Ricardo M. Mata y Martín

DELINCUENCIA INFORMÁTICA Y DERECHO PENAL

Presentación
Sergio J. Cuarezma Terán

Delincuencia Informática y Derecho Penal

Ricardo M. Mata y Martín
Profesor Titular de Derecho Penal
Universidad de Valladolid (España)

Presentación
Sergio J. Cuarezma Terán

EDITORIAL
HISPAMER

INSTITUTO CENTROAMERICANO
DE ESTUDIOS PENALES
UNIVERSIDAD POLITÉCNICA
DE NICARAGUA

N
345
M 425 Mata y Martín, Ricardo M.
Delincuencia Informática y Derecho Penal / Ricardo M. Mata y Martín – 1a ed. – Managua : HISPAMER, 2003.
196 p.

ISBN: 99924-57-27-9

1. DERECHO PENAL 2. INFORMÁTICA-ASPECTOS JURÍDICOS 3. PROPIEDAD INTELECTUAL 4. DERECHO DE AUTOR

Equipo editorial

Autor : Ricardo Mata y Martín

Coordinación editorial : MSc. Conny Villafranca Flores

Diseño interior y de portada : Sergio Flores Balmaceda

Costado este de la UCA, Apartado A-221, Zona 13
Managua, Nicaragua

Depósito Legal: 0192 – octubre 2003

Impreso en Nicaragua,
por Impresión Comercial La Prensa, S.A.

A Teresa, por todo.

Indice general

PARTE TERCERA

Presentación

Para el Instituto Centroamericano de Estudios Penales de la Universidad Politécnica de Nicaragua (ICEP de la UPOLI) y, en particular, para mí constituye una distinción presentar el libro *Delincuencia Informática y Derecho Penal* del Prof. Dr. Ricardo Mata y Martín, penalista español y gran amigo.

De todos los temas estudiados por el Derecho penal moderno, la delincuencia informática es, sin discusión un tema de fundamental importancia. La obra del Prof. Dr. Ricardo Mata y Martín, estudia este tema a la luz del derecho penal y llega en el momento justo, cuando la sociedad está acechada por un entorno denominado "sistemas o redes informáticas".

El Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente que se llevó a cabo en Viena del 10 al 17 de abril de 2000, expresa que la globalización ha generado un medio ambiente propicio para formas de delincuencia nuevas y más extensas. El cambio de la estructura del comercio, las finanzas, las comunicaciones, el desarrollo de las tecnologías y la información han ayudado a fomentar un espacio en el que la delincuencia no está confinada dentro de las fronteras nacionales. Este hecho se complica con el surgimiento de las redes internacionales informáticas como Internet, que permite a los usuarios desarrollar transacciones con otras personas usuarias de la denominada Aldea global. En este tipo de comunicación existen personas que exploran los nuevos medios de las computadoras y las redes con fines delictivos. Robo de información, falsas ofertas, sabotaje informático, espionaje informático, interceptación no autorizada, piratería, estafas de subastas *online*, intrusiones en redes y un sinnúmero de

denominados "delitos cibernético", o "ciberdelitos" o "cibercrimen" jaquean permanentemente a personas naturales, instituciones públicas y empresas privadas de todo el mundo.

Este fenómeno, el profesor y querido amigo Ricardo Mata y Martín lo aborda en su obra con seriedad, profundidad y un riguroso manejo y nos ofrece un meditado análisis de las implicaciones jurídico penales de las tecnologías informáticas y de la comunicación. También hace un ponderado llamado, especialmente en aquellas experiencias donde no se ha legislado sobre el tema, para que el legislador a la hora de tipificar estos comportamientos debe de actuar previo investigaciones y estudios sobre el tema con la finalidad de evitar decisiones emotivas y regular la delincuencia informática de forma adecuada con visión de largo plazo.

El profesor Ricardo Mata y Martín es doctor por la Universidad de Valladolid, España y Profesor Titular de Derecho Penal en la Universidad de Valladolid. Ha realizado estancias de Investigación para su preparación en Friburgo de Brisgovia (Alemania) en el Max-Planck-Institut für Auslandisches und Internationales Strafrecht. Es Premio Extraordinario de Licenciatura y está en posesión del Primer Sexenio de investigación reconocido por la Comisión Nacional de Evaluación de la Actividad Investigadora del Ministerio de Educación y Cultura de España. Entre sus publicaciones cuenta con tres monografías (una de ellas dedicada al mundo de las nuevas tecnologías: *Delincuencia informática y Derecho Penal*, Edisofer, Madrid 2001, otra *Bienes Jurídicos y Intermedios y delitos de peligro*, Granada 1997 y la primera sobre *El delito de robo con fuerza en las cosas*, Valencia 1995) y una veintena de artículos en revistas científicas nacionales e internacionales (entre ellos "Algunas consideraciones sobre informática y Derecho penal. El caso de la estafa informática" y "Algunos aspectos de la delincuencia patrimonial en el comercio electrónico"). Ha dirigido un Proyecto de Investigación sobre "El Derecho penal ante el reto de la criminalidad informática" con la Universidad Carlos III de Madrid y otro sobre la "La protección penal del consumidor en el comercio electrónico" con la Junta de Castilla y León. Ha sido invitado a impartir múltiples cursos como especialista sobre distintos ámbitos del Derecho penal en países como Argentina, Bolivia o Portugal. Participa en un Programa de la AECI sobre "Gobierno Electrónico" a

desarrollar en Chile, Cuba y Uruguay. Igualmente toma parte en un Programa Alfa de la Unión Europea dedicado al "Gobierno Electrónico" con las Universidades de Münster, Belfast, Burgos, Zaragoza y Valladolid.

La obra constituye una referencia para el estudio de la delincuencia informática. Consta de tres partes. La primera parte dedicada a los aspectos generales y elementos comunes de los delitos vinculados a la informática (concepto de delito informático, bien jurídico, problemas criminológicos y políticos-criminales). La segunda parte, aborda distintos tipos penales de delincuencia informática (estafa informática, propiedad intelectual, daños, protección de la intimidad, pornografía y otros delitos contra la libertad e indemnidad sexual). Y la tercera parte, analiza algunos problemas procesales de la delincuencia informática (determinación de la ley aplicable, medios electrónicos y proceso penal).

Sergio J. Cuarezma Terán
Director
Instituto Centroamericano de Estudios Penales
de la Universidad Politécnica de Nicaragua

Managua, 16 de mayo de 2003

Nota a la edición nicaragüense

La creciente dependencia de todos los sectores de la vida social de su conexión a procedimientos automatizados e informatizados hace que los hechos irregulares e ilícitos que puedan ser cometidos a través o sobre este tipo de sistemas alcancen progresivamente una mayor trascendencia. Los servicios públicos (sanidad, regulación del tráfico rodado, aéreo o marítimo), la producción industrial, el comercio, la defensa de un país o la enseñanza, van integrándose inexorablemente en el entramado de las tecnologías de la información y Telecomunicaciones. Junto a las indudables aportaciones y beneficios que proporcionan al ser humano, las Nuevas Tecnologías también engendran nuevos riesgos y ocasiones para la realización de hechos ilícitos. Desde este punto de vista los medios informáticos constituyen un factor criminógeno relevante. De esta manera se han convertido en habituales múltiples formas de fraudes en pagos electrónicos, la difusión prohibida de contenidos a través de la Red, el acceso ilegítimo a informaciones confidenciales contenidas en bases de datos, los ataques a sistemas informáticos que bloquean la prestación de determinados servicios o la difusión mundial de virus que producen efectos en terminales de todo el planeta. Pero a pesar de las enormes cifras exhibidas de perjuicios a causa de este tipo de hechos y la alarma que sin duda generan, hay que reconocer que formas de pago ilícitas, incluso mediante tarjetas de crédito, existían ya antes y también ahora con Internet, que la difusión de material pornográfico se llevaba a cabo de forma precedente, la publicidad fraudulenta o engañosa no es un fenómeno que aparezca con las Nuevas Tecnologías, ni la falsificación documental se nos puede presentar como algo novedoso. En la práctica sabemos que no existe ningún campo del actuar humano en el que la seguridad esté garantizada plenamente.

Lo cierto es que la historia nos muestra cómo las invenciones e ingenios del ser humano a lo largo del tiempo han producido asombro pero también alarma entre sus contemporáneos. Así hoy nos puede sorprender las cautelas y temores que inspiraron la llegada de la imprenta. Los medios de transporte como el barco de vapor o el ferrocarril, el teléfono, la luz eléctrica o el automóvil. Desde nuestra perspectiva actual el impacto producido y los temores consiguientes pueden parecernos de una gran inocencia. Puede que pasadas unas décadas suceda lo mismo con nuestros miedos y alarmas.

A pesar de ello, sin embargo, es posible que, junto a la mundialización que implican necesariamente, exista una nueva dimensión en estos fenómenos que aporten un cambio cualitativo. Y esta nueva dimensión hace referencia a la posibilidad de que sea el propio ser humano el objeto de ataque de una manera hasta ahora cualitativamente desconocida. Las posibilidades abiertas por los nuevos sistemas de almacenamiento y tratamiento de información personal, de acceso y descubrimiento de un conjunto amplio de datos de toda índole, hacen que estos hechos adquieran una significación añadida. Por su propia naturaleza los sistemas informáticos permiten contener una ingente cantidad de información sobre un número elevadísimo de personas, un tratamiento automatizado y a gran velocidad de esa misma información, así como una gran capacidad de adaptación a las exigencias actuales del hombre. Estas características técnicas de los sistemas de almacenamiento y tratamiento automatizado de datos viene a cubrir una necesidad de las sociedades más avanzadas, cada vez más complejas y que ofrecen una más amplia prestación de servicios de todo género. Se ha destacado como valor más innovador de las nuevas tecnologías el que la información haya pasado a constituir un valor económico de primera magnitud. Los procedimientos informáticos representan desde esta perspectiva la capacidad de acceso a la información, la posibilidad de información sobre la información. Las sociedades modernas requieren, por su propio dinamismo y complejidad, la existencia de sistemas de información de una amplia gama de datos personales (sanitarios, fiscales, financieros, profesionales, de prestación de servicios, etcétera).

Pero con todo ello lo que sucede es que se genera la posibilidad no sólo de acceder y manejar aspectos de la privacidad de las personas, sino que potencia la construcción o, mejor, la reconstrucción

de la personalidad en su conjunto de un hombre o de una mujer. Son los llamados perfiles personales que pueden ser objeto de utilización con fines comerciales, políticos o puramente personales. Esto nos puede convertir en lo que se conoce como "ciudadanos transparentes", situación en la que en realidad lo que quiebran son los presupuestos para un actuar libre en la vida social.

Este nuevo fenómeno vinculado a las Nuevas Tecnologías resulta cualitativamente semejante en una y otra orilla del Atlántico. Por ello he aceptado con sumo placer la amable invitación de mi querido amigo, el Prof. Sergio Cuarezma Terán para realizar una nueva edición en Nicaragua de mi obra Delincuencia Informática y Derecho Penal. El interés mostrado por el profesor Cuarezma Terán por éste y otros temas decisivos de la actualidad jurídico-penal revelan una honda preocupación por la orientación del sistema penal de su país y, en definitiva, por los derroteros de la Nación. Al margen de diferencias en las soluciones concretas del derecho positivo, que naturalmente deben ser conocidas y estudiadas, parte relevante de la perspectiva jurídica, a propósito de la existencia de los medios y sistemas informáticos, resulta del análisis de los cambios que pueden introducir los mismos en el Ordenamiento Jurídico así como su fundamento y el del tratamiento legal establecido. La monografía que sigue a estas notas pretende mostrar la fundamentación jurídico-penal de las necesidades atribuidas a esta nueva realidad en relación a los delitos de mayor trascendencia en este campo. Igualmente se analizan las soluciones adoptadas por el legislador penal español en lo concerniente a los problemas interpretativos más sobresalientes en los tipos penales de la parte especial más implicados en la delincuencia informática. Por lo reciente de la edición europea tampoco se ha considerado la posibilidad de introducir modificaciones en el contenido del libro.

La lucha frente a la criminalidad informática desborda naturalmente el campo propio del Derecho penal, pues se trata de un fenómeno cuyo control reclama además otros instrumentos más amplios y complejos (de tipo jurídico –no penal–, de tipo técnico, formativo, así como educativo). Sin embargo, es preciso abordar con seriedad y estudio profundo las implicaciones penales de las tecnologías informáticas y de la comunicación. El legislador penal antes de tomar decisiones apresuradas en este campo deberá contar con estudios e

informes previos de personas e instituciones especializadas en su análisis. Una política criminal racional es imprescindible en este terreno tan abonado al alarmismo, alejada de la conmoción producida por determinados hechos, por importantes que sin duda resulten, si se quiere obtener una respuesta legal adecuada y de largo alcance. A ello quisiera contribuir, modestamente, la presente obra.

Ricardo M. Mata y Martín
Profesor Titular de Derecho Penal
Universidad de Valladolid (España)

Introducción

Con las palabras que siguen únicamente se pretende un acercamiento a las más sobresalientes conductas, relacionadas con la informática, que desde la óptica penal poseen significación. Algunas de ellas ya se encontraban en la regulación penal con anterioridad al nuevo CP español. Otras se han introducido con el CP de 1995, que sobre todo ha venido a precisar las conductas objeto de atención jurídico-penal, refiriéndose expresamente al nuevo texto legal en distintas ocasiones a los medios informáticos y sus aplicaciones a lo largo de su articulado.

En las dos últimas décadas ha tomado cuerpo la eclosión del fenómeno informático en amplias parcelas de nuestra sociedad. La enorme expansión de que viene gozando el procesamiento automatizado de datos en una sociedad cada vez más receptiva a las posibilidades crecientes que ofrecen los medios informáticos tiene consecuencias indudables para el mundo del Derecho. De auténtica conmoción para el Ordenamiento Jurídico califica GUTIÉRREZ FRANCÉS[1] el impacto de las nuevas tecnologías sobre el mundo jurídico. Singularmente Internet ha supuesto un cambio tan espectacular en las posibilidades de comunicación e intercambio de información en el contexto global del planeta que, desde una perspectiva histórica ha sido comparado con la revolución industrial o con otros hitos históricos de semejante magnitud.

1 *Fraude informático y estafa*, Ministerio de Justicia 1991, p. 42.

Junto a la contribución al progreso social que representan sin duda las nuevas técnicas y procedimientos informáticos, aparecen a la vez prácticas anómalas en este mismo campo, con producción de perjuicios a particulares y al conjunto de la comunidad, que en los casos más graves pueden suponer hechos delictivos.

En el ámbito de los intereses patrimoniales y económicos surgen innumerables modalidades con incidencia en el mismo. Casos de sabotaje informático dirigidos especialmente contra las empresas creadoras de *software*. La piratería de programas supone en ocasiones la lesión de la propiedad intelectual como hecho delictivo. Los numerosos procedimientos informáticos abren la posibilidad de realizar todo tipo de contrataciones comerciales, como operaciones en bolsa o servicios de compras integrados. También éstos representan una gran potencialidad lesiva para intereses personales y colectivos.

En otros campos no patrimoniales, que suponen por tanto la lesión de derechos o bienes jurídicos de contenido no económico, aunque en el caso concreto pueda poseer trascendencia y finalidad lucrativa, aparecen operaciones relativas al tráfico de drogas, difusión de material pornográfico, incitación a la pedofilia, ataques a la intimidad, falsedades, etc. Estos son algunos de los hechos que en relación a los nuevos medios informáticos se presentan como potenciales delitos.

La descripción de la situación anterior representa sin duda un reto para el Derecho y en particular para el Derecho Penal. La aparición de los instrumentos informáticos con una serie de características específicas hace de ellos un factor criminógeno de primer orden. Sin embargo los recursos legislativos en el sector del Derecho penal hasta el reciente Código Penal de 1995 tomaban como referencia fundamentalmente el contexto histórico y tecnológico propio del siglo XIX, en el que se asentaba sustancialmente nuestra legislación penal. La incongruencia entre los textos legales decimonónicos y la radical novedad representada por los hasta entonces prácticamente desconocidos nuevos medios tecnológicos, hacía –quizás– que muchos supuestos delictivos previstos tradicionalmente no resultaran aplicables sin forzar la letra de la ley, en conculcación del principio de legalidad, vertebrador del moderno Derecho penal. Además, dado lo reciente y poco conocido de estas técnicas no

se había dispuesto del margen necesario para la reflexión y estudio de estos nuevos campos y así conseguir la formación de un cuerpo doctrinal sólido sobre la materia.

