**Tribunal Supremo (Sala de lo Penal, Sección 1ª).Sentencia núm. 1328/2009 de 30 diciembre**

***RESUMEN: CONCEPTO DE DATOS RESERVADOS DE CARÁCTER FAMILIAR O PERSONAL: ART.197 C.P.; "libertad informática":*** *médico coordinador de Centro de Salud que de manera subrepticia entra en el historial médico de un colega para averiguar su médico de cabecera: dato inocuo.*

El TS declara haber lugar al recurso de casación interpuesto contra la Sentencia de 11de febrero de 2009, dictada por la Audiencia Provincial de Palma de Mallorca, Sección Primera, absolviendo al recurrente del delito continuado de acceso a datos reservados de carácter personal.

## I. ANTECEDENTES DE HECHO:

El acusado Juan Carlos, mayor de edad y sin antecedentes penales, en su condición de médico coordinador del Centro de Salud, accedió en dos ocasiones, a través del programa informatizado de consulta clínica, al Historial clínico del también médico en el mismo Centro, Bienvenido, y obtuvo así el dato allí registrado referente al nombre de su médico de cabecera. Dichos accesos, producidos sin conocimiento ni autorización de aquél y sin que existiera entre ambos ninguna relación asistencial; el primero, que el acusado ejecutó directamente desde el terminal informático de su despacho y el segundo, realizado por la enfermera del centro Adoración por orden expresa y directa del acusado.

El modo en que dichos accesos fueron realizados a través del programa informático consistió, en ambos casos, en introducir informáticamente el nombre de Bienvenido en la hoja informatizada de pacientes del día del médico acusado y, desde ella, acceder la pantalla en la que aparecen, entre otros, el icono "ficha del paciente", introducirse en él y visualizar el dato referido.

No consta debidamente acreditado que, además, accediera a algún otro dato de la historia clínica del Dr. Bienvenido.

La Audiencia de instancia dictó el siguiente pronunciamiento:
FALLO: Que debemos condenar y condenamos a Juan Carlos como autor responsable de un delito continuado de acceso a datos reservadas de carácter personal precedentemente definido, sin circunstancias modificativas de la responsabilidad criminal e inhabilitación absoluta por un periodo. En el orden civil, Juan Carlos abonará a Bienvenido, en concepto de indemnización por daño moral.

Se preparó recurso de casación por quebrantamiento de forma, infracción de precepto constitucional e infracción de Ley, por Juan Carlos

## II. FUNDAMENTOS DE DERECHO DE INTERÉS:

SEXTO

Articula a continuación la parte cuatro motivos de casación por infracción de Ley, **por aplicación indebida del** art. 197.2, in fine del C.P., alegando en síntesis que el nombre del médico de cabecera del Dr. Bienvenido era de acceso permitido al personal administrativo, enfermeras, médicos y al coordinador del Centro de Salud, por lo que el recurrente en su doble condición de médico del IB. Salud y Coordinador del Centro de Salud estaba autorizado a conocerlo (**motivo cuarto);** que el recurrente actuó en la creencia de que como médico y como coordinador del Centro de Salud estaba autorizado a conocer el nombre del médico de Dr. Bienvenido y por tanto, actuó sin dolo ( **motivo quinto),** que el conocimiento del dato personal consistente en la identidad del médico de cabecera del Dr. Bienvenido por parte del recurrente, médico del Ib Salud y Coordinador del Centro de Salud no es un dato protegido penalmente ( **motivo sexto);** y que toda vez que el delito se consuma tan pronto como el sujeto activo "accede" a los datos, ha de entenderse que la norma refiere la existencia de un perjuicio añadido para que la violación de la reserva integre el tipo; perjuicio añadido que no se da en el presente caso ( **motivo séptimo),** motivos todos que en cuanto afectan a la estructura típica y requisitos del delito del art. 197.2 pueden ser analizados conjuntamente.

Siendo así debemos recordar que el art. 197.2 se encuentra ubicado en el capitulo primero "Del descubrimiento y revelación de secretos, del Titulo X del Libro II del Código Penal que se rotula como "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio".

En este sentido los derechos a la intimidad personal y a la propia imagen garantizados por el art. 18.1 C.E., forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida privada. Salvaguardan estos derechos un espacio de intimidad personal y familiar que queda sustraído a intromisiones extrañas, destacando la necesaria protección frente al creciente desarrollo de los medios y procedimiento de captación, divulgación y difusión de la misma y de datos y circunstancias que pertenecen a la intimidad.

