Ludopatía: adicción a los videojuegos como circunstancia atenuante en delito de hacking

21-02-2006

Procedimiento Abreviado 332/05
SENTENCIA Núm. 42/06

En BADAJOZ, a quince de febrero de dos mil seis.

El Ilmo. Sr. D. EMILIO FRANCISCO SERRANO MOLERA, Magistrado-Juez del Juzgado de lo Penal Núm. 2 de BADAJOZ y su Partido Judicial, HA VISTO Y OIDO, en Juicio Oral y Público, el Procedimiento Abreviado núm. 332 /2005, seguido por delito de REVELACION DE SECRETOS, contra R.J.B., natural de Badajoz, nacido el día ....., hijo de .... y de ...., con domicilio en.... y con DNI ....

Habiendo sido partes, el Ministerio Fiscal, representado por D/D..... , y dicho/s acusado/s, representado/s por el/los Procurador/es D/Dña. .....y defendido/s por el/los Letrado/s D/Dña. ..... y como Acusación Particular la Entidad "WANADOO ESPAÑA S.L.", representada por la Procuradora ..... y defendida por el Letrado .....

ANTECEDENTES DE HECHO

PRIMERO.- Las presentes diligencias se iniciaron en el Juzgado de Instrucción nº 2 de Badajoz, en virtud de denuncia, siguiéndose por sus peculiares trámites hasta la celebración del oportuno Juicio Oral en este Juzgado de lo Penal. —

SEGUNDO.— El Ministerio Fiscal, en sus conclusiones definitivas, calificó los hechos como constitutivos de dos delitos de descubrimiento y revelación de secretos, previstos en los arts. 197. 1 y 197.2 del C. Penal, considerando responsable/s en concepto de autor/es al/los imputado/s R.J.B., interesando se le/s impusiera por cada delito, la pena 1 año de prisión y 20 meses de multa a razón de 10 euros de cuota diaria, con responsabilidad personal subsidiaria en caso de impago, con inhabilitación especial para la profesión de programador, según el art. 56 del C. Penal, comiso del material intervenido (art. 127 del C.Penal) costas y como responsabilidad civil, indemnice el acusado a la empresa Wanadoo en 104.876,80 euros por los perjuicios ocasionados como consecuencia de los costes originados por la reparación del sistema en relación con la conducta del acusado y en aquellos daños y perjuicios morales y que por lucro cesante sean convenientemente acreditados en el Juicio Oral y en ejecución de sentencia por los hechos de esta causa, cantidades que devengarán los intereses legales de art. 576 de la L.E.Civil.—

La Acusación Particular añade que el acusado ha comunicado a terceros los datos y hechos descubiertos por la intrusión. En cuanto al resto se adhiere al Ministerio Fiscal,

salvo que acusa por tres delitos, arts. 197.1.2 y 3 del C. Penal y solicita pena de 2 años y 6 meses de prisión por los delitos del art. 197.1. 2; y 3 años y 6 meses por el delito del. apartado 3º.—

TERCERO.— Por la/s defensa/s del/los acusado/s se interesó elevar a definitivas sus conclusiones provisionales formuladas en su día y alternativamente art. 21,6ª del C. Penal atenuante analógica en relación a las eximentes y la pena, en su caso conforme arts 87 y 88 del C. Penal, trabajos en beneficios de la Comunidad.—