La toma en consideración por las legislaciones penales de este nuevo fenómeno es, por tanto, reciente. En primer lugar se estableció en EEUU la *Crime Control Act* de 1984, seguida de la *Computer Fraud and Abuso Act* de 1986 que incluía cinco grupos de ilícitos informáticos. En Alemania en el marco de la segunda ley de lucha contra la criminalidad económica de 15 de mayo de 1986, se introduce la regulación relativa a la conocida como *Computer Kriminalität*. La seguridad informática se formalizó en Francia mediante la llamada ley *Godfrain* de 5 de enero de 1988, después incorporada al nuevo Código penal francés. En Italia la ley de 23 de diciembre de 1993 (n. 547) ha supuesto la adaptación del Código penal italiano a la nueva criminalidad informática.

En algunos de los anteriores casos el legislador penal ha llevado a cabo la actualización mediante una norma específica (ley especial). En el caso español la previsión a los sistemas informáticos en el ámbito de los hechos punibles contemplados en el articulado, se ha producido simultáneamente a la reforma general del sistema penal con la aprobación del nuevo Código Penal de 23 de noviembre de 1995. En el mismo, en algunos casos se especifican los supuestos delictivos en los que pueden aparecer los objetos o medios informáticos o se determina la modalidad informática de un delito (casos de la estafa informática, daños informáticos o ataques a la intimidad mediante procesos informáticos).

Con ello se evita la duda de si determinados hechos punibles resultan aplicables en el caso de intervención de sistemas informáticos. Pese a ello surge ahora la necesidad de interpretar los elementos que especifican estos supuestos cometidos sobre o mediante procesos automatizados de datos. Es preciso determinar el alcance y sentido de estos nuevos elementos y supuestos. Por otra parte no todos los posibles delitos relacionados con la informática han sido expresados en el nuevo Código penal. Lo novedoso y pujante de estos medios hacen compleja esta labor.

Otro aspecto de gran interés es el de la prueba. La novedad y diferencias fundamentales con los métodos tradicionales de ejecu-

ción del delito hacen de la investigación y prueba de estos hechos un campo singular. El rastreo de los procesos automatizados de datos resulta especialmente complejo. Igualmente la reproducción de la prueba en el proceso oral, único momento procesal en el que resulta válida la realización de la prueba de cargo suficiente para un veredicto de culpabilidad.

De acuerdo a lo anteriormente indicado, la presente monografía –iniciada como proyecto de investigación en el marco del Instituto de Estudios de Seguridad Pública "Duque de Ahumada"– consta de tres partes: una primera dedicada a los aspectos generales y comunes de los delitos vinculados a la informática (concepto de delito informático, bien jurídico, problemas criminológicos y político-criminales). Una segunda en la que se abordan en particular distintos tipos penales de delincuencia informática (estafa informática, propiedad intelectual, daños, protección de la intimidad, pornografía y otros delitos contra la libertad e indemnidad sexual). Finalmente en la tercera y última parte se analizan algunos problemas procesales del tema (determinación de la ley penal aplicable, medios electrónicos y proceso penal).

PARTE PRIMERA

ASPECTOS COMUNES EN LA DELINCUENCIA INFORMÁTICA

I. PRESUPUESTOS GENERALES DE LOS DELITOS INFORMATICOS

1. Nuevas tecnologías: posibilidades y riesgos

a. Los cambios sociales provocados por las tecnologías de la información resultan decisivos en todos los ámbitos y por supuestos también tienen su repercusión en el campo del Derecho penal.[2] Las inmensas posibilidades que abren las nuevas tecnologías, evitando al ser humano cierto tipo de tareas más mecánicas, suponen como señala SIEBER[3] unos cambios más radicales que los que introdujo la revolución industrial del siglo XIX con la sustitución del trabajo físico de los hombres por el de las máquinas. Los avances de la informática sitúan al Derecho penal ante problemas nuevos, o ante problemas que debe abordar con una nueva visión de los mismos.

Las enormes potencialidades que se abren para el tratamiento automatizado de datos, tienen un reverso que son los riesgos que se introducen para facilitar la realización de hechos que afecten a los intereses fundamentales de las personas. Es decir la informática o, en general, el tratamiento automatizado de datos se presenta como factor criminógeno, pues permite el acceso y el manejo de bases de datos, programas de cualquier género, en ocasiones de forma lesiva para los intereses básicos de las personas y de la socie-

---

2 Sobre los cambios de perspectivas en los planos cultural y jurídico con la irrupción de las nuevas tecnologías, en lo que se denomina la nueva etapa del "simio informatizado", puede verse la exposición de TÉLLEZ AGUILERA, A. *Nuevas Tecnologías. Intimidad y protección de datos*, Edisofern, 2001, pp. 21 y ss.

3 SIEBER, U. *Computerkriminalität und Strafrecht*, München, 1977, p. 23.

dad, siendo más costosa la averiguación del autor y la prueba de los hechos debido a la naturaleza del procedimiento informático.

b. Naturalmente aquí vamos a prestar atención a los aspectos más gravosos para el hombre derivados del uso de la informática. Tan gravosos que forman parte del catálogo de hechos a los que la ley vincula la aplicación de una sanción criminal o, incluso, debido a la novedad de estos comportamientos, se plantea si deben tener cabida entre los mismos cuando el legislador todavía no ha tomado una decisión sobre la trascendencia jurídica de los mismos. Por ello debemos hacer referencia a los presupuestos necesarios para que estas conductas irregulares e ilícitas relacionadas con la informática alcancen la calificación de merecedoras de sanción penal. Es decir, conviene abordar en este momento también el tratamiento y la consideración, desde el punto de vista del derecho penal, de aquellas conductas que emergen de la realidad social vinculadas a la informática y que plantean serias interrogantes sobre su trascendencia penal. Los perfiles de mayor contribución a la vida del ser humano se corresponden con el buen uso de las potencialidades que encierra la informática.[4]

2. La Selección y protección restrictiva de los bienes jurídicos penalmente relevantes

Sin embargo conviene dejar sentado desde el principio que no todos los hechos socialmente reprochables e incluso ilícitos resultan jurídico-penalmente relevantes, pues el Derecho penal única-

4 Puede verse al respecto el ensayo de J. MARÍAS *Cara y Cruz de la Electrónica*, Colección Austral, Espasa-Calpe, 1985, quien pone de relieve cómo el ser humano se ve liberado con estas nuevas técnicas de tareas puramente mecánicas, lo que le permite dedicarse con mayor plenitud a la reflexión y el pensamiento. "Los computadores… eliminan el pensamiento bruto y nos dejan en franquía para pensar, para ejecutar el pensamiento lúcido, inteligente". "La más prodigiosa hazaña de la Electrónica consiste en la eliminación de todo aquello que es mecánico e inercial en el pensamiento… para dejar libre el ejercicio de la razón" (pp. 98-99). En este sentido GARCÍA CAMARERO señala cómo la segunda revolución industrial (la revolución informática) significa un desplazamiento masivo de mano de obra de trabajos tradicionales hacia otra forma de actividad y para la que se requerirá el empleo de las potencialidades más propias del hombre. *La revolución*

mente se legitima cuando la conducta afecte a intereses fundamentales de la persona o la sociedad (principio de lesividad) y, además, las medidas disponibles desde otros sectores y disciplinas del ordenamiento jurídico no resulten adecuadas para su tutela (principio de subsidiariedad o intervención mínima).

Para que se pueda apreciar la presencia de un interés merecedor de protección jurídico-penal no es suficiente que estemos ante un bien jurídico, en el sentido de una entidad reconocida y amparada por el ordenamiento jurídico. Las especiales exigencias propias del Derecho penal hacen que no baste la conculcación de un interés jurídico para que el legislador penal intervenga creando una figura delictiva, sino que la agresión a tal interés deberá verse rodeada de ulteriores requisitos para que pueda alcanzar la tutela mediante los recursos propios del Derecho penal. Estas ulteriores exigencias en las que se muestra la naturaleza y autonomía del Derecho penal, se manifiestan en el principio de subsidiariedad y en el de fragmentariedad de la protección penal.[5]

Estamos en definitiva ante principios relativos al sentido y alcance del Derecho penal como protector de bienes jurídicos. En ambos, aunque de diferente manera, puede verse la especial significación que representan los medios de reacción del Derecho penal frente a los comportamientos punibles, pues inciden de manera decisiva en la persona a la que se aplica. En este sentido MEZGER,[6]

---

informática, Cuadernos Historia 16, Madrid 1997, p. 31. Este autor indica también cómo esta segunda revolución industrial la liberación total del trabajo con la posibilidad de que los sistemas productivos, el control de los transportes, los procesos administrativos y otros servicios puedan funcionar completamente sin la participación directa del hombre, de forma automática. Por otra parte la misma produce un gran impacto en los procesos cognitivos y culturales facilitando el acceso a grandes yacimientos de información (p. 31).

5 Sobre estos principios, KAUFMANN, Arthur. "Subsidiarietätsprinzip und Strafrecht", *Festschrift für HENKEL*, 1974, pp. 89 y ss. MIR PUIG, S., "Sobre el principio de intervención mínima", *Revista de la Facultad de Derecho de la Universidad de Granada*, 12/1987 (publicado en 1989), pp. 243 y ss. MARTOS NÚÑEZ, J.A. "El principio de intervención penal mínima", *ADPCP* 1987, pp. 99 y ss. NIGGLI, M.A., "Ultima ratio?", *ZStrR*, 111 (1993), pp. 236 y ss.

6 *Tratado de Derecho penal I*, trad. J.A. RODRÍGUEZ MUÑOZ, Madrid 1955, p. 140.

en una conocida formulación, señaló que el Derecho penal, a través de la actividad de la Administración de justicia penal, conlleva "los más graves ataques a la libertad, al honor, al patrimonio, incluso a la vida de los ciudadanos".

El principio de subsidiariedad hace referencia al momento de intervención del Derecho penal en la perspectiva de la actuación coordinada de los distintos sectores de la regulación jurídica. Este sólo deberá incriminar una conducta lesiva para un determinado interés jurídico cuando, reconocido previamente el interés como merecedor de protección penal, el resto de los medios de que dispone el ordenamiento jurídico se hayan mostrado ineficaces e incapaces de tutelar adecuadamente el mismo. El principio de subsidiariedad, el carácter de última *ratio* o el principio de intervención mínima vendrían a representar esta posición del Derecho penal respecto a los instrumentos propios de otras disciplinas jurídicas. La mayoría de los intereses penalmente tutelados tienen su ámbito de regulación y protección en otros sectores normativos: propiedad o medio ambiente como intereses jurídicos están presentes en plurales disciplinas jurídicas. Únicamente deberán alcanzar configuración en un tipo penal aquellos comportamientos que escapen a un adecuado control y protección de las regulaciones extrapenales. De manera que como señala ROXIN[7] "el bien jurídico recibe una doble protección: *del* Derecho penal y *antes* del Derecho penal".

Por tanto el principio de intervención mínima o carácter de última *ratio* del Derecho penal supone que los medios sancionatorios del ordenamiento penal, debido a su efecto de intensa restricción o lesión de los derechos de las personas, sólo pueden entrar en juego cuando las medidas disponibles en otros sectores del ordenamiento no resultan suficientes para la protección del bien jurídico.

El principio de fragmentariedad, por su parte, viene a señalar el carácter no completo o absoluto de la protección otorgada a los bienes jurídicos penales. Una vez ingresado un bien en el ámbito

7 "Sentido y límites de la pena estatal", en *Problemas básicos del derecho penal*, trad. D.M. LUZÓN PEÑA, Madrid, 1976, p. 22.

jurídico penal no resulta, sin embargo, protegido frente a cualquier tipo de agresión. Únicamente frente a aquellos supuestos en los que se aprecie la necesidad de la tutela intensificada mediante la pena criminal el hecho será punible. El tipo penal determina las modalidades de agresión que resultan abarcadas por el Derecho penal y, negativa e implícitamente, excluye el resto de modalidades en las que el bien puede ser objeto de transgresión.

El bien jurídico que resulta tutelado no recibe una protección ilimitada e indiscriminada, sino que, únicamente encuentran amparo los ataque más intolerables a los mismos. Debido a este carácter fragmentario del Derecho penal, por el que no toda agresión al bien jurídico protegido encuentra respuesta en el Derecho penal, aquél se limita a intervenir para los supuestos de determinadas modalidades de agresión o cuando se producen ciertas consecuencias especialmente gravosas. En definitiva desde ambos ángulos, el del principio de subsidiariedad y el del principio de fragmentariedad del Derecho penal, se produce una selectiva protección de bienes jurídicos.

3. El llamado delito informático

a. En ocasiones la referencia a los hechos delictivos relacionados con la informática se realiza mediante la expresión o denominación de "delito informático", expresión que posee cierto atractivo por su simplicidad y por responder a la terminología anglosajona *computer crime*. En realidad se trata de un concepto ambiguo que no se corresponde en sentido estricto con ninguna categoría jurídico-penal, con un exclusivo hecho punible de los previstos en el Código penal.

La polimórfica realidad de la criminalidad informática, se refleja y manifiesta en los intentos de definición o conceptuación de la misma, así como en las clasificaciones de los hechos a las que da lugar el estudio de este fenómeno. Así la aproximación a un concepto genérico, omnicomprensivo del hecho informático penalmente relevante da lugar necesariamente a definiciones muy amplias. Por ello el grupo de expertos convocado por la OCDE en el año 1985 para el análisis de este tipo de delincuencia habla de "delitos relacionados con los ordenadores" (*computer-related crime*), en el que se integra "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automatizado de

datos".[8] Igualmente la definición del delito informático como "Toda acción dolosa que provoca un perjuicio a personas o entidades, en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas",[9] deja ver la carga de generalización que la acompaña. Por los mismos motivos el sistema de codificación de delitos informáticos de la Secretaria General de Interpol cuenta con una treintena de tipos delictivos relacionados con estos medios, lo que da nuevamente idea de la heterogeneidad y extensión de los campos a los que afecta.[10]

Si se quiere optar por un cierto criterio restrictivo a la hora de establecer una noción general, habría que incluir exclusivamente los supuestos en los que el ordenador representa el medio de ejecución,[11] pues sólo en éstos se aprecian las peculiaridades y características de los sistemas informáticos o del procesamiento electrónico de datos que convierte estos hechos en algo novedoso, diverso, al menos desde el punto de vista criminológico. Pero incluso en esta aproximación más restrictiva a una compresión global de este género de delincuencia se deja notar la mencionada heterogeneidad y considerable amplitud.

Esta multiformidad y pluralidad se acredita nuevamente a la hora de clasificar y organizar las conductas incluidas en este grupo. SIE-

---

8 Cfr. SIEBER, U. "Documentación para una aproximación al delito informático". *Delincuencia económica.* MIR PUIG, S. (Comp.), PPU, Barcelona 1992, p. 66.

9 Definición que aparece en las conclusiones del Congreso celebrado en Zaragoza en el año 1989 sobre el "delito informático". Véase CONSENTINO, G. y otros. "Tras los pasos de la seguridad perdida. Delitos informáticos", *Informática y Derecho* 23,26 (1998), p. 1199.

10 SCHREIBER, W., "La delincuencia asistida por ordenador", *Interpol* 464 (1997), p. 9. Quien indica al mismo tiempo las dificultades que esta misma amplitud origina a la hora de lograr un intercambio internacional de información para actuar cohesionadamente frente a este tipo de comportamientos desde la perspectiva supranacional. Sobre los problemas asociados a la denominación de este tipo de hechos GUTIÉRREZ FRANCÉS, Mª.L, *Fraude informático y estafa*, Ministerio de Justicia 1991, pp. 51 y ss.

11 En este sentido MILITELLO, V. "Nuoeve esigenze de tutela penale e trattamento electtronico della informazione", *Verso un nuovo Codice penale*, Giuffrè, Milano, 1993, p. 476.