Por intimidad, por tanto, se pueden entender diversos conceptos, siendo significativo a estos efectos que la terminología usada para referirse a dicho concepto varia en los distintos países, así en Italia se habla de "riservatezza", en Francia de "vie priveé", en los países anglosajones de "privacy", y en Alemania de "privatsphare", pero que vienen a coincidir en la existencia de una esfera de privacidad que cabe considerar secreto en el sentido de ser facultad de la persona su exclusión del conocimiento de terceros. El Código actual ha hecho además especial referencia a la llamada "libertad informática", ante la necesidad de conceder a la persona facultades de control sobre sus datos en una sociedad informatizada, siguiendo las pautas de la Ley Orgánica de Regulación del tratamiento Automatizado de Datos personas (LORTAD), relacionada con el Convenio del Consejo de Europa de 28 de enero de 1981 y la Directiva 95/46 del Parlamento de la Unión Europea relativos a la protección de tales datos y a su libre circulación.

Esta segunda dimensión de la intimidad conocida como libertad informática o **habeas data,** encuentra su apoyo en el **art. 18.4 CE**, en donde taxativamente se dispone que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". De esta proclamación se deriva su poder de acción del titular para exigir que determinados datos personales no sean conocidos, lo que supone reconocer un derecho a la autodeterminación informativa, entendido como libertad de decidir qué datos personales pueden ser obtenidos y tratados por otros. **La llamada libertad**

**informática significa, pues, el derecho a controlar el uso de los datos de carácter personal y familiar que pueden recogerse y tratarse informaticamente (habeas data); en particular -como señala la doctrina- entre otros aspectos, la capacidad del ciudadano para oponerse a que determinados datos personales sean utilizados para fines distintos de aquél legitimo que justificó su obtención: SSTC. 11/98 de 13 de enero y 45/99 de 22 de marzo.**

Esta evolución del **concepto de intimidad** puede apreciarse en la **jurisprudencia del Tribunal Constitucional** así en un primer momento la intimidad se configura como el derecho del titular a exigir la no injerencia de terceros en la esfera privada, concibiéndola pues, como un derecho de corte garantista o de defensa. En un segundo momento a partir de la STC. 134/99 de 15 de julio, la intimidad pasa a ser concebida como un bien jurídico que se relaciona con la libertad de acción del sujeto, con las facultades positivas de actuación para controlar la información relativa a su persona y su familia en el ámbito público: "el derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a una persona o a su familia, pudiendo imponer a terceros (sean estos simples particulares o poderes públicos, su voluntad de no dar a conocer dicha información, prohibiendo su difusión no consentida" (SSTC. 134/99 de 15 de julio y 144/99 de 22 de julio).

**En esta dirección la STS 358/2007 de 30 de abril destacó analizando el art. 197 C.P. que dicho precepto contiene varias conductas en una compleja redacción y sanciona en primer lugar al que se apodere de los papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales de otra persona, al quien interceptare las comunicaciones de otro y al que utilizare artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o la imagen o de cualquier otra señal de comunicación, en todos los casos sin su consentimiento y con la finalidad de descubrir sus secretos o vulnerar su intimidad. Se trata de conductas distintas que no precisan que el autor llegue a alcanzar la finalidad perseguida. En los dos primeros casos requiere sin embargo un acto de apoderamiento o de interceptación efectivos, mientras que en el supuesto de utilización de artificios basta con la creación del peligro que supone su empleo con las finalidades expresadas para la consumación de la infracción penal.**

**También sanciona a quien, sin estar autorizado, se apodere, en perjuicio de tercero, de datos reservados de carácter personal o familiar de otro, que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Así como a quien simplemente acceda a ellos por cualquier medio sin estar autorizado y a quien los altere o utilice en perjuicio del titular de los datos o de** un tercero.

El bien jurídico protegido es la intimidad individual. Aunque la idea de secreto puede ser más amplia, como conocimientos solo al alcance de unos pocos, en realidad deben estar vinculados precisamente a la intimidad pues esa es la finalidad protectora del tipo. En este sentido, la STS nº 666/2006, de 19 de junio, en la que se dice que "la idea de secreto en el art. 197, 1º C.P. resulta conceptualmente indisociable de la de intimidad: ese «ámbito propio y reservado frente a la acción y el conocimiento de los demás» (SSTC 73/1982 y 57/1994 entre muchas)". Así se desprende de la ubicación del precepto en el Título dedicado a los delitos contra la intimidad, y es coherente con su propia redacción, pues en el primer apartado relaciona los papeles, cartas o mensajes de correo electrónico con otros documentos o efectos personales. Y en el segundo apartado se refiere a datos reservados de carácter personal o familiar.