HECHOS PROBADOS

UNICO.— Probado y así se declara que durante la segunda quincena de agosto y hasta el 20 de noviembre del año 2.003, R.J.B., mayor de edad, con antecedentes penales cancelables, de profesión Administrador de sistemas y Programador Informático, procedió desde su ordenador personal en su domicilio en la calle …….. de Badajoz, y valiéndose de su habilidades informáticas a acceder a la red interna de administración del juego informático de pago vía Internet denominado “Dark Age of Camelot” utilizando para ello ilegítimamente y sin consentimiento de sus titulares legales una cuenta interna con permisos de administrador para los empleados de la empresa Wanadoo, obteniendo así, los Códigos Binarios y la disposición absoluta sobre el acceso del citado juego con posibilidades de utilización y modificación de cuentas, vulnerando inconsentidamente las reglas y normas de seguridad en el funcionamiento y explotación del mencionado juego. Ordenado legalmente el correspondiente registro Judicial en el domicilio del inculpado, se le ha incautado diverso material informático con 2 CDS que contienen códigos, permisos de administración del juego, diversas cuentas y datos de clientes, así como correos personales de los empleados de Wanadoo. Los perjuicios ocasionados a la empresa Wanadoo por los costes externos de reparación del sistema ascienden a 24.876,80 euros.

No ha quedado acreditado el ocasionamiento de otros daños y perjuicios de orden material por costes internos o moral y por lucro cesante.—

FUNDAMENTOS JURIDICOS

PRIMERO.- Se imputa al acusado la comisión de tres delitos de descubrimiento y revelación de secretos, respectivamente previstos en los apartados 1.2. y 3. del art- 197 del C. Penal.

Dispone el art. 184 de la Constitución Española 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 este modo la Constitución incorpora una garantía constitucional, como forma de respuesta a una nueva amenaza concreta a la dignidad y a los derechos de la persona. Ello quiere decir que nos hallamos ante un instituto básicamente de garantía del derecho al honor y a la intimidad, pero también de un instituto que es, en sí mismo, un derecho a libertad fundamental, cual es el “derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes del uso ilegítimo del tratamiento mecanizado de datos informáticos”. La garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. Así pues, la llamada libertad informática es,

también, el derecho a controlar el uso de los mismos datos insertos en un programa informático (vid en este sentido las SSTC 101/91, 254/93 o 143/94).

El articulo 197 del Código Penal, contempla el tipo básico del delito de descubrimiento y revelación de secretos, que tutela el derecho fundamental a la intimidad personal —es el bien jurídico protegido—, garantizado por el artículo 18.1 de la Constitución Española -derecho a la intimidad personal y familiar y a la propia imagen—, superando la idea tradicional del concepto de libertad negativa, materializado en el concepto de secreto que imperaba en el Código Penal derogado, artículo 497.

Los elementos objetivos del artículo 197.1, se integra en primer término por la conducta típica, en la que se pueden distinguir dos modalidades:

a) Apoderamiento de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, y

b) La interceptación de telecomunicaciones o la utilización de artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido o de la imagen, o cualquier otra señal de comunicación. Esta última cláusula general, trata de subsanar las posibles lagunas de punibilidad que se pueden derivar de los avances de la tecnología moderna.

Sujeto activo del tipo básico podrá ser cualquiera, “el que”, dice el texto legal; y sujeto pasivo, ha de ser el titular del bien jurídico protegido y se corresponderá con el de objeto material del delito, pues el concepto que se examina utiliza el posesivo “sus” referido papeles, y también al otro supuesto, intercepta “sus telecomunicaciones”.

Respecto al “iter criminis” es una figura delictiva que se integra en la categoría de los delitos de intención, y en la modalidad de delito mutilado de dos actos, uno de apoderamiento, interceptación o utilización de artificios técnicos, unido a un elemento subjetivo adicional al dolo, consistente en el ánimo de realizar un acto posterior, descubrir el secreto, o vulnerar la intimidad de otro, sin necesidad de que éste llegue a producirse. Por ello, la conducta típica del artículo 197.1, se consuma con el apoderamiento, interceptación etc., sin necesidad que se produzca el efectivo descubrimiento de los secretos, o vulneración de la intimidadad, siendo posibles las formas imperfectas de ejecución, tentativa acabada o inacabada.

El elemento subjetivo del delito, constituido por la conducta típica que ha de ser dolosa, pues no se recoge expresamente la incriminación imprudente, exigida conforme al artículo 12 del texto legal, que ha de llevarse a cabo con la finalidad de descubrir secretos o vulnerar la intimidad, ya que la dicción literal del precepto emplea la preposición “para”.