BER[12] trazó un esquema de las distintas conductas según la forma de aparición o realización del hecho que todavía se sigue en muchas ocasiones. En primer lugar se sitúa la alteración o manipulación de datos (*Computer manipulationen*), que puede tener lugar en cualquiera de los momentos a lo largo de los cuales discurre el procesamiento automatizado de datos o en el programa, e incluso sobre los elementos mecánicos de servicio en la instalación del proceso de datos, con una modificación no autorizada del resultado final del procesamiento. La destrucción de datos (*Computer sabotage*) hace referencia a los distintos medios y mecanismos a través de los cuales se logra la destrucción o inutilización de los datos almacenados o en procesamiento electrónico. La obtención no autorizada de datos (*Computerspionage*) toma en consideración el acceso inconsentido y apropiación de datos significativos contenidos en un sistema informático, con especial relevancia en el ámbito del espionaje económico. Finalmente se incluyen las distintas formas de agresión al Hardware (*Angriffe auf die Computer-Hardware*), es decir, cualquier forma de ataque a los elementos materiales constitutivos del sistema informático. Quizá hoy el desarrollo espectacular y la expansión en la aplicación a múltiples campos –si no a casi todos– hace que las formas de aparición de estos hechos y el ámbito de aplicación resulte casi ilimitado, como se podrá ver en los particulares comportamientos punibles que se expondrán a lo largo de este trabajo.

b. En realidad legislativamente existe una diversidad de conductas típicas en distintos ámbitos y formuladas con distinta óptica. Precisamente esto refleja las plurales manifestaciones e implicaciones del fenómeno informático en el ámbito penal, así como la técnica seleccionada por el legislador penal para incorporar estos hechos a la regulación positiva, especificando y concretando las modalidades delictivas ya existentes en las que el ordenador y sus aplicaciones pueden tener cabida.

---

12 ComputerKriminalität und Strafrecht, München, 1977, pp. 39 y ss. Las distintas propuestas de clasificación en la criminalidad informática pueden verse en GUTIÉRREZ FRANCÉS, Mª.L. *Fraude informático y estafa*, Ministerio de Justicia, 1991, pp. 58 y ss.

En unos casos el ordenador y sus aplicaciones constituyen el objeto material del delito (sobre el que recae físicamente la acción) y en otros un mero instrumento para cometer hechos generalmente tipificados en los CP. Por eso la doctrina alemana define estos supuestos como el conjunto de actos (punibles o dignos de incriminación) en los cuales el ordenador (o el procesamiento automatizado de datos) es el instrumento o el objeto de la comisión.[13]

Por tanto podemos encontrar supuestos delictivos que recaen sobre objetos pertenecientes al mundo de la informática destrucción o sustracción de programas o material (alteración, destrucción o reproducción de datos almacenados) y también comisión de delitos variados (contra la intimidad, administración pública, patrimonio, seguridad nacional) en los que la informática representa sobre todo el medio de comisión o ejecución del hecho.

Entre la regulación legal española en la que se menciona expresamente los objetos o medios informáticos, podemos destacar: estafa informática (art. 248.2), supuesto específico de daños informáticos (art. 264.2), hechos relativos a la propiedad intelectual sobre obras en soporte informático (art. 270), descubrimiento de secretos de empresa en soporte informático (art. 278.1), descubrimiento, modificación o revelación de secretos personales y familiares (art. 197), uso indebido de terminales de telecomunicación (art. 256), fabricación o tenencia de programas o aparatos destinados a la falsificación (art. 400) e interceptación de las telecomunicaciones y su divulgación por autoridad o funcionario público (art. 536).

II. CRIMINOLOGÍA Y POLÍTICA-CRIMINAL ANTE EL EMERGENTE FENÓMENO DELICTIVO

Ante la nueva realidad que emerge con la criminalidad informática y la incertidumbre que plantean hechos que socialmente se

13 ROMEO CASABONA, C.M., *Poder Informático y Seguridad Jurídica*, Madrid 1987, p. 22. También PANSIER, F.J./JEZ, E. *La criminalitè sur l´Internet*, PUF, 2000, pp. 101-102. GUTIÉRREZ FRANCÉS, Mª.L. *Fraude informático y estafa*, Ministerio de Justicia, 1991, pp. 44-5 y 50.

consideran nocivos e incluso resultan ilícitos desde una perspectiva general, se suscita la duda sobre las repercusiones jurídico-penales de los mismos. En estas circunstancias los fenómenos que así se presentan deben ser abordados inicialmente desde la perspectiva de la política criminal y la criminología, como instrumentos de que dispone la ciencia global del Derecho penal o la Enciclopedia de las Ciencias penales.

1. Criminología y delincuencia informática

La criminología se centra en la fenomenología, en el modo de operar el autor y de aparición en la realidad de estos hechos. En un sentido semejante puede entenderse como "la disciplina que se ocupa del estudio de las distintas manifestaciones del delito o crimen como fenómeno empírico".[14] El análisis criminológico de la delincuencia informática constituye el aspecto más relevante de los estudios sobre esta materia, pues aparte de tratarse de un fenómeno reciente, que necesita conocer exactamente en qué consiste, es la vertiente de mayor singularidad y novedad. Dogmáticamente, aunque los delitos ya existentes necesiten el esfuerzo de los juristas para determinar las dificultades y soluciones al atraer y regular estos nuevos hechos, en realidad, resulta dudoso si están presentes nuevos bienes jurídicos tutelados y nuevas categorías delictivas.

La informática y sus aplicaciones se toman en consideración por la criminología en cuanto hecho real que proporciona enormes potencialidades y posibilidades propias de los sistemas informáticos para cometer hechos ya punibles o merecedores de pena, con circunstancias de hecho que hacen más dificultosa la averiguación y la prueba. Por ello la criminología aborda desde esta perspectiva tanto las características propias de los sistemas informáticos que los convierten en objetos o instrumentos cualificados del delito, como la descripción de los concretos hechos informáticos de carácter delictivo, cuanto la determinación de los tipos de autores concurrentes en estos hechos.

---

14 LUZÓN PEÑA, Diego-Manuel, *Curso de Derecho Penal. Parte General I*. Universitas, Madrid, 1996, p. 104.

De esta manera el procesamiento electrónico de datos se convierte en un relevante factor criminógeno[15] en el seno de las distintas entidades públicas y privadas que se sirven de sistemas informáticos como modo de conseguir una eficiente organización. Desde la perspectiva del autor del hecho ilícito la presencia de estos sistemas acrecienta las posibilidades de actuación ilícita y la posición cualificada de quienes poseen especiales conocimientos en esta materia y de quienes están encargados del manejo de tales sistemas informáticos. La mayor facilidad de acceso y el conocimiento de la información procesada o almacenada proporciona una plataforma y la ocasión para que quienes se sitúan en contacto con los sistemas informáticos se conviertan en autores de hechos punibles en los que estos sistemas jueguen un papel destacado.[16] Se puede hablar así de autores internos, frente a los autores externos que realizan el hecho desde fuera del sistema.[17]

También en relación a los hechos mismos introducen estas nuevas técnicas factores favorecedores de la comisión de un hecho delictivo. La propia naturaleza de los métodos de procesamiento y almacenamiento informático de datos refuerzan esta posición. Características como la gran capacidad de almacenamiento de datos mediante ellos, la enorme velocidad de trabajo y rapidez en las operaciones, la exactitud y seguridad que proporcionan, su flexibilidad para conseguir muy diversas aplicaciones,[18] así como la dificultad de reconocer los comportamientos ilícitos cometidos a través del manejo de sistemas informáticos y la no visualización de los pasos seguidos en la ejecución del hecho, constituyen aspectos que facilitan la elección de

15 Ya puesto de relieve por SIEBER, U., Computerkriminalität, München, 1977, pp. 158 y ss. También GUTIÉRREZ FRANCÉS, Mª.L., *Fraude informático y estafa*, Ministerio de Justicia, 1991, p. 42.

16 Sobre el perfil de los autores de estos hechos puede verse, entre otros, PANSIER, F.J./JEZ, E., *La criminalitè sur l´Internet*, PUF, 2000, pp. 95 y ss.

17 TIEDEMANN, K., "Computerkriminalität und Strafrecht". *Internationalen perspektiven in Kriminologie und Strafrecht II. Festschrift für Günther Kaiser zum 70. Geburtstag*. Berlín, 1998, p. 1376.

18 Estas características de los sistemas informáticos mencionadas ya por SIEBER, U., Computerkriminalität, München, 1977, pp. 14 y ss.

objetivos con un elevado rendimiento, la ejecución del hecho, y dificultan seriamente el conocimiento y persecución del infractor.

Desde el punto de vista criminológico sí que se pueden destacar un conjunto de características generales a estos hechos delictivos y que los dotan de un eje común al conjunto de delitos informáticos.[19] Se trata en primer lugar de hechos en los que es característico su permanencia y automatismo. Precisamente por la propia naturaleza del procesamiento electrónico de datos es posible repetir la operación innumerables veces, una vez detectada una laguna en el procesamiento o creado un procedimiento ilícito de intervención en el mismo. Por otra parte este tipo de hechos delictivos acarrean o pueden acarrear unos efectos con gran expansión, pues actúan sobre objetos normalmente sin límite físico. Así si tomamos como ejemplo el dinero, los resultados cuantitativos de la criminalidad clásica son mucho más limitados al verse constreñida a actuar sobre elementos materiales, pero en este caso al tratarse de dinero contable los perjuicios pueden alcanzar dimensiones mucho mayores.

Además las dificultades para la averiguación y persecución de estos hechos son notables: aparecen reflejados en los sistemas un elevadísimo número de procesos singulares ejecutados, con lo que la individualización del hecho se entorpece gravemente, los procesos sobre los que se ejecuta el delito no son directamente visibles y están cifrados, e incluso finalmente los costos económicos de esta tarea investigadora pueden en muchos casos no resultar rentables para la víctima. Igualmente el autor de estos hechos responde a un cierto perfil criminológico. En unos casos, sobre todo los que se produjeron al comienzo de la aparición de estas modalidades delictivas, se trata de jóvenes infractores que manejan o juegan con el ordenador durante muchas horas al día, y que sin perseguir fines

19 Véase SIEBER, U., "Criminalidad informática: peligro y prevención". *Delincuencia informática*. PPU, MIR PUIG (Comp.), Barcelona, 1992, pp. 29 y ss. Sobre los rasgos generales de la criminalidad informática puede verse GUTIÉRREZ FRANCÉS, Mª L. *Fraude informático y estafa*, Ministerio de Justicia 1991, pp. 71 y ss. También en LEGANÉS GÓMEZ, S./ORTOLA BOTELLA, Mª E. *Criminología, Parte Especial*, Tirant lo blanch, Valencia 1999, p. 335. Una referencia a este tipo de criminalidad en KAISERE/KERNER, *Kleines Kriminologisches Wörterbuch*, Heidelberg, 1993, pp. 75 y 590.

determinados disfrutan rebasando límites y consiguiendo metas con su ordenador. En los hechos delictivos con mayor contenido patrimonial aparecen personas de más edad, con una buena formación en esta materia y que son habitualmente los encargados del manejo de sistemas informáticos en empresas y administración.

Como se ha dicho estos procedimientos representan particulares dificultades en el descubrimiento de los hechos y su persecución. En el ámbito de la delincuencia informática se presentan sin duda importantes complicaciones para el descubrimiento y la investigación de los hechos en y mediante el ordenador, de forma que puede en ocasiones no ser raro que muchos de los casos no lleguen nunca a detectarse. Según datos del FBI sólo se llegan a descubrir un 1% de los casos, de éstos únicamente el 14% se ponen en conocimiento de las autoridades y, finalmente, tan sólo un 3% de estos últimos acaba en una sentencia condenatoria,[20] con lo que se evidencian los graves problemas que –desde muchas ópticas– se ciernen sobre la lucha contra este tipo de hechos. Las alteraciones de datos y programas y los accesos a sistemas informáticos no dejan huellas semejantes a la de la delincuencia tradicional, de forma que las "huellas electrónicas" introducen una gran novedad y complejidad. Existe la posibilidad de identificar quiénes de manera ilícita introducen y procesan datos mediante *loggins* y otros registros.[21]

Pese a ello desde el punto de vista técnico se aprecian problemas de envergadura en la investigación, pues el rastreo informático de la ejecución delictiva se entorpece con la característica falta de visualización de los pasos lógicos ejecutados y la numerosa acumulación de procesos individuales que se ejecutan diariamente y a lo largo del tiempo en un sistema informático.[22] Con ello la indivi-

---

20 Datos aportados por SIEBER, U. "Criminalidad informática: peligro y prevención". *Delincuencia informática*. PPU, MIR PUIG (Comp.), Barcelona, 1992, pp. 31-32, de forma que de cada 22.000 autores de estos hechos, solamente 1 de todos ellos resultaría condenado por los Tribunales, según menciona el propio SIEBER.

21 SIEBER, U., "Documentación para una aproximación al delito informático". *Delincuencia informática* (MIR PUIG Comp.), PPU, Barcelona 1992, p. 94.

22 Véase al respecto CONSENTINO. G. y otros. "Tras los pasos de la seguridad perdida. Delitos informáticos". *Informática y Derecho,* 23, 26 (1998), p. 1198.

dualización del concreto proceso de ejecución del hecho delictivo alcanza cotas elevadas de complejidad técnica, duración y coste económico. Una alternativa frente a los anteriores obstáculos consiste en seguir la pista al dinero mismo a los efectos patrimoniales en el caso de que se trate de un asunto con contenido económico.[23] Además todo ello se ve agravado desde el momento en que, precisamente para esquivar la investigación, el acceso a la red o los contenidos introducidos pueden ser trasladados convenientemente a otros servidores.[24]

2. La política criminal ante la aparición de la criminalidad informática

La política criminal, por su parte, examina el merecimiento de pena de nuevos hechos surgidos en torno a la informática y la forma más eficaz de la lucha contra el delito. "Es aquella ciencia que trata de determinar con arreglo a determinados criterios las conductas que deben ser consideradas y definidas como delitos y los medios que es posible, necesario, eficaz y adecuado emplear para prevenir delitos".[25] Por ello las funciones básicas de la política criminal en este campo serán las de estudiar y formular un conjunto de medidas preventivas que traten de evitar este tipo de hechos tanto con relación al autor como a los hechos mismos,[26] la de deter-

---

23 Así SIEBER, U. "Documentación para una aproximación al delito informático". *Delincuencia informática*. MIR PUIG (Comp.), PPU, Barcelona, 1992, pp. 94 y ss.

24 En este sentido MORON LERMA, E., *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red*. Aranzadi, 1999, p. 122.

25 LUZÓN PEÑA, D-M., *Curso de Derecho Penal. Parte General I*. Universitas, Madrid, 1996, p. 98.

26 Para estos aspectos en general y en relación a todo lo que sigue en cuanto a las medidas de precaución en empresas y Administración para evitar la vulneración de sus sistemas informáticos, puede verse TIEDEMANN, K., "Computerkriminalität und Strafrecht". *Internationalen perspektiven in Kriminologie und Strafrecht II. Festschrift für Günther Kaiser zum 70. Geburtstag,* Berlín, 1998, pp. 1376 y ss. SIEBER, U., "Criminalidad informática: peligro y prevención". *Delincuencia informática*. (MIR PUIG Comp.). PPU, Barcelona, 1992, pp. 34 y ss. Y del mismo autor "Documentación para una aproximación al delito informático". *Delincuencia informática*. (MIR PUIG Comp.), PPU, Barcelona, 1992, pp. 83 y ss. La Association International de Droit penal en su Resolución sobre "Infractions informatiques et

minar dentro del conjunto de hechos ilícitos relacionados con la informática aquellas conductas más graves y relevantes que deban ser consideradas merecedoras de sanción criminal, así como el examen de la legislación vigente para comprobar su adecuación a estas nuevas realidades del mundo delictivo, formulando, en su caso, propuestas legislativas para la incorporación de nuevas conductas a la legislación criminal o modificaciones de la legislación vigente.

La prevención de los ataques a los sistemas informáticos exigen la adopción planificada de un conjunto de medidas de seguridad previo un análisis de las necesidades de protección específicas y de las hipotéticas fuentes de peligro. Sólo la toma de conciencia de esta necesidad permitirá el establecimiento de una auténtica estrategia de seguridad informática.

Las distintas medidas de seguridad hacen referencia a distintos aspectos. En el ámbito de la organización de la empresa o de las oficinas públicas cabe la creación de un departamento especializado en la seguridad del sistema informático, encargado de la planificación de este sector y de la ejecución de las medidas de seguridad así como de la verificación periódica del desarrollo de las medidas ya implantadas. En cuanto al personal de la empresa o empleados públicos responsables del procesamiento de datos deben ser seleccionados cuidadosamente. Debe procederse a una correcta configuración de los contratos de trabajo de este personal, con especial énfasis en algunas obligaciones de sigilo profesional durante su permanencia en la empresa y aún después, al menos durante un tiempo.

Técnicamente se puede restringir el acceso a las distintas partes del sistema informático según las necesidades, mediante las correspondientes claves. Entre los datos almacenados en el sistema se puede introducir, preventivamente, alguna dirección del personal de seguridad o de dirección con alguna errata. Si estas personas reciben alguna oferta de la competencia se habrá detectado el

---

autres crimes contre la technologie informatique" propone una serie de medidas de seguridad no técnicas, sino de formación y éticas. *International Review of Penal Law, 66 (1995)*, pp. 27 y ss.

problema. Percibidas a tiempo estas intromisiones ilegítimas en el sistema se puede evitar la ejecución de acciones completas, reduciendo los perjuicios al mínimo.