En relación a la conducta enjuiciada, interesa resaltar que **el tipo objetivo requiere**

**solamente un acto de apoderamiento, sin necesidad de que el autor llegue a descubrir los secretos o vulnerar la intimidad en el primer caso, y en el mero acceso de los datos protegidos en el segundo. El tipo subjetivo exige, sin embargo, aquella finalidad, junto con el dolo en el acto de apoderamiento o de acceso.**

Centrándonos en el análisis de los delitos recogidos en el segundo apartado del art. 197, éstos tienen un sentido claramente distinto a los recogidos en el apartado primero: ya que las conductas afectan a datos que no están en la esfera de custodia del titular, sino en bancos de datos y pueden causar perjuicios a terceros distintos del propio sujeto al que se refiere la información concernida.

Un sector doctrinal considera que en el art. 197.2 se protegen, en realidad, dos bienes jurídicos. Por una parte, la intimidad del sujeto pasivo, en relación con las conductas de apoderarse, acceder y utilizar los datos. Por otra parte, la integridad de los datos, en relación con los comportamientos de modificar o alterar. Distinción, no obstante, relativa por el hecho de quien pretende modificar o alterar, primero debe acceder, con lo que se habría lesionado también la intimidad en estas modalidades de conducta.

Consecuentemente, como ya hemos indicado, lo que se protege en este apartado segundo es la **libertad informática** entendida como **derecho del ciudadano a controlar la información personal y familiar que se encuentra recogida en ficheros de datos,** lo que constituye una dimensión positiva de la intimidad que constituye el bien jurídico protegido.

Según el art. 3 a) de la Ley Orgánica 15/99 de 13 de diciembre, de Protección de Datos de Carácter Personal (LPDP) **dato de carácter personal** es "**cualquier información concerniente a personas físicas identificadas o identificables”**. No se define, sin embargo, qué datos son reservados, ni siquiera se utiliza la denominación de datos de carácter familiar.

Advierte la doctrina que el calificativo de **reservado** carece en absoluto de sentido, debiendo descartarse -como después se analizará más extensamente- la tesis de que la protección penal haya de limitarse a solo cierto tipo de datos personales de mayor relevancia, con exclusión de otros, cuya protección quedaría reservada al ámbito administrativo. Prueba de que ello no es así lo proporciona el apartado 5º que agrava la pena que corresponde a las conductas realizadas sobre esos datos de especial relieve, lo que evidencia que los demás están incluidos dentro del apartado 2. Por ello en el sentido del tipo el entendimiento más adecuado del carácter reservado de los datos es considerar que son tales los que no son susceptibles de ser conocidos por cualquiera. El precepto insiste en ello al aclarar por partida doble que el delito lo comete el que accede a los datos o los utiliza "sin estar autorizado", evidencia de que no son datos al alcance de cualquiera.

Los datos, además, ha de estar **"recogidos (registrados) en ficheros o soportes** informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. **Fichero** es todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso (art. 3 b. LPDP). En el sentido del art. 197.2 debe exigirse que se trate de un conjunto organizado de información relativa a una generalidad de personas. Dado el carácter reservado de los datos, los ficheros o registros han de ser de acceso y utilización limitada a personas concretas y con finalidades especificas, siendo indiferente, su naturaleza: personal, académica o laboral, medica, económica, etc... Se trata, en realidad de informaciones de carácter personal relacionadas más con la privacidad que con la intimidad. No tienen por qué ser informativos, porque se acoge también a **cualquier otro tipo de archivo o registro** público o privado.

Las conductas van dirigidas a **datos que se hallen registrados,** es decir a bancos de datos preexistentes, entendiéndose por la doctrina que no es típica la creación clandestina de

bancos de datos, que queda en el ámbito administrativo sancionador.