Por demás como establece la STS 23—10—2000, para la comisión del delito del art. 197 C.P. es necesario no sólo el dolo genérico de saber lo que se hace y la voluntad de hacerlo, sino también el dolo especifico requerido por esta figura delictiva, caracterizado por el ánimo tendencial de invadir la esfera de privacidad e intimidad, significando que, si bien el tipo penal aplicado se ubica en el capítulo 1 del Título X del Libro Segundo del Código Penal, bajo la rúbrica de “Del descubrimiento y revelación de secretos”, lo cierto es que el art. 197.1, tutela dos distintos bienes que son objeto de la

protección jurídico penal: la salvaguarda de los secretos propiamente dichos y; aparte, la intimidad de las personas, viniendo a representar este tipo penal una especie de desarrollo sancionador a las conductas que vulneren el derecho fundamental a la inviolabilidad de las comunicaciones consagrado en el art. 18 C.E.: como parte integrante del derecho a la intimidad personal del individuo.

En lo que se refiere al segundo tipo penal objeto de acusación el articulo 197.2 de C. Penal sanciona al que sin estar autorizado se apodere, utilice o modifique en perjuicio de tercero, 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. No calma por tanto la exigencia del tipo el apoderamiento, entendido en sentido amplio, de datos, ha de tratarse de datos reservados de carácter personal o familiar, extendiéndose la sanción penal en el último inciso de párrafo al que, sin estar autorizado, accediere por cualquier medio a tales datos y a quienes los altere o utilizare en perjuicio de su titular o de un tercero.

La sentencia del TS 2ª de 18 de febrero de 1999, expone que no todos los datos reservados de carácter personal pueden ser objeto del delito contra la libertad informática tipificado en el artículo 197.2 del C.Penal. 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, pues solo con eso se ha quebrantado la reserva que los cubre, 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 al titular de los datos o a un tercero. No es fácil, a priori y en abstracto, cuando el desvelamiento de un dato personal o familiar produce ese perjuicio. Baste decir que lo produce siempre que se trata de un dato que un 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 trasciendan fuera de la esfera en que se desenvuelve la privacidad de las personas y de su núcleo familiar.

Por su parte, el último tipo penal o subtipo agravado previsto en al apartado 3 del artículo 197 del C.Penal sanciona la difusión, revelación o cesión (hemos de entender onerosa o gratuita) a terceros de los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. -

SEGUNDO.— Debe en primer término destacarse que los tipos penales anteriormente expuestos describen un abanico o elenco de conductas que implican abusos informáticos (o de otra índole) sobre datos personales informatizados (extensible a los demás datos obrantes en otro tipo de órdenes públicos o prívados, como por ejemplo ficheros manuales no automatizados), tal y como se infiere de las conductas descritas en el apartado 2, que cabe completar con la difusión, cesión, etc..., de los datos descubiertos (apartado 3) ; y con la interceptación de las comunicaciones telemáticas o de cualquier otro signo) para descubrir los secretos o vulnerar la intimidad o otro, apoderándose de mensajes de correo electrónico etc...

Viene ello a colación porque uno de los principales problemas que se plantean en la presente causa es el relativo al incardinamiento de la conducta o conductas desarrolladas por el acusado en alguno o algunos de los supuestos de hecho de las normas penales a que se ha hecho anterior referencia.

No sería aventurado adelantar (como con posterioridad se concretará a la luz del resultado que arrojan las pruebas practicadas) que desde el punto de vista sociológico y en terminología anglosajona utilizada en el ámbito informático; las conductas que han sido descritas en e "factum" son las propias de un "Hacker" o persona que utiliza determinadas técnicas para acceder sin la debida autorización a sistemas informáticos ajenos, o dicho en castellano, nos encontraríamos ante un intruso, figura diferente a la del "cracker" o pirata virtual que de manera intencionada se dedica a eliminar o borrar ficheros, a romper los sistemas informáticos y a introducir Virus.