Para el desarrollo de las funciones propias de la política criminal a las que acabamos de aludir, es preciso señalar que hoy se entiende generalmente que dogmática jurídico-penal y política criminal no son disciplinas contrapuestas, sino que, al contrario, ambas se complementan y se necesitan para llevar a cabo su específica misión. Distinguiéndose y gozando cada una de ellas de su ámbito de actuación se constata cómo en su implementación resultan interdependientes y cada una se sirve, para actualizar su propia función, de conceptos y principios de la otra, de manera que en muchas ocasiones no se podrá precisar con exactitud en qué lado nos encontramos. En casos la interpretación dogmática acude a las finalidades político criminales a la hora de decidir la antijuricidad de una conducta o cuando desarrolla y concreta el alcance de reglas generales o aspectos no legislados.[27]

También la política criminal en el desempeño de sus funciones acude a categorías y contenidos proporcionados por la dogmática. Los modelos regulativos propuestos por la política criminal no pueden desconocer las reglas de la dogmática, así como la política criminal debe contar con categorías jurídico-dogmáticas como bien jurídico, desvalor de resultado, o desvalor de acción cuando pretende evaluar la necesidad de incorporar nuevas conductas a la zona abarcada por la legislación penal. Igualmente resulta decisivo para la política criminal contar con los datos e imágenes empíricas de la realidad proporcionadas por la criminología.

La conducta merecedora de sanción penal destaca fundamentalmente a través de dos datos: desvalor de acción y desvalor de resultado, como contenidos fundamentales requeridos por la antijuricidad de un hecho penalmente relevante. El *desvalor de resultado*, en cuanto hace referencia a la causación de un estado jurídicamente desaprobado, se concibe como la lesión o puesta en peligro

27 Cfr. ROXIN, C., *Derecho Penal, Parte General, Tomo I*, Civitas, 1999, &7 nm. 71-2.

de un bien jurídico-penalmente relevante. Por otra parte el desvalor de acción se concibe aquí considerando especialmente su componente objetivo,[28] es decir, en relación a las propiedades materiales de la acción que la hacen peligrosa para el bien jurídico protegido.

En primer lugar cabe entonces acercarse al problema que plantea el contenido del desvalor de resultado. Con la aparición de la delincuencia informática SIEBER[29] suscita el interrogante de sí con estos hechos se incorpora un nuevo bien jurídico autónomo –individualizado– para estos casos, es decir, los ilícitos penales informáticos suponen ¿una nueva técnica de ofensa a bienes tradicionales o un nuevo bien jurídico penalmente tutelable?[30]

En un primer momento estos nuevos hechos se recogen y tratan de forma imprecisa en el marco amplio de la ascendente delincuencia económica. Así el Proyecto Alternativo alemán (parte especial, delitos económicos) incluye en un anexo los delitos informáticos y la reforma penal que introduce los supuestos de delincuencia informática, en el Código penal alemán se efectúa a través de la llamada Segunda Ley de lucha contra la criminalidad económica.[31] Esta asociación inicial se establece de forma casi tácita, aun cuando finalmente se reconoce que la criminalidad informática "es independiente de la conformación de los sistemas económicos".[32]

De otro modo distinto para SIEBER,[33] tomando como punto de referencia la teoría sistémica sociológica, en estos casos se produce

---

28 Sobre el doble aspecto objetivo y subjetivo del desvalor de acción puede verse LUZÓN PEÑA, D-M., *Curso de Derecho Penal. Parte General I*. Universitas, Madrid, 1996, pp. 332-336.

29 Computerkriminalität und Strafrecht, München, 1977, pp. 251 y ss.

30 Así lo plantea MILITELLO, V., "Nuoeve esigenze de tutela penale e trattamento electtronico della informazione", *Verso un nuovo Codice penale*, Giuffrè, Milano, 1993, p. 475.

31 TIEDEMANN, K., *Poder Económico y delito*. Ariel, Barcelona, 1985, pp. 32 y ss. En el sentido de establecer una relación con los intereses económicos se encuentra la Resolución de la Association International de Droit Penal en el XV Congreso Internacional de Derecho Penal sobre "Infractions informatiques et autres crimes contre la technologie informatiche". *International Review of Penal Law 66 (1995),* p. 28, punto 3.

32 TIEDEMANN, K., *Poder Económico y delito*. Ariel, Barcelona, 1985, p. 121.

33 Computerkriminalität und Strafrecht, München, 1977, pp. 257 y ss.

una coexistencia de bienes colectivos e individuales, dispensando pues protección tanto a intereses personales como de la Comunidad. Así en el ámbito de las falsedades documentales se apunta el proceso de interacción como bien jurídico funcional.

Cuando MILITELLO[34] indaga si se dan las condiciones para individualizar un nuevo bien jurídico en relación a este particular fenómeno delictivo, toma como ejemplo la estafa informática en la legislación alemana para hacer ver la novedad que representan estos hechos en cuanto al objeto jurídico de tutela. Para él, en el caso mencionado de la estafa informática, la determinación del objeto material como el resultado no influenciado de un proceso de elaboración de datos patrimonialmente relevantes introduce la posibilidad de confusión entre el objeto material y el bien jurídico protegido.

Señala este autor que la determinación de un bien jurídico descansa en la relevancia que tal objeto represente en el concreto sistema de referencia –la Constitución, indica–, y como de acuerdo a la amplia difusión de los elaboradores electrónicos en nuestra vida comunitaria se puede establecer un nuevo objeto de tutela unitario y autónomo que suponga un denominador común para todas las infracciones penales cometidas mediante el ordenador: la intangibilidad informática. Ésta indicaría la multiforme exigencia de no alterar la relación triádica entre dato de la realidad, respectiva información y sujeto legitimado para elaborar la misma en sus distintas fases (creación, transferencia y recepción). La constatación de este interés jurídico-penal no impide sin embargo que en determinados casos puedan aparecer, complementariamente, otros bienes jurídicos tradicionales (delitos pluriofensivos).[35]

---

34 "Nuoeve esigenze de tutela penale e trattamento electtronico della informazione", *Verso un nuovo Codice penale*, Giuffrè, Milano, 1993, p. 478.

35 ACHENBACH señala como bien jurídico protegido el funcionamiento del sistema informático libre de perturbaciones. "*Das* Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität". *Neue Juristisches Wocheschrift* 30 (1986), p. 1838. También MORON, aunque de una manera muy inicial, señala que en los casos de sabotaje informático –delito de daños– el bien jurídico no puede identificarse con el patrimonio *sensu stricto*. *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, Aranzadi, 1999, pp. 59 y ss.

PICA[36] señala que la mencionada intangibilidad informática como objeto general expresa la necesidad de garantizar la confianza general en los procesos de elaboración informática y de utilización de las nuevas tecnologías, sin embargo, la misma no, sino un aspecto parcial de lo que representan los ilícitos informáticos. En realidad, manifiesta este autor,[37] las nuevas tecnologías representan nuevas modalidades de ejercicio de actividades y libertades ya reconocidas y tuteladas, y al mismo tiempo modalidades de ilícitos ya previstos en el ordenamiento jurídico contra bienes jurídicos ya constituidos y tutelados.

Así la libertad informática, como expresión de la libertad del individuo, consiste en el derecho a utilizar lícita y libremente, con los límites constitucionales y legales, la tecnología informática.[38] De forma que los delitos informáticos pueden verse como violación de esa misma libertad informática, como infracción de las distintas libertades a las que puede extenderse el empleo de estas tecnologías (intimidad, domicilio, libre circulación, asociación, etcétera).

Con todo ello se constataría para PICA[39] que la tentativa de delinear un bien jurídico unitario que abrace la entera materia informática está inevitablemente destinada al fracaso. Y este necesario desenlace se produce por cuanto estos hechos no representan un nuevo objeto de tutela cuanto un nuevo modo de agresión y de comisión de actividades ilícitas que se atienen a bienes jurídicos ya reconocidos y tutelados.

Si bien se aprecia en el conjunto de delitos informáticos una unidad criminológica y hasta político-criminal, no parece acertado, sin embargo, reconducirlos a un proceso unitario, homogéneo, desde el punto de vista dogmático. La amplísima gama de comportamientos punibles relacionados con los ordenadores, el papel muy diverso que pueden representar en estos hechos los elementos de

36 *Diritto penale delle technologie informatiche*, Utet, Torino, 1999, pp. 34 y ss.

37 *Diritto penale delle technologie informatiche*, Utet, Torino, 1999, p. 10.

38 PICA, G. *Diritto penale delle technologie informatiche*, Utet, Torino, 1999, pp. 7 y ss.

39 *Diritto penale delle technologie informatiche*, Utet, Torino, 1999, p. 35.

los sistemas informáticos, hacen ciertamente complejo establecer un nexo común que haga presente un nuevo interés jurídico-penalmente relevante que quepa entender introducido por el legislador penal. Todavía más: los bienes jurídicos propuestos unitariamente para el conjunto de los delitos en los que aparecen los diversos elementos de los sistemas informáticos carecen de una mínima precisión que posibilite cumplir con las funciones encomendadas al bien jurídico en el seno de la teoría jurídica del delito.

En definitiva, todo lo anterior muestra cómo esta reciente fenomenología delictiva no tiene la consecuencia de aportar ningún nuevo bien jurídico penalmente relevante, concepto en torno al cual se articulan los delitos recogidos en el Código penal. Tampoco está presente ningún otro aspecto o criterio que permita una incriminación conjunta de estos hechos. Entonces si bien no es posible hablar de "delito informático" en sentido estricto, sí parece adecuado denominar "delincuencia informática" o "criminalidad informática" a este conjunto de hechos con relevancia penal aunque desde distintos ángulos.

Los medios informáticos representan en sí mismos una conducta con un elevado desvalor de acción, por su carácter insidioso y clandestino. Pero además es preciso conectarlos al peligro o lesión de un bien jurídico de relevancia penal para que nos encontremos ante un comportamiento merecedor de incriminación y sanción penal. Entre los aspectos que hacen de los medios informáticos un cualificado medio de realización de hechos delictivos podemos citar:[40]

- Ingente potencialidad para el almacenamiento de datos.
- Gran velocidad de sus operaciones, pues procesa los datos a tiempo real.
- Exactitud y fiabilidad de sus operaciones.

---

40 Véase ROMEO CASABONA, C.M., *Poder informático y Seguridad Jurídica*, Madrid, 1987, pp. 19 y ss. Como criterio delimitador de lo que sea la criminalidad informática se propone "la especificidad de lo informático", en el sentido de atender a las peculiares características de los sistemas informáticos, de su modo de operar y de las funciones que tiene asignadas. GUTIÉRREZ FRANCÉS, Mª.L., *Fraude informático y estafa*, Ministerio de Justicia, 1991, pp. 63 y ss.

- Extraordinaria adaptabilidad a las exigencias humanas.
- No visualización directa del modo de ejecución del hecho, basado en los elementos lógicos del sistema informático.

Así se requiere la presencia tanto de uno como de otro; no basta la presencia de un bien jurídico penalmente relevante si no concurre un especial desvalor de acción en la conducta (protección del patrimonio en el caso de mero incumplimiento de contrato), pero tampoco un especial desvalor de acción no vinculado a un bien jurídico penalmente protegido.

Este último es el caso de las conductas relacionadas con la informática merecedoras de sanción penal. En ellas concurre el desvalor de acción propio de los medios informáticos, por lo que resulta necesario determinar los bienes jurídicos frente a los que la informática posee una especial vinculación, para que la conducta, en su caso, pueda resultar incriminada por el legislador.

Por tanto de todo lo anteriormente señalado podemos concluir que cuando nos referimos al "delito informático" estamos ante una categoría criminológica que, al margen de las formas concretas de incriminación en la legislación penal, atiende sobre todo a la fenomenología delictiva en la que aparece –desde la anterior década– los ordenadores y sus aplicaciones como relevante objeto del delito o como medio de comisión de hechos delictivos.

PARTE SEGUNDA

CONDUCTAS PUNIBLES EN RELACIÓN CON LA INFORMÁTICA

Vamos a hacer un repaso general del conjunto de conductas en las que –de una forma u otra de las mencionadas– la informática y sus aplicaciones desarrollan un papel relevante en una conducta punible. Los distintos delitos que van a ser expuestos pueden distinguirse entre aquellos que se incluyen en el ámbito de los hechos punibles que tutelan penalmente el patrimonio y aquellos otros que toman como objeto de protección bienes jurídicos de distinta índole a los de carácter patrimonial. En los primeros se toman en cuenta principalmente la protección penal del conjunto de bienes que pueden formar parte del patrimonio individual y resultan abarcados por la tutela penal. En el segundo grupo aparecen otros bienes jurídicos penalmente relevantes como la intimidad, el correcto proceso de maduración de los menores o la autenticidad de los documentos en el tráfico jurídico.

SECCIÓN PRIMERA

Estafa informática

Con la estafa se viene a castigar la causación de un perjuicio patrimonial cometido mediante engaño. Tan acrisolado delito, que se remonta al *Stellionatus* romano, ha ido perfilando a lo largo del tiempo los elementos constitutivos del mismo, y a los que nos vamos a referir a continuación de manera breve y sintética para dar una imagen suficiente del delito que nos ocupa y así, posteriormente, poder abordar las novedades que supone la estafa informática. Hay que tener en cuenta la importancia de este hecho punible –la estafa electrónica o informática– que puede catalogarse acertadamente como el centro del Derecho penal informático.[41]

41 Así SCHMID, N., *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich, 1994, p. 218.

I. ELEMENTOS CLÁSICOS DEL DELITO DE ESTAFA[42]

El primero de los elementos del delito de estafa es el engaño o conducta engañosa. Tal elemento según la conocida formulación de ANTÓN consiste en la simulación o disimulación capaz o apta para inducir a una o varias personas a error.

Las formas de engaño que aparecen en la práctica son de lo más variado, como la realización de algún tipo de maniobras fraudulentas o puesta en escena, atribución de cualidades falsas, uso de nombre o representación no veraz, simulación de hechos falsos, deformación u ocultación de hechos verdaderos, etc.

En el ámbito de este elemento GUTIÉRREZ FRANCÉS[43] pone de relieve la ausencia de predeterminación legal del concepto de engaño en nuestra legislación penal y como en realidad la fórmula empleada por el legislador es la de "engaño bastante", con trascendencia para la estafa informática. Según la redacción del tipo básico del delito de estafa el engaño debe ser bastante, es decir, que tanto desde la perspectiva objetiva como de la subjetiva debe resultar idóneo para conducir a error a otra u otras personas.

El error se presenta como el segundo requisito, en cuanto situación de error de quien sufre el engaño, es decir, consecuencia a la que conduce el previo comportamiento engañoso o fraudulento.

Error es el conocimiento viciado de la realidad. Consiste en la situación intelectual provocada por el engaño que supone una discordancia entre la representación de la realidad por el engañado y la realidad.

Posteriormente se debe producir un acto de disposición consecuencia de la situación de error. El engañado pues, a raíz de su

---

42 Sobre ellos puede verse ANTÓN ONECA, J., *Las estafas y otros engaños*, Seix, Barcelona, 1957, p. 4-14. En GUTIÉRREZ FRANCÉS, Mª.L. *Fraude informático y estafa*, Ministerio de Justicia, Madrid 1991, especialmente pp. 277 y ss. se ofrece un amplio desarrollo de los elementos de la estafa convencional y su relación con la estafa informática. También PÉREZ MANZANO, M., en BAJO FERNÁNDEZ (Director), *Compendio de Derecho Penal (Parte Especial), volumen II*, Ceura, Madrid, 1998, pp. 443 y ss.

43 *Fraude informático y estafa*, Ministerio de Justicia, Madrid, 1991, pp. 336 y ss.

error al que le induce el sujeto activo, lleva a cabo un comportamiento que implique algún tipo de disposición patrimonial.

El mismo puede afectar a cualquier elemento patrimonial, de manera que podría concretarse en la entrega de una cosa (material o dineraria), en la realización de un acto documental con trascendencia económica (gravamen de un bien), o la prestación de cualquier tipo de servicio, todo ello siempre cuantificable económicamente.

En este momento se exige identidad entre engañado y disponente, es decir, resulta necesario que quien lleva a cabo este acto con contenido patrimonial sea la misma persona que la que ha sufrido el engaño, pues sino, no estaría presente la relación medial necesaria entre ambos elementos.