**Se apodere** se ha interpretado por un sector doctrinal en sentido estricto como el apoderamiento que precisan los delitos contra el patrimonio. Otro sector se inclina por una interpretación más amplia, comprendiendo los supuestos en que se copian los datos, dejando intactos los originales o simplemente se capta, se aprehende, el contenido de la información, acepción en la que "apoderarse" resultaría **equivalente a acceder** al dato que se castiga también en el inciso final. **Utilizar** es usar sin apoderarse de ellos. **Modificar** es alterar los mismos, tanto si se trata de mejorar como de perjudicar la situación del sujeto al que afectan.

Las conductas tienen que producirse **sin estar autorizado** para acceder, manipular o modificar el banco de datos y realizarse **en perjuicio de tercero**, tercero que puede ser distinto al titular de los datos produciéndose una triple implicación de sujetos (sujeto activo, titular de lo datos y eventual perjudicado) que responde, a la idea de que el titular de los datos no puede ser sujeto activo del delito porque él es el sujeto pasivo, dado que lo tutelado es su intimidad.

NOVENO

En cuanto a la infracción denunciada en el motivo sexto cual es que el dato personal consistente en la identidad del médico de cabecera del Dr. Bienvenido por parte del recurrente, médico del Ib-Salud y Coordinador del Centro de Salud, no es un dato protegido penalmente, es necesario realizar unas consideraciones previas, tal como precisó la STS. 1461/2001 de 11 de julio:

a) En principio, todos los datos personales automatizados, son "sensibles" porque la Ley Orgánica de Regulación del Tratamiento de Datos Personales (LORTAD) 5/92 de 29 de octubre, no distingue a la hora de ofrecerles protección (veáse art. 2.1º y 3º de dicha Ley). Datos en principio, inocuos al informatizarlos, pueden ser objeto de manipulación, permitiendo la obtención de información.

No existen, por consiguiente, datos personales automatizados reservados y no reservados, por lo que debe interpretarse que todos los datos personales automatizados quedan protegidos por la comunicación punitiva del art. 197.2 C.P.

b) Tampoco hacen distinción alguna, ni la Ley vigente de Protección de Datos Personales, LO. 15/99 de 13 de diciembre, que ha sustituido a la LORTAD, ni la Directiva 95/46 de la Unión Europea, ni el Convenio del Consejo de Europa, en la propia LORTAD.

c) No es posible, a su vez, interpretar que "los datos reservados" son únicamente lo más sensibles, comprendidos en el "núcleo duro de la privacidad", (v.g. ideología, creencias, etc.) para quedar los no reservados en el grupo de los sancionables administrativamente, por cuanto dicho enfoque hermenéutico chocaría con una interpretación sistemática del art. 197 CP , ya que si en él se prevé un tipo agravado para esta clase de datos (numero 5) "a sensu contrario" los datos tutelados en el tipo básico, serian los no especialmente protegidos (o "no reservados") en la terminología de la Ley.

En consecuencia y en línea de principio, no importa la trascendencia e importancia objetiva de los datos personales y familiares. No cabe, pues, diferenciar a efectos de protección entre datos o elementos "objetivamente" relevantes para la intimidad que serian los únicos susceptibles de protección penal y datos "inocuos" cuya escasa significación los situaría directamente fuera de la intimidad penalmente protegida. En esta dirección la STS. 725/2004 de 11.6 nos dice que el art. 197. 2 CP no hace distinciones respecto del objeto de la acción que tengan fundamento en normas no penales y se refiere a "datos reservados de carácter

personal o familiar" registrados en soportes informáticos, electrónicos o telemáticos de archivos o registros públicos o privados. Es decir, que el legislador ha querido alcanzar todos los datos de estas características porque, indudablemente, todos son merecedores de protección penal.

Ahora bien si debe exigirse que los datos o información pertenezcan al ámbito privado y personal o familiar del sujeto. La STS. 358/2007 de 30 de abril, recordó que aunque en el segundo apartado del art. 197 se refiere a datos reservados de carácter personal o familiar, no siendo preciso que pertenezcan al núcleo duro de la privacidad, pues de ser así se aplicaría la agravación del apartado quinto del artículo 197 , si es necesario que afecten a la intimidad personal.