La conducta del hacker está guiada por un deseo de vencer el reto intelectual de saltar las barreras del sistema. Tratan de vencer a las claves informáticas de los accesos, de descubrir en suma las lagunas de la protección. Por ello no es de extrañar que muchas compañías los contraten para que, antes de instalar sus sistemas informáticos, analicen si estos presentan grietas por las que se puede alguien colar en ellas.

Como señala González Rus, su éxito presupone que se hayan burlado los medios de seguridad (contraseñas, claves de acceso, passwords), que están ahí colocados para impedirlo y que ponen de manifiesto la voluntad del titular de que la información que se contiene en los mismos no sea conocida más que por quienes están autorizados a ello.

Vaya por delante la afirmación de que en nuestro C.Penal no existe tipificado corno delito de manera expresa y autónoma la conducta del "hacker". Ello no obstante tal conclusion no implica que no puedan encontrar acomodo los concretos actos desarrollados por el intruso dentro de algunas de las conductas encuadradas en el art. 197 del mentado Código.

Si el "hacker" más allá de navegar por los circuitos de la red, llega a averiguar las claves de acceso al sitio, las quebranta y entra al lugar en que se alojan los circuitos protegidos por la clave averiguada descubre "los secretos" de otro.

Las conductas desarrolladas por el intruso al lograr el quebrantamiento de las claves de acceso a los passwords ponen de manifiesto no sólo el dolo genérico de saber lo que se hace y la voluntad de hacerlo sino también el dolo y ánimo especifico requerido por esta figura delictiva, caracterizado por el ánimo tendencial de invadir la esfera de la privacidad que representa precisamente la existencia y colocación de una contraseña de acceso impeditiva del paso al contenido que hay detras de la misma.

Bastará por ende para la consumación del delito la interceptación, entendiendo por tal el descubrimiento del password, independientemente del descubrimiento efectivo de la intrusión o secretos ajenos que se esconden detrás de la clave de acceso (que pertenecen a la fase del agotamiento delictual)

TERCERO.— Si examinamos al amparo de las anteriores consideraciones las conductas descritas en el "factum" propias del "hackering" (figura que no tiene relevancia penal autónoma) resulta meridiano que al acceder el acusado a la red interna de administración del juego informático de pago vía Internet denominado "Dark Age of Camelot", utilizando para ello ilegítimamente y sin consentimiento de sus titulares legales

una cuenta interna con permisos de administrador para los empleados de la empresa Wanadoo, obteniendo así los Códigos Binarios y la disposición absoluta sobre el acceso al citado juego; se accedió a información secreta preservada a los titulares o administradores del juego informático en cuestión, habida cuenta de que los Códigos Binarios, tenían como finalidad lo de impedir el acceso a terceros, de suerte que al acceder a tales Códigos obtuvo la disposición absoluta sobre el juego, con posibilidad de utilización y modificación de cuentas, vulnerando inconsentidamente las reglas y normas de seguridad en el funcionamiento y explotación del mencionado juego, conducta ésta incardinable en el tipo penal previsto en el artículo 197 apartado 1 del C.Penal y ello porque concurren tanto los elementos objetivos (apoderamiento de una clave o código binario que tiene por finalidad impedir el acceso al sistema; con acceso inconsentido al mismo y alteración de su contenido) , con afectación del "know how" de la empresa y subjetivos (intención de acceder a los secretos de otros) del delito en cuestión.—

CUARTO.— Por contra, no es posible extender la respuesta punitiva a los otros delitos por los que viene siendo acusado R.J.B. En lo que se refiere al tipo penal previsto en el apartado 2 del art. 197, cabe señalar que dicho precepto sanciona conductas que implican abusos informáticos contra la denominada "privacy" o libertad informática o dicho siguiendo el tenor literal de la Norma; conductas que tienen por objeto "datos reservados de carácter personal o familiar de otros".