El conjunto de hechos anteriores va a producir un perjuicio propio (de quien recibe directamente el comportamiento engañoso) o de un tercero. Al tratarse de un perjuicio propio o de tercero ya no es preciso la coincidencia entre ambos sujetos, quien recibe directamente el previo comportamiento y quien finalmente ve alterado su saldo patrimonial. Pueden ser distintos el engañado y el perjudicado en su patrimonio.

Este perjuicio patrimonial constituye el auténtico resultado del delito, como consecuencia derivada del comportamiento del sujeto activo que el legislador selecciona y exige para que el delito pueda entenderse consumado. Perjuicio patrimonial de la víctima, en el sentido de un saldo patrimonial negativo, debiendo haber sufrido su patrimonio una disminución comparado el mismo antes y después del hecho.

El Ánimo de lucro[44] forma parte también de los elementos necesarios en la ejecución del delito de estafa. El ánimo de lucro concebido como la pretensión del autor del hecho de conseguir, derivado del mismo, un beneficio patrimonial para sí mismo o para un

44 Sobre el concepto de ánimo de lucro en general, con la pugna entre el concepto amplio manejado generalmente por los Tribunales y el concepto restrictivo de sentido exclusivamente patrimonial, puede verse MATA y MARTÍN, R.M., *El delito de robo con fuerza en las cosas*, Ed. Tirant lo blanch, Valencia, 1995.

tercero, informa también el hecho punible aunque ahora desde la esfera interna del autor, como elemento que exige también el delito pero desde la vertiente subjetiva, la propia del sujeto activo.

Todos estos elementos que acabamos de ir exponiendo como los que dan origen al delito de estafa, se encuentran encadenados en una relación de progresión, de manera que el anterior siempre debe ser causante del posterior. Es decir, se precisa sucesivamente entre ellos una relación causal en cadena. Relación de causalidad entendiendo la jurisprudencia el engaño como condición cuantitativamente dominante en la producción del resultado (s. TS 22-5-97[45] –FJ 4º–), según la fórmula procedente de ANTÓN.

La tipicidad del delito depende de la afirmación de la relación de causalidad entre el comportamiento del sujeto activo y el resultado patrimonial desfavorable, por una parte, y, por otra, de la imputación objetiva del hecho a su autor. La imputación objetiva reclama tanto la efectiva peligrosidad del comportamiento engañoso en la causación del perjuicio patrimonial como la superación del riesgo permitido con el mismo.[46]

La peligrosidad objetiva del comportamiento necesaria para inducir a error a la víctima y producir el consiguiente menoscabo patrimonial fruto de la previa disposición sobre alguno de los elementos constitutivos de su propia masa patrimonial. También resulta exigible desde esta perspectiva que el riesgo creado mediante el engaño constituya un riesgo no permitido, excluyéndose del ámbito de la tipicidad de la estafa todas aquellas exageraciones o inexactitudes que son práctica habitual en el tráfico jurídico.

---

45 (A. 4435). Caso en el que no media manipulación informática alguna, pero que en fecha reciente nos recuerda esta construcción sobre la relación de causalidad en el ámbito del delito de estafa que mantiene la jurisprudencia.

46 Véase PÉREZ MANZANO, M., en BAJO FERNÁNDEZ (Director), *Compendio de Derecho Penal (Parte Especial), volumen II*, Ceura, Madrid 1998, p. 453. Véase también CHOCLAN MONTALVO, J.A., *El delito de estafa*, Bosch 2000, pp. 294 y ss. También de M. PÉREZ MANZANO, con mayor detenimiento, "Acerca de la imputación objetiva en la estafa". *Hacia un Derecho Penal Económico Europeo, Jornadas en honor del profesor Klaus Tiedemannn*, BOE 1995, pp. 285 y ss. Ya antes referencias a la imputación objetiva en el ámbito del delito de estafa en TORÍO LÓPEZ, A., "Acción y resultado típico en la estafa procesal". *Libro homenaje al prof. J. Antón Oneca*, Universidad de Salamanca, 1982, p. 877.

Como pone de relieve GUTIÉRREZ FRANCÉS[47] la moderna teoría de la imputación objetiva permite fundamentar satisfactoriamente la no relevancia penal de ciertos engaños habituales en el tráfico comercial. Siendo cierto que tales comportamientos fraudulentos consiguen generar una transferencia patrimonial, sin embargo no aportan un peligro para tal patrimonio jurídicamente prohibido, o bien el riesgo que pudieran crear para la masa patrimonial fuera de los catalogados como permitidos en el tráfico.

II. EL PROBLEMA DEL ENGAÑO COMO ELEMENTO DE LA ESTAFA

El comportamiento nuclear de la estafa gira en torno al engaño, a la acción fraudulenta. El engaño constituye el específico desvalor de acción de la estafa. Ahora bien en el ámbito de la estafa ha existido tradicionalmente el problema de no admitirse los engaños a las máquinas o instrumentos automáticos.

La Postura tradicional[48] sobre este aspecto del delito ha mantenido claramente que no se puede engañar a las máquinas. Entre los

---

47 *Fraude informático y estafa*, Ministerio de Justicia, Madrid, 1991, p. 387.

48 Por todos véase ANTÓN ONECA, J. *Las estafas y otros engaños*, Seix, Barcelona, 1957, p. 10. Ampliamente expuesto el problema en GUTIÉRREZ FRANCÉS, Mª.L. *Fraude informático y estafa*, Ministerio de Justicia, Madrid 1991, pp. 336 y ss. Problemas que, por otra parte, también se suscitaron en la doctrina comparada. Así para el caso de Suiza puede verse SCHMID, N. *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich 1994, pp. 255 y ss. De otra manera, aunque con igual conclusión, CONDE-PUMPIDO FERREIRO no ve el problema en el engaño sino en el acto de disposición. Según este autor la dificultad reside en que el acto de disposición ha de ser realizado por otro, esto es una persona, y además ser fruto de un acto de voluntad. Aquí ni la transferencia la realiza una persona, ni el requisito de que tal transferencia sea "no consentida" permite hablar de un acto de disposición voluntario. Por ello estamos, de acuerdo al mencionado autor, ante una estafa especial y analógica, independiente del tipo básico y de sus elementos constitutivos. Véase *Estafas*, Tirant lo blanch 1997, pp. 215 y 217. En realidad esta opción cae en los mismos errores que achaca acertadamente a quienes no admiten el engaño realizado a través de los sistemas informáticos. La transferencia en estos supuestos se realiza mediante el intermediario informático pero no deja de poder ser atribuida a una persona. No puede llegarse al extremo de pensar que es algo que sucede sin que tenga que ver con alguna decisión humana. Es irreal que el mencionado acto de disposición no tenga que ver con ninguna voluntad humana.

argumentos esgrimidos en apoyo de esta tesis pueden mencionarse los siguientes: Si la estafa requiere que el engaño produzca un error en otro, una máquina no puede ser ese "otro", sino que ese otro sólo puede ser una persona física, ya que sólo la persona física podría tener una falsa representación de la realidad.[49] Es decir vendría a afirmarse la "exigencia de que la estafa se desarrolle en el marco de una relación *intuitu personae*. Es decir la necesidad de que el engaño se dirija directamente a una persona física, a que ésta debe captar el contenido del engaño y, por lo tanto, debe darse el error como estado psicológico".[50] En este sentido se llega a señalar que, de evitarse esta concepción del engaño, la aplicación de la norma de la estafa supondría analogía prohibida contra reo.[51]

Estos mismo problemas se habían suscitado previamente en la doctrina comparada, singularmente entre los autores alemanes, pues se entendía que la estafa como tipo penal más próximo presentaba ciertas limitaciones en su tipo objetivo, especialmente en relación al engaño sobre aparatos automáticos. Para estos casos tratados con antelación en la doctrina alemana se había acuñado la expresión "*Eine maschine kann nicht irren*"[52] lo que excluía de raíz la aplicación del tipo de estafa.

Pero también se entendía que "engaño, error y disposición patrimonial lesiva, que exigen la presencia de una persona física, receptora material del engaño, a consecuencia del cual incurra en un error que desencadene el acto de disposición patrimonial".[53] La acep-

---

49 Véase al respecto, BAJO/PÉREZ MANZANO, *Manual de Derecho Penal (Parte Especial) (Delitos patrimoniales y económicos),* Ceura, 1993, pp. 299-300.

50 PÉREZ MANZANO, M. en BAJO FERNÁNDEZ (Director), *Compendio de Derecho Penal (Parte Especial), volumen II*, Ceura, Madrid 1998, p. 455.

51 VALLE MUÑIZ, en QUINTERO OLIVARES (Director*), Comentarios a la Parte Especial del Derecho Penal*, Aranzadi 1999, p. 522, citando a GUTIÉRREZ FRANCÉS.

52 Véase CARSTEN, U. "Computerbetrug (&263ª StGB*)", Internet-Zeitschrift für Rechtsinformatik*, p. 4, en http://www.jurpc.de/aufsotz/.

53 Sobre las necesidades político-criminales y dogmáticas de llevar a cabo una nueva tipificación para estos hechos CARSTEN, U. "Computerbetrug (&263ª StGB*)", Internet-Zeitschrift für Rechtsinformatik*, pp. 2 y ss. Ampliamente en GUTIÉRREZ FRANCÉS, Mª.L., *Fraude informático y estafa*, Ministerio de Justicia, Madrid 1991,

tación de las insuficiencias de la regulación penal ante el fenómeno criminal vinculado a los medios informáticos tuvo como consecuencia la aprobación de la llamada "Segunda Ley de Lucha contra la criminalidad económica"[54] con el fin de atajar fundamentalmente este grupo de deficiencias.

Sin embargo sobre este mismo problema no ha dejado de suscitar una nueva postura doctrinal, incluso antes de la aprobación del CP de 1995, de acuerdo a la cual el engaño no comporta necesariamente una relación directa y personal entre dos seres humanos, defendida por autores como GUTIÉRREZ FRANCÉS o DE LA MATA.[55] Para estos autores, en realidad las máquinas o los ordenadores no sufren engaño alguno ni realizan por error acto de disposición, sino que se limitan a ejecutar el traspaso patrimonial ordenado y dispuesto por quien ha efectuado la programación (engaño al programador o a la institución).[56] Puede entenderse que, con mayor o menor distancia temporal y física, al final sufre engaño una persona, aun cuando no sea personal ni directo.

---

pp. 154 y ss. Esta misma autora señala cómo la jurisprudencia francesa había admitido estos hechos como una maniobra fraudulenta más del tipo clásico de la estafa. También CONDE-PUMPIDO FERREIRO señala que la jurisprudencia francesa no tuvo reparo en aplicar la estafa en los casos de defraudaciones sobre aparatos automáticos. *Estafas*, Tirant lo blanch 1997, p. 215.

54 *Zweite Gesetz zur Bekämpfung der Wirtschafts Kriminalität (2. WiKG)*. Pese a este intento de subsanar los problemas dogmáticos para la aplicación del delito de estafa y evitar lagunas político-criminalmente improcedentes, la nueva regulación del & 263ª StGB no ha dejado de suscitar otros inconvenientes. Entre ellos se menciona las posibles fricciones que la redacción del precepto presenta con las garantías dimanantes del principio de legalidad. Así KINDHÄUSER, U. "Der Computerbetrug (% 263ª StGB) –ein Betrug*?", Festschrift für Geral GrünWald*, Baden-Baden, 1999, p. 285. También CARSTEN, U. "Computerbetrug (&263ª StGB*)", Internet-Zeitschrift für Rechtsinformatik*, p. 12.

55 GUTIÉRREZ FRANCÉS, M.L., *Actualidad Informática Aranzadi*, 11 (1994), p. 11. También DE LA MATA BARRANCO, N. "Utilización abusiva de cajeros automáticos: apropiación de dinero mediante la tarjeta sustraída a su titular", *Poder Judicial* número especial IX (nuevas formas de delincuencia) (1988), pp. 172 y ss.

56 GUTIÉRREZ FRANCÉS, M. L., "Fraude informático y estafa", *Actualidad Informática Aranzadi* 11 (1994), p. 11.

GUTIÉRREZ FRANCÉS[57] propuso la revisión crítica del concepto tradicional de engaño con base en los cambios sociales surgidos en el mundo contemporáneo y por la singularidad de nuestra legislación –frente a otras– que no acota un concepto prejurídico de engaño, sino que alude al engaño con carácter general y su delimitación puede efectuarse mediante criterios normativos. Recuerda esta autora la no concreción legal del contenido y alcance del engaño como elemento de la estafa. Es más entiende que la indeterminación legal sobre el engaño no es sólo político-criminalmente aceptable sino que resulta necesaria. Al contenido del engaño se le ha dado un protagonismo inmerecido. Lo que interesa son las conductas engañosas a que se refiere el tipo vigente de estafa. La clave la proporcionaría el tipo mismo cuando alude al empleo de "engaño bastante para producir error en otro". Lo que caracteriza al engaño es que la falsedad objetiva que se exterioriza sea consciente y que vaya dirigida a provocar error. Es decir lo que se requiere es la idoneidad, aptitud o suficiencia del comportamiento para generar error en otro. La descripción típica pone en relación engaño y error a través de la idea de suficiencia, idoneidad o aptitud.

La posición de la jurisprudencia sobre el problema aludido, como consecuencia de la primera de las opiniones antes expuestas, ha sido la negativa a admitir el engaño sobre máquinas o aparatos automáticos. Antes del CP 1995 se niegan por los Tribunales la posibilidad de entender realizado el delito de estafa en los fraudes informáticos, como resultado de la aplicación de la concepción del engaño que se ha mencionado. Así la sentencia del TS de 19-4-91,[58] en relación al apoderado de un banco que haciendo apuntes falsos vía ordenador consigue un enriquecimiento ilícito, excluye la aplicación del delito de estafa.

---

57 *Fraude informático y estafa*, Ministerio de Justicia, Madrid 1991, pp. 341 y ss, 409 y ss.

58 *Actualidad Penal* 541/1991, p. 1194, en la que el autor resulta condenado por un delito de apropiación indebida por la condición de apoderado del Banco Hispano Americano con lo que se entendía que los fondos le habían sido entregados para su administración. La sentencia procede de la AP de Granada que inicialmente consideró probado un delito de estafa y que como señalamos corrige el TS al entender inaplicable la figura de acuerdo a la comprensión del elemento del engaño.

III. LA ESTAFA INFORMÁTICA EN GENERAL

a. El legislador de 1995 zanja el tema al admitir un supuesto específico de estafa informática donde se sustituye el término engaño por el de manipulación informática. De este modo el legislador prevé un supuesto específico de estafa informática (art. 248.2) en la que se castiga la manipulación de datos almacenados en sistemas informáticos para lograr una transferencia no consentida de activos patrimoniales.

b. Con el cambio mencionado se plantea inmediatamente la relación que guarda este nuevo supuesto con el tipo básico de estafa del art. 248.1.[59] En la discusión sobre esta relación de la estafa informática con la estafa genérica, surgen enseguida dos alternativas:

Por una parte, quienes entienden que los elementos de la estafa informática siguen manteniendo los de la estafa genérica,[60] es decir que en realidad se trata de una mera adaptación legislativa a las necesidades que incorpora la estafa informática, pero siempre dentro de la dogmática y criterios interpretativos propios de este delito. Con ello resultaría perfectamente válido todo lo señalado por doctrina y jurisprudencia para la estafa genérica, pues el nuevo precepto no representa sino una especificación del legislador para evitar dudas sobre la aplicación del delito a estas recientes realidades. Para VIVES/GONZÁLEZ CUSSAC[61] se trata de una estafa genérica, si bien aquí no hay engaño ni error, pero su estructura típica es exactamente la misma.

De otra manera nos encontramos con quienes entienden que el concepto general de estafa no ejerce como criterio interpretativo, pues no comparte la dinámica de la estafa tradicional, ya que estas

---

59 Discusión que ha surgido en la doctrina comparada y se mantiene en fechas recientes. Así Urs KINDHÄUSER se pregunta "Der Computerbetrug (&263ª StGB) –ein Betrug?". *Festschrift für Gerald Grünwald*, Baden-Baden, 1999.

60 Así GONZÁLEZ RUS, J.J. *Curso de Derecho Penal Español, Parte Especial I*, Marcial Pons, Madrid 1996, p. 687.

61 *Derecho Penal, Parte Especial*, Tirant lo blach, 1999, pp. 453 y ss.

nuevas modalidades son ajenas al engaño.[62] Desde este punto de vista en realidad la nueva estafa informática sólo presenta afinidades con escasos elementos de la estafa en su configuración tradicional y por tanto no sirve como referencia.