Hay que distinguir entre la irrelevancia "objetiva" del contenido e importancia de la información para que la protección penal opere en el caso de datos de carácter personal o familiar, a que se refiere el art. 197.2 , que, desde el punto de vista sustancial y aisladamente considerados, son generalmente inocuos; y la necesaria equiparación que debe establecerse entre "secreto" y "reservados" a efectos de la intimidad personal y familiar. En efecto de una interpretación teleológica y sistemática se debe concluir que el término reservados" que utiliza el Código hay que entenderlo como "Secretos" o "no públicos", parificándose de este modo el concepto con el art. 197.1 C.P. Secreto será lo desconocido u oculto, refiriéndose a todo conocimiento reservado que el sujeto activo no conozca o no esté seguro de conocer y que el sujeto pasivo no desea que se conozca.

DÉCIMO

En el caso actual, según los hechos probados, el único dato que el acusado obtuvo con uso inadecuado del programa informático de consulta clínica, fue el relativo al nombre del médico de cabecera del también médico del mismo Centro Bienvenido , no estando debidamente acreditado que, además accediera a algún otro dato de su historia clínica.

Resulta evidente que toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley, formando parte de su derecho a la intimidad (art. 7.1 Ley 41/2002 de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica).

La historia clínica definida en el art. 3 de esta ley como el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial, estaría comprendida en ese derecho a la intimidad, pero aunque en el Capitulo V historia clínica, en el art. 14 relativo a la definición y archivo de la historia clínica se señala que ésta comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, **con la identificación de los médicos** y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos en el ámbito de cada Centro, lo cierto es que el art. 15 relativo al contenido de la historia clínica de cada paciente, en el apartado 2 al especificar su contenido mínimo, en los dieciséis datos que enumera no se refiere al nombre del facultativo, dato, por tanto, que aunque pudiera referirse a la intimidad personal, no puede entenderse secreto o reservado de los efectos del tipo del art. 197.2 C.P., al tener la posibilidad de acceso al mismo cualquier persona a través de las formas que la propia acusación particular señaló en su escrito de conclusiones: a través del personal administrativo de cada Centro de Salud o Punto de Atención Continuada con consulta de la hoja de datos administrativos de cada paciente; llamando al servicio de cita

previa ("call center") al numero 902079079 y/0 contactando con los servicios de la Tarjeta Sanitaria de la Gerencia de atención Primaria.

Consecuentemente la propia Administración Sanitaria considera que no se debe proteger como dato accesible y privado el nombre del médico de cabecera, siendo un dato totalmente inocuo dentro del historial clínico del paciente, no pudiendo equipararse el acceso al conocimiento de un dato médico como puede ser el conocimiento de una enfermedad -máxime si es psíquica- con el acceso a un dato meramente administrativo.

Siendo así no resulta aplicable la propia jurisprudencia recogida en la sentencia recurrida (SSTS. De 18 de febrero de 1999, STS de julio de 2001, STS de 2 de diciembre de 2004, STS de 29 de septiembre de 2005 y STS de 18 de noviembre de 2005), el dato del médico de cabecera no es un dato que el hombre medio de nuestra cultura considera "sensible" por ser inherente al ámbito de su intimidad más estricta, dicho de otro modo, un dato perteneciente al reducto de los que, normalmente, se pretende no transciendan fuera de la esfera en que se desenvuelve la privacidad de la persona y de su núcleo familiar, pues es un dato de conocimiento público, al menos potencial -y no inherente a la intimidad, dato administrativo al alcance de todos los empleados del Centro- y no se trata de un dato personal secreto como "ámbito propio y reservado" frente a la acción y conocimiento de los demás (SSTC. 73/82 y 57/94).

En este punto debe resaltarse como la propia sentencia (FJ. Tercero apartado III) destaca como el Dr. Jesús Manuel ha afirmado que todo el mundo en el Centro de Salud (y no ha excluido al acusado) conocía que él era el médico de cabecera del Dr. Bienvenido (afirmación que ha de ponerse en relación con otra, hecha por el propio Dr. Bienvenido , relativa en una ocasión, tuvo un proceso de baja por un cuadro banal y su medico, que era el Dr. Jesús Manuel , le extendió la baja, la cual, debió entregar al coordinador del Centro -el acusado- lo que evidenciaría que éste tuvo conocimiento de quien era su médico.

Consecuentemente, la cuestión no reviste carácter penal, y en todo caso no quiere decir, que tal conducta no puede ser objeto de acción en el ámbito administrativo sancionador, que parece el cauce procesal idóneo para solucionar este tipo de conflictos, respetando el principio de mínima intervención inherente al Estado Social y Democrático del Derecho (art. 1.1 C.E. en el que la respuesta penal constituye la "ultima ratio" del Derecho).