En el supuesto sometido a enjuiciamiento, si bien es cierto que el acusado ha tenido acceso a los correos personales de los empleados de Wanadoo y a los archivos de los usuarios del juego; también lo es que no ha quedado acreditado que la acción se desarrollara "en perjuicio de tercero"; ni por ende, que la intención del acusado fuera la de atentar contra la intimidad de los empleados de Wanadoo, o de los usuarios del videojuego.

Por contra, más bien parece que la intención perseguida por el. agente o intruso no ha sido otra que la de acceder sin más a las entrañas del sistema, franqueando cuantas barreras le fueron instaladas, conducta esta típica del "hacker".

Es igualmente descartable la comisión del delito previsto en el art. 197 apartado 3 del C.Penal.

Aunque se alza la sospecha de que el acusado haya podido difundir, revelar o ceder a terceros los datos descubiertos (códigos binarios o disponer directamente del juego instalándolo en otro servidor y dar acceso a un número ilimitado de usuarios); no ha quedado acreditado que se hayan desarrollado tales conductas, ni en definitiva el traspaso a terceros de la información, ilícitamente obtenida, con intercambio de "logins", contraseñas o códigos binarios.

QUINTO.— Los hechos anteriores resultan de la ponderada valoración de las pruebas practicadas en la vista oral, a los efectos previstos en el art. 741 de L.E.Criminal.

Como primera premisa debe señalarse que no cabe analizar el presente supuesto desde el habitual prisma de la prueba directa de los hechos; prueba de imposible obtención o diabólica exigencia, puesto que la actividad de intrusión informática se desarrolla en la más absoluta clandestinidad, buscando la impunidad de los hechos y

utilizando equipos de alquiler en ciber—cafés o entornos similares, ajenos a la dirección del autor del delito.

A mayor abundamiento, si bien es posible rastrear la actividad delictiva cometida, nadie se identifica por sus datos de filiación, al hacer uso de los servicios informáticos; registrándose normalmente en las cuentas con nombres supuestos; practica esta que dificulta aún más tarea de averiguación de la verdad material acaecida.

Salvando los anteriores escollos es posible, no obstante acudir a determinadas pruebas directas, amén de las indiciarias, y a establecer las consecuentes presunciones, en enlace directo y racional con los correspondientes hechos base.

En tal sentido cabe destacar: 1/ que el acusado R. J, según el mismo ha reconocido, es un experto informático (de profesión administrador de sistemas y programador informático), gozando de los conocimientos precisos para realizar los actos ilícitos que se le imputan, 2/ dicho acusado posee igualmente las herramientas adecuadas y los procedimientos necesarios para conseguir el ilegal propósito (es titular de un complejo equipo informático y tiene acceso a Internet a través de ADSL con IP dinámica, 3/ en el registro practicado en la vivienda en que habita el acusado (diligencia obrante al folio 33 de la causa) , se encuentran CDS con los códigos binarios (clave que permite el acceso al “alma” del juego) y en el disco duro del ordenador (USB, Hi Computer, sin nº de serie por ser clónico); se hallaron convenientemente analizado ficheros y archivos informáticos propiedad de Wanadoo. Así resulta de la testifical, practicada en la vista oral, de los agentes del Cuerpo Nacional de Policía que intervinieron en la diligencia de entrada y registro con nº 82.673 y 78.568 y ratificaron lo actuado en la misma, 4/ el propio acusado reconoce que el ordenador intervenido es de su propiedad. En definitiva el acusado tiene las herramientas (instrumentos) del delito y se le ocupa el fruto (objeto) del mismo, 5/ sometido a análisis el ordenador de R. J. por parte de funcionarios adscritos al Grupo de Seguridad Lógica de la Brigada de Investigación Tecnológica dependiente de la Comisaría General de Policía Judicial, los mismos emitieron el informe obrante a los folios 133 a 137 de la causa; en el que se concluye que: “en primer lugar se encuentran en el disco duro, tres correos electrónicos con archivos adjuntos (posiblemente donde se encuentran los códigos y permisos de administración del juego DAOC) , así como una tabla con datos de cuentas de clientes del juego, dichos correos fueron enviados por el intruso (en este caso el ordenador de R. J.) , desde el propio servidor de Wanadoo hacia sus propias cuentas de correo.