Como apoyo a esta posición se señala que "Quienes realizan la conducta descrita en esta disposición no cometen estafa, sino que 'se consideran' (como dice la redacción del art. 248.2) legalmente reos de estafa. De esta manera con esta fórmula se pretendería colmar una posible laguna de punición, que había sido observada por la doctrina, sin desvirtuar el contenido dogmático de los elementos de la estafa ni las relaciones entre ellos", según PÉREZ MANZANO.[63] Con ello esta autora entiende la declaración legal en el sentido de que precisamente al decir "se consideran" está señalando que realmente no lo son, pero –bajo otro punto de vista– también puede tratarse de una mera fórmula lingüística para reforzar la idea de que debe incluirse este tipo de comportamientos en el ámbito de la estafa y por tanto resultar punibles estos hechos, frente a las dudas que siempre suscitan las nuevas realidades.[64]

c. Con estos pasos previos podemos ya abordar la estructura de la estafa informática, en la que se reúnen los elementos que deben concurrir para poder apreciar este nuevo supuesto. Para ello, vamos a tomar como referencia, pues entendemos que nada se opone pese a lo anteriormente señalado, la estructura de la estafa genérica. Ello permite sin duda una mayor claridad y precisión en la determinación del comportamiento típico.

---

62 VALLE MUÑIZ, J.M., en QUINTERO OLIVARES (Director), *Comentarios a la Parte Especial del Derecho penal*, Aranzadi 1999, p. 521). También CHOCLAN MONTALVO, J.A., "Estafa por computación y criminalidad económica vinculada a la informática", *Actualidad Penal,* 1997, p. 1079. Sin embargo la posición de este autor resulta más matizada en momentos posteriores. Entiende que la afinidad no es total con los elementos de la estafa pero que el legislador la considera una modalidad más de estafa por lo que resultan de aplicación la penalidad y agravaciones del tipo básico de la estafa. *El delito de estafa*, Bosch, 2000, p. 297.

63 BAJO FERNÁNDEZ (Director), *Compendio de Derecho Penal (Parte Especial), volumen II*, Ceura, Madrid, 1998, p. 454).

64 Argumento que recuerda las viejas disquisiciones sobre el antiguo artículo 14 que comenzaba "Se consideran autores…" y que se remonta al menos a PACHECO. Cfr. CÓRDOBA/RODRÍGUEZ MOURULLO, *Comentarios al Código penal, T.I*, Barcelona, 1976, p. 801.

En primer lugar se sitúa el elemento que más caracteriza esta nueva modalidad: la manipulación informática. Manipulación informática o artificio semejante, que equivale al *engaño bastante* y el *error* al que debe conducir al sujeto pasivo o tercero. Puede entenderse también que el error de la estafa genérica se ve sustituido en la fórmula legal por la falta de consentimiento, según señala PÉREZ MANZANO.[65]

La redacción legal se refiere al logro mediante la manipulación informática una transferencia no consentida de algún tipo de activo patrimonial. Transferencia de cualquier activo patrimonial, en el sentido de cambio fáctico de adscripción del elemento patrimonial, como transmisión de bienes o servicios que tienen valoración económica.[66] Pese a esta visión tan amplia, que abarca no sólo la transmisión de bienes sino también prestación de servicios –como sucede en el acto de disposición patrimonial de la estafa genérica–, sin embargo, la s. AP de Madrid de 21-4-99[67] entiende que pasar con el cupón de abono del que no se es titular para franquear el torniquete de entrada a un transporte público no supone la existencia de transferencia de activo patrimonial alguno (tampoco manipulación informática).

Parece que la referencia legal a los activos patrimoniales tiene como clara finalidad justamente comprender como objeto de la acción valores patrimoniales sin correspondencia con un objeto mate-

---

65 BAJO FERNÁNDEZ (Director), *Compendio de Derecho Penal (Parte Especial), volumen II*, Ceura, Madrid, 1998, p. 455.

66 PÉREZ MANZANO, M. en BAJO FERNÁNDEZ (Director), *Compendio de Derecho Penal (Parte Especial), volumen II*, Ceura, Madrid, 1998, pp. 456-7.

67 (A. 2047). Acordando el Tribunal la absolución. Realmemte esta sentencia introduce no pocos elementos de debate. No está tan claro que el comportamiento no implique la transferencia de un activo patrimonial en el sentido señalado, que incluye la prestación de servicios. La negación de la manipulación informática también resulta dudosa, pues no queda determinado en la descripción de hechos probados el modo de funcionamiento del torniquete. En todo caso la solución de no condenar deja pendiente la posible aplicación de la estafa propia, pues lo normal en este caso es la existencia de una relación personal más o menos inmediata, y los presupuestos de hecho del caso no contradicen la doctrina que permitía incluir los supuestos de polizonaje, salvo que llevara a cabo una conducta puramente pasiva –y por tanto sí crear error en otro–, lo que realmente no puede entenderse para este hecho. Críticamente frente a la mencionada sentencia CHOCLAN MONTALVO, J.A., *El delito de estafa*, Bosch 2000, p. 304.

rial (dinero contable o escritural),[68] evitando lagunas de punibilidad en relación a los modernos tipos de operaciones patrimoniales.

La transferencia lograda a través de la manipulación informática finalmente va a provocar el perjuicio patrimonial para el tercero, como elemento requerido en todos los supuestos de estafa. Este también debe concebirse en los mismos términos que en el ámbito de la estafa genérica, pues no existe razón que oponer a ello, en el sentido de resultado final de desbalance patrimonial, creándose con el comportamiento fraudulento un déficit patrimonial para el titular de los bienes comparando el estado del mismo antes y después de los hechos. Igualmente a la estafa del número primero del art. 248 el autor debe obrar guiado por el ánimo de lucro, como elemento subjetivo que completa desde la perspectiva del autor el conjunto de rasgos objetivos del hecho punible.

IV. LA MANIPULACIÓN INFORMÁTICA Y OTROS ASPECTOS DE LA REGULACIÓN

El elemento que por tanto presenta mayor novedad e interés es el de la manipulación informática, mediante el que se logra la transferencia patrimonial no consentida, de forma que se hace necesario abordar el contenido de este requisito.

La manipulación a que hace referencia el precepto parece que implica la actuación del sujeto activo sobre un sistema informático de manera que este altere, de modos muy diversos, el resultado a que habría de conducir el normal procesamiento automatizado de datos. Manipulación consiste, según ROMEO,[69] en la incorrecta modificación del resultado de un procesamiento automatizado en cualquiera de las fases de procesamiento o tratamiento informático con ánimo de lucro y perjuicio de tercero.

---

68 Así CHOCLAN MONTALVO, J.A., "Estafa por computación y criminalidad económica vinculada a la informática", *Actualidad Penal,* 1997, p. 1083.

69 ROMEO CASABONA, C.M. *Poder informático y seguridad jurídica*, Madrid 1987, p. 47. CHOCLAN MONTALVO, J.A., *El delito de estafa*, Bosch, 2000, pp. 278-9. SCHMID, N. *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich, 1994 p. 226.

Se puede entender de otra manera tal manipulación como alteración del *software*, tal como lo hace PÉREZ MANZANO.[70] Esto, si lo entendemos de manera estricta, tiene un efecto muy restrictivo a la hora de señalar las conductas abarcadas, pues solamente se incluiría la manipulación del programa y no otras, generalmente aceptadas, que supongan la alteración de los datos sobre los que opera el sistema e incluso sobre elementos materiales del mismo. Realmente las consecuencias posibles no se llevan hasta el extremo, pues la propia autora no utiliza un concepto estricto de manipulación del *software*, como se evidencia al aceptar la anterior definición de manipulación informática de ROMEO que incluye la alteración de datos al introducirlos o los ya incluidos.

La referencia legislativa a la conducta punible termina con una cláusula general que se refiere a cualquier otro "Artificio semejante", para evitar algunos problemas de aplicación de esta modalidad delictiva en algunos casos en los que no quepa hablar en sentido estricto de manipulación informática pero esté muy próxima a la misma e incluso para permitir una rápida adaptación de la norma a las nuevas realidades que en el campo de las nuevas tecnologías se suceden a gran velocidad.

Ahora bien, para que esa cláusula general no pierda sentido y se convierta en una fórmula vacía en la que quepa cualquier contenido, y por tanto contraria al principio de legalidad, es necesario exigir una relación de semejanza con la manipulación informática. Así ha sucedido que la jurisprudencia ha extendido esta cláusula residual a supuestos de dudoso encaje, como el de la sentencia de la AP Lugo de 9-7-98,[71] en la que ciertos individuos se servían de dos monedas de quinientas pesetas a las que tenían adheridas un hilo de seda y que introducían en máquinas tragaperras en situación de juego, devolviendo la cantidad correspondiente al cambio de ese dinero.

---

70 En BAJO FERNÁNDEZ (Director), *Compendio de Derecho Penal (Parte Especial), volumen II*, Ceura, Madrid, 1998, p. 455.

71 (A. 3839). Señala la sentencia que "esta legislación viene a penalizar como estafa, expresamente, lo que hasta entonces la Jurisprudencia había dicho que no se podía castigar como tal" (en referencia a "artificio semejante").

Sin embargo la ya mencionada s. de la AP de Madrid de 21-4-99,[72] que entiende que pasar con el cupón de abono del que no se es titular para franquear el torniquete de entrada a un transporte público no supone la existencia de manipulación informática, aparte de otros problemas ya señalados, no contempla la posibilidad de acudir a este inciso incluyendo el paso fraudulento del torniquete entre los artificios semejantes, lo que no podría excluirse fácilmente.

Respecto a este punto resulta interesante y explicativo de lo que en última instancia parece una mala comprensión de este tipo de supuestos, las aclaraciones de CHOCLAN MONTALVO.[73] Señala este autor cómo la referencia al "artificio semejante" tiene su antecedente en el informe del Consejo General del Poder Judicial sobre el Anteproyecto de Código penal de 1994, con el objeto de poder castigar también las manipulaciones en máquinas automáticas que proporcionan servicios o mercancías sin que la manipulación sea propiamente informática. Pero naturalmente sucede que, como indica el autor, la obtención fraudulenta de prestaciones de un aparato automático (bebidas, combustible, billetes de transporte público, espectáculos, cabina telefónica, etc.), nada tiene de semejante a la manipulación en un sistema informático.

La manipulación puede producirse de cualquier forma, en el mismo programa o en cualquier momento del procesamiento o tratamiento automatizado de datos, y también desde cualquier lugar. Desde estos distintos puntos de vista se efectúan clasificaciones sobre las diversas manipulaciones posibles.[74] En este sentido cabe clasificar los distintos tipos de manipulaciones según puntos de vista distintos que nos facilitan la imagen global de las posibilidades plurales de realizar el comportamiento.

---

72 (A. 2047). Ya hemos indicado cómo el Tribunal acuerda la absolución y cómo la negación de la manipulación informática también resulta dudosa.

73 *El delito de estafa*, Bosch, 2000, pp. 302 y ss.

74 ROMEO CASABONA, C.M., *Poder informático y seguridad jurídica*, Madrid, 1987, pp. 47 ss. CORCOY, M./JOSHI, U. "Delitos contra el patrimonio cometidos por medios informáticos". *Revista Jurídica de Cataluña* 3 (1988), pp. 135 y ss. También PICA, G. *Diritto penale delle tecnologie informatiche*. Utet, 1999, pp. 145 y ss.

Respecto al momento de la manipulación pueden señalarse las alternativas en cuanto a este enfoque temporal de la actuación sobre el sistema informático. Cabe hablar en primer lugar de manipulación previa (en la fase de *input*), cuando se actúa en los datos sobre los que opera el programa. Y esta manipulación de carácter previo puede ser en su ejecución práctica tanto activa, en sentido estricto, como omisiva. Por acción, modificando datos reales o añadiendo otros ficticios. Caso de la s. de la AP de Granada de 23-3-99[75] en el que el empleado del banco mediante apuntes informáticos a través del ordenador detrae dinero de la caja del banco (hasta 18.026.834 ptas.) ingresándolo en cuentas de su titularidad.

También la s. TS 30-10-98[76] refleja un caso en el que empleados del INEM introdujeron datos falsos en el sistema informático del mismo haciendo acreedores de prestaciones del Instituto a personas que no reunían los requisitos y con quienes se repartían los ingresos, aun cuando este supuesto concreto el Tribunal se aparta del delito de estafa por razones distintas a las relativas al problema de la manipulación. Por omisión, en el registro de datos, no incorporando al procesamiento de datos los que correspondían al tratamiento llevado a cabo, y de esta forma alterando el resultado ordinario al que debía conducir el procesamiento de haberse llevado a cabo correctamente.

En la manipulación del programa se modifican las instrucciones del programa, alterando o eliminando algunos pasos o introduciendo partes nuevas en el mismo. Se incluirían así la llamada técnica del salami (*salami technique*), en la que el autor actúa redondeando céntimos por defecto en determinadas y múltiples opera-

75 (A. 1382). No cabe la apropiación indebida pues no siendo apoderado no ha tenido el dinero en administración. Hecho enjuiciado en la AP de Granada e igualmente consistente en la realización de apuntes informáticos irregulares, como el de años atrás, en una oficina del Banco Central-Hispano (con independencia de las fusiones ocurridas en el transcurso de estos años).

76 (A. 8566). En realidad la sentencia condena por delito de Malversación de Caudales, dada la condición funcionarial de los autores, pues entiende que la introducción de datos en el sistema informático no puede ser reputado como engaño toda vez que siendo el INEM una persona jurídica y no física no es susceptible de padecerlo.

ciones bancarias, que en su conjunto suponen cantidades importantes desviadas hacia cuentas propias. También se presenta en este ámbito la técnica conocida como el Caballo de Troya (*Troyan horse*),[77] mediante la que se introducen clandestinamente instrucciones en un programa ya activo que permite obtener determinados resultados no previstos en la configuración inicial del mismo. Con cualquiera de estas manipulaciones en el programa se puede lograr resultados distintos y no previstos en la programación originaria y que puede afectar a cualquier ámbito con trascendencia patrimonial, como por ejemplo, pagos de servicios, prestaciones o bienes inexistentes.

También cabe hablar de manipulaciones posteriores, o en la salida de datos ("*output*"), que generan directamente una alteración en el reflejo exterior del resultado del procesamiento automatizado de datos. Como ya se ha señalado en todas las manipulaciones finalmente se producirá una alteración del resultado del procesamiento de datos, pero en este caso la actuación permite la alteración inmediata del resultado, que por tanto ya no es efecto de actuaciones previas en otros momentos del procesamiento (en los datos, en el programa). Como tal manipulación en el resultado, la misma puede llevarse a cabo de distintas maneras: en el reflejo último en la visualización por pantalla, en el papel escrito mediante la impresora o en el registro en banda magnética cuando van a ser transmitidos a otros ordenadores.

Pero en todo caso sólo deben resultar asimilables las manipulaciones producidas en el ámbito de un procesamiento automatizado de datos, con lo que resultan excluidas las que se produzcan antes de la fase de entrada de los datos o después de la salida de los mismos.[78]

En cuanto al lugar desde el que se lleva a cabo la manipulación, como otra forma de conseguir la misma, pueden distinguirse diversas situaciones. En primer lugar la manipulación a distancia o exte-

---

77 Ambos ejemplos en CHOCLAN MONTALVO, J.A., "Estafa por computación y criminalidad económica vinculada a la informática", *Actualidad Penal* 1997, p. 1082.

78 En este sentido SCHMID, N., *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich, 1994, p.227.

rior, que a su vez puede entenderse de dos maneras. En relación al sujeto infractor, se puede hablar de manipulación exterior cuando el mismo es ajeno a la persona o institución de la que depende el sistema informático y por lo tanto cualquier acceso resulta ilegítimo.

En relación al lugar desde el que se efectúa también cabe referirnos a manipulación a distancia o exterior, pero ahora, por tanto, desde un punto de vista distinto. A través de la telemática (ordenador comunicado con otras terminales por línea telefónica mediante un modem) es posible el acceso al ordenador a distancia sin necesidad de presencia física. Cuando el sistema es accesible por terceros y éstos lo manipulan (caso de utilización de Internet o autopistas de la información para realizar algún tipo de operación comercial con manipulación informática). Media, entonces, distancia espacial entre el equipo informático en el que opera el sujeto activo y aquél en el que se producen los efectos.[79]

Respecto a la manipulación interna al sistema informático de que se trate, también cabe entenderla relacionada con el autor o con el lugar de realización del hecho. Con relación al sujeto: Cuando quien realiza la manipulación es una persona que está autorizada a acceder al sistema y operar con el mismo.[80] En principio los hechos anteriores es posible realizarlos mediante el acceso físico y directo al ordenador por quienes puedan legítimamente hacer uso del mismo. Por ejemplo un apoderado o empleado de una entidad financiera o de una empresa con el sistema informático propio. En relación al lugar se entenderá por manipulación interna la que se lleva a cabo con acceso físico al sistema informático en el que se encuentran los elementos objeto de manipulación.