UNDÉCIMO

El motivo por lo razonado debe ser estimado con la consiguiente absolución del recurrente, máxime cuando -como indica en el motivo séptimo, al amparo del art. 849.1 LECrim. por aplicación indebida del art. 197.2 C.P. Este artículo, en su inciso final preceptúa, según jurisprudencia de esta Sala, que el acceso a datos reservados debe hacerse en perjuicio del titular de los datos, perjuicio añadido al acceso que no se da en el presente caso.

Aun cuando la prosperabilidad del motivo precedente haría innecesario el estudio de la cuestión planteada, dado el contenido de la impugnación del Ministerio Fiscal y la jurisprudencia en cierto punto equivoca sobre este extremo, se entiende conveniente analizar el sentido y alcance de la expresión "en perjuicio de un tercero" del inciso primero del art. 197.2, y "en perjuicio del titular de los datos o de un tercero " de su inciso final.

Un sector doctrinal considera que "en perjuicio" es un elemento subjetivo del injusto, de manera que el propósito de perjudicar a otro debe presidir el apoderamiento, la utilización o modificación de los datos. El inconveniente que tiene esta postura es que aunque anticipa el momento de la intervención penal -pues la consumación ya no tiene que esperar a la efectiva producción de resultado alguno-, a la vez limita el ámbito de lo punible, pues solo los

comportamientos que vayan presididos de esa particular intención resultan típicas. Por ello otro sector de opinión estima que el "en perjuicio de tercero" no debe ser interpretado como un elemento subjetivo del injusto, sino como el resultado de la conducta, causalmente añadido a la simple utilización, modificación o al apoderamiento de los datos. Esta es la línea que siguió esta Sala en la STS. 234/99 de 18 de febrero, al matizar que **parece razonable que no todos los datos reservados de carácter personal o familiar puedan ser objeto del delito contra la libertad informática, puesto que, precisamente porque el delito se consuma tan pronto el sujeto activo "accede" a los datos, esto es, tan pronto los conoce y tiene a su disposición (...), es por lo que debe entenderse que la norma requiere la existencia de un perjuicio añadido para que la violación de la reserva integre el tipo, un perjuicio que puede afectar, como hemos visto, al titular de los datos o a un tercero, perjuicio que se produce siempre que se trata de un dato considerado "sensible" por ser inherente al ámbito de su intimidad más estricta.**

Es cierto que esta postura ha sido objeto de criticas al limitar los datos que causan un perjuicio apreciable a los datos "sensibles", los de mayor relevancia para la intimidad y ha sido matizada en otras posteriores, como la 1461/2001 de 11 de julio, que a la pregunta de si la expresión de tercero debe interpretarse como un plus en la lesión del bien jurídico protegido, entendió que existían argumentos para responder negativamente:

a) Si el ámbito de la intimidad protegida se restringe mucho, se produce el efecto de asimilar el perjuicio a la parte más básica de la intimidad ("núcleo duro de la privacidad"): salud, ideología, vida sexual, creencias, etc. que ya se castiga como subtipo agravado en el art. 197.5, lo que conllevaría la inaplicación del art. 197.2.

b) De la sentencia de 18 de febrero de 1999, parece colegirse que ese posible mayor perjuicio proviene y se traduce en el desvelamiento de un dato personal o familiar, exclusivamente.

c) La conducta se consuma, sin necesidad de que un ulterior perjuicio se produzca como textualmente exprese las tantas veces referida sentencia de esta Sala.

d) Derivada de la anterior afirmación hemos de entender que sí el perjuicio se materializa habría que acudir a un concurso medial de infracciones penales.

e) El precepto analizado tutela o protege exclusivamente la intimidad y no contempla con tal previsión penal la lesión de otros bienes jurídicos. En realidad se trata de poner freno a los abusos informáticos contra la intimidad, es decir, contra aquellas manifestaciones de la personalidad individual o familiar cuyo conocimiento queda reservado a su titular.

f) En una interpretación sistemática, si quisiéramos establecer una simetría con las descripciones típicas contenidas en el art. 197.1 y referidas al aspecto subjetivo del tipo, advertiríamos que en esta figura delictiva, la acción típica se dirige "a descubrir los secretos o vulnerar la intimidad de otro", que en cierto modo estaría sustituida por la frase "en perjuicio de otro", contenida en el tipo penal previsto en el art. 197.2, habida cuenta de que ambas infracciones penales, tratan de proteger idénticos bienes jurídicos.