En segundo lugar se encuentran varios correos electrónicos de personal de la sección GOA de Wanadoo que no tendrían que estar en el ordenador de R. J., ya que estos correos son comunicaciones internas de trabajo entre dicho personal que administra la plataforma de los juegos.

Igualmente en el ordenador de R J, se encuentra una tabla de datos “mailboxes.sql” la cual contiene información sobre la configuración de los correos electrónicos del personal de la sección GOA.

En tercer lugar se encuentran conversaciones de R. J. mantenidas con otros usuarios a través de Chat en las que claramente dice que es conocedor de cómo atacar las máquinas que contienen el juego “Dark Age Of Camelot” para hacerse con el control,

describiendo a sus interlocutores como hacerlo, intercambiando login's y password's de accesos a distintos servidores que alojaban el juego.

Por todo lo anteriormente expuesto se puede afirmar que R. J. B., tuvo acceso a los servidores donde se alojaba el juego "Dark Age Of Camelot" y de la sección GOA de Wanadoo, consiguiendo información interna de la empresa que le permitió el control juego y la obtención de datos personales de empleados y clientes"; 6/ en "proces—verbal de constat", seguido a solicitud de Wanadoo France, en las dependencias de dicha entidad sitas en la localidad de Issy Les Moulineaux y ante los fedatarios públicos franceses, que aparecen identificados en el documento obrante a los folios 116 y SS. de la causa (traducido al castellano en documental incorporada a los folios 122 y ss de las actuaciones); se entabló un "chat", con un usuario denominado "vadrek", estando asociado ese seudónimo en IRC a la dirección de correo …….r@... …..—-……—…… …….— El interlocutor (Sr. C. S.) utilizó el nombre de usuario "Zargar" y entabló conversación con "vadrek" que quedó guardada en su archivo del tipo " log" (diario de conexiones cuya impresión original y traducida al castellano aparece incorporada respectivamente a los folios 119-12l y 125—127) . Cabe destacar que a las 17:22 "vadrek", facilita los datos de R. J. B. y su domicilio; C/……., de Badajoz España; así como la dirección de correo ……@.....com. En dicha conversación "vadrek" (o R. J.) reconoce estar en posesión de los códigos binarios del juego "Dark Age Of Cainelot"; 7/ los testigos J. E. y C. V. manifestaron en la vista oral que solo pueden ser "game masters" o administradores del juego y conocedores de los códigos binarios los empleados de Wanadoo y que detectaron la presencia de un intruso que se hizo con los código binarios monitorizando hasta la administración del programa. Manifestaron que el intruso amenazó con comunicar a otros los fallos de seguridad del sistema si no le volvían a abrir su cuenta. Indicaron que en los "logs" (archivos en los que queda registrado el histórico de una actividad informática) quedó constancia de la intrusión.

Por demás descartaron que un navegador cualquiera pudiera acceder a los códigos; 8/ el perito ingeniero en Informática J.B.S. ratificó el informe emitido que consta en pieza separada y manifestó haber llegado a la conclusión de que un intruso accedió al sistema de juego. Por demás el disco duro del ordenador de R. J. que analizó tenía datos y "passwords" o contraseñas de Wanadoo y material reservado de dicha empresa; siendo los códigos binarios la clave de todo juego de ordenador. Además el 80% del material que se sustrajo a Wanadoo lo encontró en el disco duro analizado.