En todo caso, como señala SCHMID,[81] la manipulación informática no reclama la producción de una auténtica "información equi-

---

79 PÉREZ MANZANO, M. en BAJO FERNÁNDEZ (Director), *Compendio de Derecho Penal (Parte Especial), volumen II*, Ceura, Madrid, 1998, p. 455.

80 Lo que representa particulares problemas. Véase SCHMID, N. *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich, 1994, pp. 240 y ss. Particulares problemas en la doctrina italiana respecto a los operadores de sistemas informáticos en PICA, G. *Diritto penale delle tecnologie informatiche*. Utet 1999, pp. 146-7.

81 *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich, 1994, p. 244.

vocada" del tratamiento de datos, en el sentido de la producción de un error propio del delito de estafa, pues el tratamiento de datos no puede calificarse como falso o verdadero.

La manipulación informática desde el punto de vista del contenido se manifiesta en esa transferencia no consentida de activos patrimoniales de la que habla el tipo penal del art. 248 en su número segundo. Aparece así la transferencia de activos patrimoniales como correlato del acto de disposición patrimonial en la estructura típica de la estafa común.[82] Se trata de una transferencia patrimonial meramente contable, como pura anotación (que puede concretarse de las formas más variadas: derecho de crédito, prestación o servicios, ingresos ficticios en cuentas corrientes, abono de salarios no debidos, órdenes de pago falsas, etc.).

Respecto a la prestación de servicios cabe plantearse el problema de si puede incluirse entre las transferencias no consentidas de activos patrimoniales.[83] Incluso en el caso español puede que este supuesto aparezca más dudoso puesto que la fórmula legal no parece que incluya actividades humanas, aun siendo económicamente evaluables, sino directa y exclusivamente elementos patrimoniales concretos.

Naturalmente debe tener una correspondencia en la realidad, de forma que suponga un incremento patrimonial del sujeto activo. Si no se llegara a reflejar de modo efectivo en el patrimonio del autor y sólo estuviéramos ante una mera anotación contable, el hecho punible no se ha consumado y podría castigarse únicamente como tentativa de estafa electrónica.[84]

Para ello no es óbice que el autor no llegue materialmente a recibir nada o no reciba anotación en su propio patrimonio, como

---

82 En este sentido SCHMID, N., *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich, 1994, p. 245.

83 Este aspecto se trata con mayor detenimiento en SCHMID, N. *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich, 1994, p. 247.

84 También en la legislación italiana requiere la consumación, la realización del enriquecimiento injusto. PICA, G. *Diritto penale delle tecnologie informatiche*. Utet, 1999, pp. 148 y ss.

cuando lo que hace es realizar una anotación contable con la que salda una deuda, de forma que en este caso también recibe un beneficio patrimonial y causa el perjuicio correspondiente.

Aun cuando de hecho la trascendencia económica del hecho suele adoptar una doble consecuencia: lesión patrimonial para la víctima y enriquecimiento para el autor, sin embargo, la redacción del tipo únicamente se refiere al aspecto de perjuicio para el sujeto pasivo. Como sucede en el tipo básico de la estafa del número 1 del art. 248 la fórmula legal requiere que se actúe "en perjuicio de tercero".[85] Lo cual a su vez puede dar lugar a la duda de si se tipifica una lesión efectiva del patrimonio o bastaría, como se plantea en otras legislaciones, con un relevante peligro para el patrimonio para fundamentar este elemento delictivo.[86] En el primer caso el menoscabo real del patrimonio debe computarse de acuerdo al concepto económico-jurídico de patrimonio.[87]

El déficit patrimonial debe proceder inmediatamente de la manipulación informática previa, lo que puede excluirse si se precisan otros pasos intermedios para conseguir el efecto final de la disposición patrimonial, como en el caso de la disposición patrimonial por decisión humana después de realizada la manipulación informática.[88] Esta inmediatez, sin embargo, puede relativizarse. No se excluye tal relación de inmediación si cabe considerar la manipulación una parte del proceso total de tratamiento automatizado de datos, de forma que es preciso completar el procesamiento para que se produzca la transferencia y como consecuencia de la misma el perjuicio patrimonial.

Cabe plantearse en relación a esta manipulación informática como elemento del tipo del art. 248.2, si la misma admite no sólo

---

85 En realidad el art. 248.1 exige que el autor obre "en perjuicio propio o ajeno", en el sentido de admitir que el resultado lesivo lo reciba el disponente u otra persona.

86 Véase SCHMID, N., *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich, 1994, p. 255.

87 SCHMID, N., *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich, 1994, p. 245.

88 SCHMID, N., *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich, 1994, pp. 248-9.

los supuestos de comisión activa en sentido estricto, sino además supuestos omisivos, es decir, realización de la manipulación mediante un dejar de hacer. Es cierto, como señala VALLE MUÑIZ[89] que "Las dificultades generales con que la doctrina admite en la estafa la comisión por omisión (tan sólo cuando la conducta omisiva puede ser reconducida a un acto concluyente), se ven acrecentadas en el fraude informático por la referencia típica a manipulaciones informáticas.

Siendo cierto esto, también lo es que en ocasiones muchos casos que aparecen inicialmente como omisivos, y que por ello resulta dudosa su admisión, sin embargo son realmente comportamientos activos en sentido estricto. Por otra parte, si admitimos como manipulación, como se hace muy habitualmente, el supuesto de no inclusión de los datos reales que deberían ser objeto de procesamiento (en el ámbito de lo que hemos llamado manipulación previa), estamos ya abarcando la omisión. Para rechazar estos casos omisivos habríamos de adoptar un concepto muy restrictivo de manipulación informática que generalmente no se toma en consideración. En otras legislaciones sin embargo es clara la admisión de conductas omisivas. En el caso Suizo la regulación prevé expresamente como conducta típica el supuesto de ocultación de una disposición patrimonial ya realizada que sirva para generar el perjuicio patrimonial correspondiente.[90]

V. EL ABUSO DE CRÉDITO O DE MEDIOS DE PAGO MEDIANTE MANIPULACIÓN INFORMÁTICA

La estafa mediante manipulación informática afecta especialmente a los modernos medios de pago. Los medios de pago que puedan hacer referencia a un supuesto de estafa informática pare-

89 QUINTERO OLIVARES (Director), *Comentarios a la Parte Especial*, Aranzadi, 1999, p. 525.

90 SCHMID, N. *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich, 1994, pp. 252 y ss. Es dudoso si estamos ante un supuesto omisivo realmente. Es posible entender que la manipulación informática con la que se oculta la disposición patrimonial ya realizada constituye el hacer activo de la conducta típica.

cen representar una transferencia electrónica de fondos, la cual se puede realizar fundamentalmente de tres formas: cajeros automáticos, terminales en puntos de venta mediante tarjetas de pago, y el llamado Banco en casa.[91]

Ahora bien, de acuerdo a los presupuestos generales que se han venido estableciendo en este trabajo, deben estar presentes siempre dos requisitos para que en el ámbito de la transferencia electrónica de fondos podamos hablar de estafa informática:

Por una parte una auténtica manipulación de un sistema informático, en el sentido de alteración de lo que hubiera sido el normal desarrollo y resultado de un procesamiento automatizado de datos sin algún tipo de intervención fraudulenta. Es decir que no basta con que esté presente sin más una operación informatizada sino que en alguna medida se manipule la misma, de cualquiera de las formas que ya hemos señalado.

Por eso resulta incorrecto calificar como estafa informática la utilización de tarjetas de crédito en comercios por alguien que no es su titular, como si hizo la s. AP Las Palmas de 19-10-98,[92] al entender que en aquellos casos en los que se asegura la operación mediante firma electrónica el engaño se sofistica. Pero en realidad en todos los casos estaban personalmente presentes sujeto activo y víctima.

Pero además, esta manipulación informática debe producirse en condiciones determinadas, de acuerdo a la concepción general del supuesto y su relación con la estafa genérica. Así debe producirse una manipulación informática sobre sistemas que operen con autonomía, sin intervención de personas físicas. De forma que si pese a emplearse alguna modalidad de manipulación informática,

---

91 DEL PESO NAVARRO, E. "El pago mediante medios electrónicos". *Actualidad Informática, Aranzadi* 5 (1992), p. 2.

92 (A. 4072). Empleada del hotel que mediante simulacros de incendio consigue despistar al personal del hotel para acceder a las habitaciones y sustraer objetos y tarjetas. En lo referente a la utilización abusiva de tarjetas de crédito en un restaurante y otros comercios, la autora resultó condenada por falsedad en documento mercantil en concurso con el delito de estafa.

la disposición patrimonial se produce finalmente a consecuencia de la falsa representación mental de alguna persona –con base en la anterior manipulación informática– estaríamos ante el engaño propio del tipo básico de la estafa.

En el sentido indicado GUTIÉRREZ FRANCÉS[93] distingue claramente ambos supuestos en los que manipulación e intervención de personas puedan simultanearse o no. Por esta razón era ya posible admitir la estafa antes del nuevo Código penal de 1995, "si el ordenador no es más que un medio auxiliar o de ayuda a la toma de decisiones, que acaba adoptando efectivamente una persona, que podría decirse había sido efectivamente engañada".[94]

También ROMEO[95] señala que para que la manipulación informática fuera admisible como engaño "es preciso que aquella sea captada, percibida, física o visualmente por una persona, una captación del contenido de los datos manipulados, de manera que como consecuencia de la misma se modifique su representación intelectual sobre un suceso, hecho o acontecimiento...". Sólo en los casos en que con carácter previo a la transferencia patrimonial se produce la concurrencia de una persona humana encargada de verificar la realidad de los datos informáticos, podrá considerarse producida la estafa, si el ordenador ha sido medio para el engaño.[96]

Por exigirse estos requisitos deberán tratarse de la siguiente manera los siguientes casos: Para los pagos mediante tarjetas de crédito por su titular con abuso del mismo en establecimientos comerciales es necesario hacer algunas consideraciones previas. Con anterioridad a la regulación actual se incluían en el ámbito de la estafa los supuestos de utilización por el titular de la tarjeta en cualquiera de estos tres supuestos: Sobrepasando el límite de crédito de la tarjeta, utilizando tarjeta caducada o cancelada o, final-

93 *Actualidad Informática Aranzadi 11* (1994), p. 11.

94 GONZÁLEZ RUS, J.J. *Curso de Derecho penal español, Parte Especial I*, Marcial Pons, Madrid, 1996, p. 687.

95 *Poder informático y seguridad jurídica*, Fundesco 1987, p. 60.

96 CHOCLAN MONTALVO, J.A., "Estafa por computación y criminalidad económica vinculada a la informática", *Actualidad Penal* 1997, p. 1078

mente, la concesión de tarjetas de crédito o de línea de crédito aportando datos falsos.

Se trata, por tanto, de supuestos que ya venían siendo incluidos en el ámbito de la estafa propia y que no podrán serlo en la estafa informática pues el proceso informático de pago se lleva a cabo sin manipulación alguna, sino que el engaño se realiza con la apariencia de crédito que en la relación personal entre cliente y comerciante se crea.

Otro ámbito diferenciado es el de **pago** por terceros no titulares de la tarjeta directamente en redes informáticas (Internet). En el ámbito de las redes informáticas pueden realizarse operaciones comerciales nacionales e internacionales, cuyo pago puede efectuarse mediante la aportación del número de tarjeta de crédito. De manera que obteniendo fraudulentamente el número de la tarjeta pueden realizarse operaciones comerciales usando fraudulentamente el número codificado de tarjetas ajenas.

En principio en estos casos concurre el engaño del tipo básico de la estafa (art. 248.9), pues no puede decirse que se produzca manipulación informática, sino el uso fraudulento de tarjeta ajena (el sistema informático funciona correctamente y los datos empleados son ciertos).

Podría ser otra la solución si se efectúa una manipulación informática *strictu sensu*: bien alterando el funcionamiento mismo del sistema informático, bien alterando los datos con que opera el sistema informático (introduciendo datos falsos u ocultando los verdaderos). En este caso, ya si concurre la estafa informática, pues aparece algún tipo de manipulación informática (art. 248.2). Además para este grupo de supuestos aparecerá el problema del posible concurso con el delito de falsedades.

También cabe considerar el empleo de tarjetas bancarias con banda magnética en los cajeros automáticos para disponer ilegítimamente de cantidades de dinero. En estos casos la disponibilidad se obtiene sin exigirse ningún tipo de manipulación, sino que, al contrario, el procesamiento automatizado de los datos funciona correctamente, lo que sucede es que quien emplea la tarjeta y obtiene el reintegro no es la persona autorizada. Como es sabido, las

tarjetas se consideran llaves falsas según lo previsto en el art. 239 CP y, por tanto, el supuesto debe ser tratado como robo con fuerza en las cosas. Aún así sería necesario realizar algunas consideraciones genéricas de acuerdo a los presupuestos del delito de robo con fuerza en las cosas, aunque no directamente dependientes del problema de la manipulación.[97]

En el sentido de excluir el delito de estafa y entender aplicable el robo para estos casos, se viene pronunciando la jurisprudencia de la Sala segunda del Tribunal Supremo desde comienzo de los años noventa. Así una última sentencia TS de 29-4-99[98] señala que constituye robo y no estafa (pese al criterio anterior de la AP de Valencia), aunque por mor del principio acusatorio no se pueda condenar por este delito. En este caso particular se plantea el problema del número secreto a la vista, es decir, con falta de diligencia por parte de su titular a la hora de ocultarlo, pero en todo caso no afecta al aspecto central de la manipulación. Igualmente s. TS 16-3-99[99] ofrece una amplia visión retrospectiva de la doctrina jurisprudencial.

Es posible, sin embargo efectuar todavía alguna matización. En los casos anteriores, si la obtención de dinero se realiza sobre la base de la alteración de los datos contenidos en la banda magnética de la tarjeta, cabe hablar de manipulación informática y con ello de estafa informática. En este sentido ya se pronunció ROMEO.[100]

---

97 Sobre esta materia MATA MARTÍN, R. M., *El delito de robo con fuerza en las cosas*, Tirant lo blanch, Valencia, 1995. Del mismo autor, "Los modernos sistemas de seguridad en el apoderamiento patrimonial", *Poder Judicial,* 49 (1998), pp. 346 y ss.

98 (A. 4127)

99 (A. 1442)

100 "Delitos cometidos con utilización de tarjeta de crédito, en especial en cajeros automáticos", *Poder Judicial*, número especial IX (1988), p. 128. En contra PÉREZ MANZANO, M. en BAJO FERNÁNDEZ (Director), *Compendio de Derecho Penal (Parte Especial), volumen II*, Ceura, Madrid, 1998, p. 455.

SECCIÓN SEGUNDA
Los daños informáticos

I. INTRODUCCIÓN

El sentido genérico del clásico delito de daños es la destrucción, inutilización, deterioro o menoscabo de una cosa. Con los avances en las tecnologías de la información se ha planteado el problema del encaje en esta figura delictiva de una serie de comportamientos recaídos sobre elementos lógicos de los sistemas informáticos (archivos, programas, etc.), produciendo la destrucción o deterioro de los mismos. Es lo que generalmente desde un punto de vista criminológico se denomina sabotaje informático.[101]

Estos comportamientos que atacan los elementos lógicos de sistemas informáticos pueden llevarse a cabo a través de procedimientos de naturaleza informática (mediante programas de destrucción progresiva, las llamadas rutinas cancerígenas, virus que dejen inoperante un programa o destruyen datos almacenados o bien mediante otras formas como las "bombas lógicas"o "Caballo de Troya").[102] Pero también es posible conseguir el mismo efecto de destrucción de archivos o programas mediante la actuación sobre los soportes físicos, al golpear o romper el disquette o el ordenador mismo donde se contienen datos, programas o documentos o insertar o verter múltiples materiales o sustancias sobre los elementos del sistema informático.[103]

La nueva regulación del Código penal de 1995 prevé expresamente el supuesto de daños sobre el *software* como tipo cualificado

---

101 También desde el punto de vista legal el & 303b del StGB alemán denomina "Computersabotage" la conducta punible de daños informáticos.