g) Asimismo la STS. 123/2009 de 3 de febrero-citada por el Ministerio Fiscal en su escrito de impugnación al recurso- al analizar el hecho del "acceso" que se ubica en la modalidad básica del art. 197.2, indica que ésta modalidad básica incluye, a su vez, tres figuras diversas: 1ª apoderamiento, utilización o modificación de datos; 2ª el mero acceso, y 3ª la alteración o utilización.

h) Pues bien, por difícil que resulta comprenderlo, las modalidades 1ª y 2ª exigen que el sujeto actué en perjuicio de tercero, la 3ª que se haga en perjuicio de tercero o del titular del dato, y lo que aquí es relevante, en la 2ª no se exige perjuicio alguno.

Baste advertir que el supuesto típico imputado -mero acceso-, es decir la modalidad 2ª, no exige tal perjuicio de tercero. El perjuicio de tercero es presupuesto de las otras modalidades típicas del apartado 2º del art. 197 C.P. constituido por la conducta de "apoderarse, utiliza o modificar" y la de "alterar o utilizar" los datos a los que nos venimos refiriendo. Es decir reservados y de carácter personal o familiar existente en los ficheros o archivos allí indicados.

Pero cuando la conducta típica es la descrita en la primera parte del inciso segundo del mismo apartado 2º del citado art. 197 C.P., es decir, el acceso a los datos por cualquier medio, no exige el perjuicio del tercero.

Pues bien creemos que es necesario realizar una interpretación integradora en el sentido de que como en el inciso primero, se castigan idénticos comportamientos objetivos que el inciso 2º (apodere, utilice, modifique) no tendría sentido de que en el mero acceso no se exija perjuicio alguno y en conductas que precisan ese previo acceso añadiendo otros comportamientos, se exija ese perjuicio, cuando tales conductas ya serian punibles -y con la misma pena- en el inciso segundo.

La solución seria -partiendo de que en el termino "tercero" debe incluirse el afectado, en su intimidad, sujeto pasivo, al que esencialmente se refiere el tipo- entender que los apoderamientos, accesos, utilizaciones o modificaciones de datos de carácter personal, realizadas en perjuicio de tercero se incluirían en el inciso inicial del art. 197.2, y en cambio, en el inciso segundo deberían ser subsumidas las conductas de acceso en perjuicio del titular de los datos.

Y en cuanto a la distinción entre **datos "sensibles**" y los que no lo son, debe hacerse en el sentido de que los primeros son por sí mismos capaces para producir el perjuicio típico, por lo que el acceso a los mismos, su apoderamiento o divulgación, poniéndolos al descubierto comporta ya ese daño a su derecho a mantenerlos secretos u ocultos (intimidad) integrando el "perjuicio" exigido, mientras que en los datos "no sensibles", no es que no tengan virtualidad lesiva suficiente para provocar o producir el perjuicio, sino que debería acreditarse su efectiva concurrencia y en el caso presente, no se ha acreditado -ni se ha articulado prueba en este sentido- de que el acceso por parte del recurrente al nombre del médico cabecera -dato administrativo, y en principio, inocuo- del Dr. Bienvenido haya ocasionado perjuicio a éste como titular de al dato.

## III. FALLO:

Que con **estimación de los motivos sexto y séptimo por infracción de Ley,** debemos **declarar y declaramos haber lugar al recurso de casación,** interpuesto por **Juan Carlos ,** contra sentencia de 11 de febrero de 2009, dictada por la Audiencia Provincial de Palma de Mallorca, Sección Primera, en causa seguida por delito continuado de acceso a datos reservados de carácter personal, y en su virtud CASAMOS y ANULAMOS referida resolución dictando nueva sentencia.

SEGUNDA SENTENCIA

I. ANTECEDENTES

Se aceptan los de la sentencia recurrida incluidos los hechos probados.

II. FUNDAMENTOS DE DERECHO

PRIMERO: Tal como se ha razonado en los Fundamentos Juridicos sexto, noveno, decimo y undecimo de la sentencia precedente, los hechos probados no constituyen el delito del art. 197.2 C.P.

III. FALLO

**Que debemos absolver y absolvemos** al acusado Juan Carlos del delito continuado de acceso a datos reservados de carácter personal por el que viene siendo condenado.