Del conjunto del material probatorio expuesto y aún cuando nadie ha comprobado "de visu" el fisgoneo informático es posible concluir en proceso lógico y racional que el acto de intrusión lo cometió el acusado R. J. B. o "mutatis mutandi", la respuesta a la pregunta relativa a la posibilidad de que otras personas hubieran sido los autores del descubrimiento de los códigos binarios; siendo estos facilitados al imputado; necesariamente ha de ser negativa, toda vez que la defensa no aportó en ningún momento la supuesta dirección de correo electrónico residenciada en Alemania de la que hipotéticamente se habían descargado los códigos binarios, lo que debe operar a modo de contraindicio, de suerte que no cabe sino concluir que el acusado es autor del delito tipificado en el art. 197.1 del C. Penal—

SEXTO.— Concurre en el acusado, como simple, la circunstancia atenuante analógica de ludopatía, de conformidad a lo que establece el artículo 21. apartado 6 del

C. Penal, en relación con lo establecido en el apartado 1 del mismo precepto y en los apartados 1 y 3 del art. 20 del mentado C. Penal.

Respecto a la situación de ludopatía ha declarado el Tribunal Supremo (S. de 19 de noviembre de 2002, que cita las de 15 de noviembre de 1999, 27 de julio de 1998, 11 de marzo de 2002) "que la característica nosológica de la manifestación neurótica de los ludópata o jugadores patológicos radica, como declaró la Sentencia de 18 de mayo de 1993 en su compulsión al juego, en el que participan de forma ansiosa, sin poder cortar con el hábito que ha creado en ellos una dependencia psicológica.

Por eso y sin entrar en si constituye o no una enfermedad (lo que niega la Sentencia de 3 de enero de 1990) o es una forma de neurosis, lo trascendente en estos casos es determinar la forma en que esa tendencia patológica a jugar se manifiesta en cada caso concreto y las repercusiones que tiene en la capacidad de raciocinio o volición del agente. Dado que la compulsión del ludópata actúa en el momento en que la oportunidad del juego se presenta y domina la voluntad en torno al acto concreto de jugar, su relevancia afectará a la valoración de las acciones temporal e inmediatamente dirigidas a satisfacer tal compulsión en el ámbito lúdico, mientras que en otros actos más lejanos obrará solo como impulso organizado para lograr el futuro placer del juego, impulso que es en esos momentos racional y dominable; y será por completo intrascendente respecto a acciones no determinadas por el impulso patológico de la ludopatía y ejecutadas por motivos o fines distintos del juego ansiado".

Partiendo de ello, es claro el informe emitido por el Médico Forense D.F.T. de la P. a los folios 370 y ss de la causa, ratificado y aclarado en la vista oral en el sentido de que R. J. B. cumple los criterios establecidos en. DSM IV para el diagnostico de adicción a video—juegos; produciendo dicha adicción una merma importante de su capacidad volitiva. El facultativo forense aclaró que el imputado cumple 8 criterios de los tenidos en cuenta para apreciar tal patología, siendo suficiente con que concurran cuatro para establecer un diagnostico.

Aun cuando el informe ha sido elaborado en fechas recientes y los hechos ocurrieron a finales del año 2.003 de la propia dinámica de estos últimos y de lo manifestado por el acusado (quien reconoce dedicar unas 12 horas diarias a su adicción) debe deducirse que la adicción a los video—juegos ha sido sostenida y persistente en el tiempo, de larga duración, extensiva a la fecha en que la ilícita actividad tuvo lugar.

No obstante, como la manera de actuar del acusado, fue sumamente compleja, cometiendo un delito muy bien planeado, con un modo de operar premeditado y reflexivo, solo es posible apreciar la circunstancia analógica como simple, puesto que la influencia que sufría le disminuía siquiera sea levemente su libertad y capacidad volitiva.—

SEPTIMO.— Procede imponer al acusado, teniendo en cuenta la regla 1 del art. 66 y lo establecido en el art. 197.1 del C. Penal, la pena de 1 año de prisión y multa de 12 meses, a razón de 6 euros de cuota, con responsabilidad personal subsidiaria de un día de arresto por cada dos cuotas impagadas.

Se fija el importe de la cuota en atención a los ingresos mensuales que el propio acusado ha reconocido percibir, en la vista oral en cuantía de 1500 euros.

