ilícitos, no existiendo ninguna de ellas que tenga un carácter autónomo, por lo que deberían de considerarse, a su vez, ilícitas según lo dispuesto en el art. 11.1 de la Ley Orgánica del Poder Judicial al tratarse de pruebas obtenidas indirectamente con vulneración del derecho fundamental a la intimidad personal (art. 18.1 CE). De este modo, la exclusión probatoria abarcaría, no sólo al referido descubrimiento, sino también a las declaraciones del denunciante y de los propios funcionarios policiales intervinientes, pues estos elementos probatorios nunca se habrían producido sin aquella intervención. Además, no puede servir como elemento incriminatorio el contenido del testimonio prestado por el acusado en el juicio oral, pues en este acto se acogió a su derecho a no declarar y el Ministerio Público no interesó la lectura de sus declaraciones prestadas en fase de instrucción.

No obstante lo anterior, descartada la nulidad de la expresada diligencia al no apreciarse lesión alguna del derecho reconocido en el art. 18.1 CE, tal como hemos desarrollado ampliamente, no cabe apreciar tampoco la nulidad subsiguiente de las restantes pruebas practicadas, por lo que también resulta procedente rechazar el presente motivo de amparo. En todo caso, concurre en este supuesto prueba de cargo suficiente y practicada con todas las garantías para enervar el derecho a la presunción de inocencia del acusado, habiendo consistido ésta, no sólo en el dato objetivo del hallazgo de los archivos de contenido pedófilo, susceptibles de ser distribuidos a terceros, sino también en los testimonios del propietario del establecimiento de informática que presentó la denuncia y del funcionario policial instructor del atestado, así como en el contenido del informe pericial elaborado por el Grupo de Pericias

Informáticas de la Policía Judicial, debidamente incorporado a las actuaciones e introducido en el plenario para su discusión por las partes.

En definitiva, ha de concluirse que la condena del demandante como autor de un delito de distribución de material pornográfico infantil del art. 189.1 b) CP se sustenta en pruebas de cargo válidamente practicadas, al haberse acomodado a las exigencias constitucionales, mediante un razonamiento debidamente explicitado en las resoluciones judiciales, como hemos comprobado, que no puede calificarse de irrazonable, puesto que los datos tenidos en cuenta resultan suficientemente concluyentes, sin que a este Tribunal le competa realizar ningún otro juicio ni entrar a examinar otras inferencias propuestas por quien solicita el amparo (SSTC 206/2007, de 24 de septiembre, FJ 4; 219/2009, de 21 de diciembre, FJ 9 y 134/2010, de 2 de diciembre, FJ 9, entre otras).

F A L L O

En atención a todo lo expuesto, el Tribunal Constitucional, POR LA AUTORIDAD QUE LE CONFIERE LA CONSTITUCIÓN DE LA NACIÓN ESPAÑOLA,

Ha decidido

Desestimar la demanda de amparo presentada por don Carlos Trabajo Rueda.

Publíquese esta Sentencia en el “Boletín Oficial del Estado”.

Dada en Madrid, a siete de noviembre de dos mil once.