De conformidad a lo dispuesto en el art. 56 del C. Penal se impone al acusado las penas accesorias de inhabilitación especial para el Derecho de sufragio pasivo durante el tiempo de la condena a la pena privativa de libertad y la de inhabilitación especial para el ejercicio de la profesión de administrador de sistemas y programador informático por tiempo de 1 año, con comiso de los efectos e instrumentos del delito intervenidos.

OCTAVO.- Todo aquél criminalmente responsable de un delito o falta, lo es también civilmente y de las costas, de conformidad con lo establecido en los arts. 116, 123 y 124 del Código Penal.

En concepto de responsabilidad civil el acusado indemnizará a France Telecome (actual titular de Wanadoo) en la cantidad de 24876,80 euros, importe de los costes externos de reparación del sistema dañado a consecuencia de la actividad delictiva desarrollada por el acusado.

No es posible extender el pronunciamiento indicatorio al resto de los capítulos interesados por el Ministerio Fiscal.

Téngase en cuenta que la propia Acusación Particular obvió la petición de Responsabilidad Civil en su escrito de calificación provisional.

El Ministerio Fiscal interesó indemnización por varios conceptos.

El referido a los costes externos de reparación del sistema aparece suficientemente acreditado según factura emitida por SETIB que obra en fotocopia al folio 218 de la causa; estimada como correcta o ajustada a las actuaciones que se desarrollaron, según concluye el perito Sr. B. S., al folio 57 de su informe.

Por el contrario no se ha acreditado la realidad de los daños y perjuicios consistentes en costes internos de reparación del sistema y daños morales y lucro cesante por perdida de imagen y usuarios. Ni Wanadoo ha acompañado al escrito que figura a los folios 210 y Ss. documentación alguna de la que quepa inferir que han existido costes internos a fin de detectar e identificar la intrusión y reparar los fallos del sistema; ni prueba alguna que justifique el cuantificación que verifica de esos hipotéticos " costes internos", ni menos aún de un supuesto lucro cesante o daños morales, que, a la fecha presente, transcurridos más de dos años desde que tuviera lugar los hechos no se han materializado, de suerte que el daño o perjuicio que se alega no es real y efectivo y si meramente hipotético, como se infiere por demás del análisis que hace a los folios 56 y 63 de su informe el perito Sr. B.—

Vistos los artículos citados y demás de general y pertinente aplicación,

FALLO

Que debo condenar y condeno a R. J. B., en quien concurre como simple la circunstancia atenuante analógica de ludopatía, como autor/es responsable/s de un delito de descubrimiento y revelación de secretos por intrusión informática, ya definido, a las penas de 1 año de prisión, con inhabilitación especial para el Derecho de sufragio pasivo

y para el ejercicio de la profesión de administrador de sistemas y programador informático durante el tiempo de la condena.

Le condeno igualmente al pago de una multa de 12 meses, a razón de 6 euros de cuota, con responsabilidad personal subsidiaria de un día de arresto por cada dos cuotas impagadas y comiso de los efectos e instrumentos del delito.

En concepto de responsabilidad civil indemnice el acusado a Wanadoo (France Telecorne) en la cantidad de 24.876,80 euros, más el interés previsto en el art. 576 de la L. E. Civil.

Absuelvo al acusado de la imputación del resto de los delitos de descubrimiento de datos de carácter personal o familiar y de difusión de tales datos de que venia siendo objeto a lo largo de la causa.

Las costas procesales se imponen al acusado.

Notifíquese la presente sentencia a las distintas partes personadas en el procedimiento, instruyéndoles que contra la misma cabe recurso de apelación, en el plazo de DIEZ DIAS, ante la Audiencia Provincial de esta ciudad y a contar desde la fecha de la última notificación.-

Así por esta mi sentencia, lo pronuncio, mando y firmo.-

PUBLICACION.- Leída y publicada que ha sido la anterior sentencia por el Iltmo. Sr. Magistrado—Juez que la ha dictado, constituido en audiencia pública en el día de su fecha, de lo que yo, el Secretario, doy fe.-