102 CORCOY BIDASOLO, M. expone detalladamente el conjunto de modalidades de destrucción lógica en "Protección penal del sabotaje informático. Especial consideración de los delitos de daños". *La Ley,* vol. 1, nº 2400 (1990), pp. 1002 y ss.

103 Sobre la amplia gama de posibilidades véase CORCOY BIDASOLO, M., "Protección penal del sabotaje informático. Especial consideración de los delitos de daños". *La Ley,* vol. 1, nº 2400 (1990), p. 1002.

en el marco de la regulación del genérico delito de daños, que se contempla legalmente como delito patrimonial, lo que a su vez sucede generalmente también en el Derecho comparado.[104]

II. LA SITUACIÓN LEGISLATIVA ANTERIOR

La regulación del delito de daños en el Código penal derogado respondía al contexto histórico del siglo pasado, en el que nada hacía necesario abordar la solución legislativa a supuestos semejantes a los actuales daños informáticos. De ahí que el sentido tradicional del delito de daños se entendiera pacíficamente referido a cosas corporales, en cuanto al objeto material sobre el que debía recaer el comportamiento destructivo propio de tal hecho punible.

Ya con la regulación anterior no dejaron de suscitarse problemas respecto al modo de concebir el delito de daños. Estos mismos debates se trasladarían de inmediato tras su aparición a los supuestos en los que se ven implicados los componentes de los sistemas informáticos. De manera que durante la vigencia del anterior Código se debatió un primer problema sobre las cualidades o naturaleza que debía reunir el objeto material de este delito. Otro aspecto también debatido sería el del tipo o modo de afectación que debía producir el comportamiento sobre el objeto material para que resultara abarcado por el tipo y, por tanto, punible. Se trata de dos aspectos íntimamente relacionados pero que a los efectos de su estudio pueden y deben separarse.

En cuanto al primero de los temas indicados trataba de determinar el objeto material idóneo en el tipo penal del delito de daños. Aquí subyace una concepción naturalística de los daños en atención a la exigencia de lesión de la sustancia, que conducía a la necesidad de una modificación constatable en la corporeidad de la cosa de modo que resulten perceptibles directamente los efectos en

104 Véase SCHMID, N. *Computer- sowie Chech- und Kreditkarten-Kriminalität*, Zürich, 1994, pp. 184 y ss. PICA, G. *Diritto penale delle Technologie Informatiche*, Utet, Torino, 1999, pp. 87 y ss.

misma materialidad o corporeidad de la cosa.[105] Al consistir en un soporte lógico (no físico, sino incorporal), el objeto de los daños informáticos, parecía contradecir los presupuestos generales del delito de daños, que exigía una cosa ajena, mueble o inmueble, y por tanto corpórea.[106] Los datos o programas informáticos, producto de impulsos eléctricos recogidos en un soporte material, se entendía que no podía asimilarse a cosa corporal tal y como se entendía tradicionalmente el delito de daños.

CORCOY[107] intentaba, para el caso del sabotaje informático, compatibilizar el concepto de daños como lesión de la sustancia con la incidencia de la acción sobre el soporte de los elementos lógicos. Así afirmaba que se presenta una transformación de la sustancia cuando la cosa no funciona correctamente o se disminuyen sus posibilidades de aplicación o de eficacia, pero siempre en relación al soporte de los elementos lógicos, con lo que se entiende que con los "mismos se altera la sustancia del portador de los datos". Con ello el objeto material de referencia no son los propios elementos lógicos sino los soportes de los mismos, por lo que se ve obligada a excluir los casos de ataque a los elementos lógicos a través de las líneas de telecomunicación sin incidencia directa en soporte material alguno.[108] Pero es que, en realidad, como la propia autora reconoce, pese al pretendido respeto al concepto de daños como lesión de la sustancia, se ha producido un deslizamiento de la noción naturalística a otra normativa de daños, pues "las propiedades esenciales de una cosa sólo pueden ser comprendidas bajo el aspecto de su funcionalidad".

---

105 Sobre el concepto naturalístico de daños y el resto de nociones de daños en sentido penal, véase SUAY HERNÁNDEZ, C., *Los elementos básicos de los delitos y faltas de daños*, PPU, 1991, pp. 52 y ss.

106 SCHMID, N. en *Computer- sowie Chech- und Kreditkarten-Kriminalität*, Zürich 1994, p. 182, recoge también el paso de a consideración del objeto material en ambos sentidos en el ámbito de los daños.

107 "Protección penal del sabotaje informático. Especial consideración de los delitos de daños". *La Ley,* vol. 1, nº 2400 (1990), p. 1013.

108 "Protección penal del sabotaje informático. Especial consideración de los delitos de daños". *La Ley,* vol. 1, nº 2400 (1990), pp. 1005 y 1013-4.

En estas consideraciones parece pesar todavía la noción romana de cosa corporal ceñida a las entidades directamente perceptibles mediante el tacto (*quae tangi possunt*) que naturalmente se circunscribía a la realidad a la que los conocimientos del momento histórico permitían acceder.[109] Otro tipo de argumentaciones puramente gramaticales para fundamentar la corporeidad de la cosa objeto del delito de daños carecen de fuerza suficiente.[110]

Puede resultar en definitiva que el sentido de la corporalidad como presupuesto del delito de daños, según el modo de comprensión de la realidad física de tiempos históricos, hiciera referencia a la necesidad de la individualización física o material del objeto para poder determinar que la acción de daños recaía sobre el mismo. Esa corporeidad permitía en tiempos pasados individualizar los objetos de la realidad y señalar la incidencia de la acción delictiva sobre la cosa. Hoy los progresos científicos y técnicos nos permiten la individualización de entidades reales aunque no sean corpóreas en el sentido tradicional.[111]

Sin embargo la doctrina ya había señalado que el requisito de la materialidad poseía verdadero sentido en los delitos de apoderamiento, en los que la naturaleza de su dinámica comisiva precisa la aprehensión material de la cosa. Efectivamente la transferencia patrimonial en sentido fáctico que es propia de los delitos de apoderamiento está condicionada, por su misma noción plasmada en los tipos penales concretos, a un desplazamiento físico de la cosa, lo que a su vez reclama un objeto material. De manera diferenciada, en los daños, no resultaba necesario y bastaba con una interpretación acorde

109 Sobre ello ANDRÉS DOMÍNGUEZ, A.C. *El delito de daños: consideraciones jurídico-políticas y dogmáticas*. Universidad de Burgos, 1999, p. 112.

110 ANDRÉS DOMÍNGUEZ, A.C. *El delito de daños: consideraciones jurídico-políticas y dogmáticas*. Universidad de Burgos, 1999, p. 110, quien señala que el significado gramatical y los términos empleados en el Código exigen un quebranto material.

111 Indica PICA con carácter general que no hay que confundir la no perceptibilidad directa del nuevo fenómeno por parte del hombre con la falta de materialidad. Diritto penale delle *delle Technologie Informatiche*, Utet, Torino, 1999, p. 34.

al progreso tecnológico, que requiera fundamentalmente que se trate de un objeto de propiedad ajena evaluable económicamente.[112]

El segundo de los problemas señalados, añadido al que acabamos de ver, hacía referencia no tanto al objeto material o cualidades de éste, sino al efecto que sobre el mismo debía producir el comportamiento típico. En este ámbito se discutía si el efecto recibido por el objeto material debía menoscabar la esencia o sustancia misma (de acuerdo a la *Substanzwerttheorie*) o, bien, era suficiente un detrimento de la funcionalidad o valor de uso del mismo (*Gebrauchswerttheorie*).[113]

Los partidarios de exigir una lesión de la sustancia de la cosa imponían como requisito necesario que el comportamiento produjera algún tipo de menoscabo en la estructura material del objeto. Frente a ello, un sector de la doctrina venía a apoyar la no exigencia de lesión de la sustancia de la cosa en el delito de daños, bastando la lesión en la capacidad de uso de la cosa. Esta tesis venía reforzada por la referencia a la inutilización como uno de los casos expresamente previstos en la regulación.

III. LA REGULACIÓN DE LOS DAÑOS EN EL CP DE 1995

1. La previsión específica de daños informáticos. Los daños informáticos como supuesto agravado

En realidad con la tesis menos restrictiva de las señaladas anteriormente, ya durante la vigencia del anterior Código, podía entenderse abarcado por el delito de daños las conductas de deterioro o inutilización de programas y archivos informáticos. Pese a ello el legislador penal de 1995 junto al tipo básico de daños del art. 263, incluye, como supuesto agravado en el número segundo del art. 264

112 ROMEO CASBONA, C., *Poder informático y Seguridad Jurídica*, Fundesco, Madrid, p. 176.

113 Véase ROMEO CASBONA, C., *Poder informático y Seguridad Jurídica*, Fundesco, Madrid, p. 177

los daños informáticos, conforme al cual resulta punible la conducta de quien "por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

La virtualidad fundamental de esta regulación expresa de los daños informáticos consiste en despejar las incertidumbres que todavía pudieran permanecer sobre la aplicación de los daños al novedoso campo de la actividad informática. GONZÁLEZ RUS[114] señala así que la previsión legal resuelve las dudas sobre la adecuación de la regulación del comportamiento de daños en elementos informáticos. También QUINTERO[115] estima que la particularizada regulación responde al temor del legislador a que no se tuviera una completa protección frente a estas modalidades de no incluirse la misma.

Como se ha indicado, no sólo aparecen con la nueva regulación los daños en elementos lógicos de los sistemas informáticos, sino que, además, se presentan como un supuesto agravado frente al tipo básico de daños del art. 263. Efectivamente éste prevé una pena de multa de seis a veinticuatro meses, mientras que los daños informáticos del art. 264.2 recogen la pena de prisión de uno a tres años y multa de doce a veinticuatro meses. Se repite aquí la constante posición cualificada que el ordenamiento Jurídico atribuye en varios campos del mismo a los instrumentos lógico-informáticos. Protección intensificada que quizás responda a la significación social y al papel destacado que se entiende desempeñan en el actual desarrollo socioeconómico de las sociedades modernas. Con ello el legislador parece otorgar una mayor importancia a los daños sobre elementos lógicos de los sistemas informáticos, frente a cualquier otro tipo de daños sobre distintos objetos, incluidos los elementos materiales de los sistemas informáticos.[116]

---

114 "Protección penal de sistemas, elementos, datos y programas informáticos". *Revista Electrónica de Ciencia Penal y Criminología* 1 (1999), p. 5, en http://criminet.vrg.es/recpc/.

115 *Comentarios a la Parte Especial del Derecho Penal*, QUINTERO OLIVARES (Director), Aranzadi, 1999, p. 592

116 Sobre ello, véase GONZÁLEZ RUS, J.J., "Protección penal de sistemas, elementos, datos y programas informáticos". *Revista Electrónica de Ciencia Penal y Criminología* 1 (1999), p. 5

2. Daños en los elementos lógicos y en los elementos materiales de un sistema informático

Esto mismo nos permite plantear la relación entre los daños en los aspectos materiales de un sistema informático y los daños en sus componentes lógicos. Teniendo además en cuenta que, como ya se ha indicado, los daños en el *software* pueden realizarse no sólo a través de procedimientos estrictamente informáticos, sino como resultado de una actuación física sobre los elementos materiales.

La duda que se presenta es determinar si ambas modalidades de daños informáticos deben tener un mismo tratamiento o bien, aplicar el supuesto del art. 264.2 a los hechos de naturaleza puramente informática y, por otra parte, el tipo básico –con penalidad inferior, como se ha indicado– a los realizados mediante comportamientos físicos sobre los elementos materiales. Esta segunda opción no dejaría de representar una incongruencia, pues siendo el mismo el resultado delictivo la penalidad a imponer sería bien diversa.

Para evitar esta posible paradoja propone GONZÁLEZ RUS[117] la aplicación en ambos casos del tipo cualificado del art. 264.2. Siendo cierta esta posible incongruencia en la penalidad a imponer, sin embargo no parece acertada la determinación del tipo aplicable sobre la base de la comparación de las consecuencias a imponer a los autores.

Previamente, en el orden lógico del planteamiento metodológico, puede señalarse que en realidad el delito castiga la producción de un determinado resultado (destrucción, deterioro, alteración o inutilización) y no el empleo de ciertos medios en la ejecución de

117 p. 7. Por otra parte, MATELLANES estima no aplicable el tipo básico pues entiende que los desperfectos en los elementos materiales del sistema informático no alcanzarían las 50.000 que, como cuantía mínima, requiere en todo caso la regulación del mismo. Esta opción, además de apuntar una mera hipótesis –difícilmente generalizable– sobre la cuantía de los daños causados en los elementos materiales del sistema, no toma en cuenta que el tipo cualificado, como modificación agravada del tipo básico exige los mismos requisitos, además de los elementos propios que lo singularizan. "Algunas notas sobre las formas de delincuencia informática en el Código Penal". *Hacia un Derecho Penal sin fronteras* (DIEGO DÍAZ-SANTOS, Mª R/ SÁNCHEZ LÓPEZ, V., Coordinadoras), Colex 2000, p. 142.

tal resultado. Esto es tan notorio que el propio art. 264.2 señala que el mismo puede cometerse "por cualquier medio" o "de cualquier otro modo". De forma que si el delito representa la causación de un resultado, siendo el mismo en ambas modalidades, la forma de comisión no impone una diferencia en el concreto tipo a aplicar sino, al revés, resultando dañados los elementos lógicos –que es el elemento que singulariza el supuesto del art. 264.2– deben ser reconducidos ambos casos a la misma regulación.

3. Elementos típicos de los daños informáticos

El análisis de los distintos elementos del tipo constituye el siguiente paso en nuestro estudio. En este momento podemos hacer referencia a los distintos requisitos que forman el delito de daños informáticos. Nos vamos a referir aquí tanto al objeto material del delito, como a la misma conducta típica delictiva, cada uno de ellos en los distintos aspectos que resulten de interés.

a. En cuanto al objeto material puede decirse que es el componente delictivo que individualiza el supuesto. Frente a la referencia general a la propiedad ajena del tipo básico, el art. 264.2 se concentra específicamente en "datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".[118]

La referencia legal al objeto material que acabamos de recordar puede resultar en alguna medida reiterativa, quizás con la pretensión de evitar cualquier laguna legal no deseada. Todos los elementos mencionados, como elementos lógicos de un sistema informático para resultar funcionales e interpretados deben ser procesados en algún sistema de esa naturaleza. La referencia a datos, con independencia de su contenido particular, deben entenderse hecha a las unidades elementales procesadas por el sistema informático, y

118 En otras legislaciones, como la suiza, este objeto material posee en principio un carácter más restrictivo al hablarse únicamente de "datos ajenos", aunque en la práctica posea un mismo ámbito de aplicación. Véase SCHMID, N. *Computersowie Chech- und Kreditkarten-Kriminalität*, Zürich, 1994, pp. 188 y ss. GONZÁLEZ RUS, J.J., "Protección penal de sistemas, elementos, datos y programas informáticos". *Revista Electrónica de Ciencia Penal y Criminología 1 (1999),* p. 4.

de cuya combinación resulta la información contenida en el sistema.[119] Los programas están constituidos por "toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión o fijación" (art. 96.1 LPI). Documentos electrónicos serían aquellos en los que se recogen los resultados del procesamiento de datos obtenidos con las distintas aplicaciones.[120]

Todos estos elementos mencionados pertenecientes a un sistema informático en sus distintas parcelas o modalidades ("recogidos en redes, soportes o sistemas informáticos"). Se trata en definitiva de lo que desde la perspectiva informática se consideran los elementos lógicos de un sistema informático (*software*), que se contraponen a los elementos físicos o materiales (*hardware*) que requiere también un sistema informático. Con la incorporación de este particular elemento del delito ya no cabe duda que el delito de daños abarca también el comportamiento realizado sobre cosas incorporales y que es suficiente con algo que pueda ser objeto del derecho de propiedad y valorable económicamente.[121]

— El objeto material sobre el que recae la acción delictiva (datos, programas...) debe ser ajeno respecto quien realiza el comportamiento típico, como expresamente recogen tanto el tipo básico como el tipo cualificado de daños informáticos. Sustancialmente implica que el hecho no resulta delictivo desde la perspectiva de los daños cuando el fichero o programa sobre el que se actúa es pro-

---

119 En este sentido GONZÁLEZ RUS, J.J., "Protección penal de sistemas, elementos, datos y programas informáticos". *Revista Electrónica de Ciencia Penal y Criminología* 1 (1999), p. 4.

120 Así GONZÁLEZ RUS, J.J., "Protección penal de sistemas, elementos, datos y programas informáticos". *Revista Electrónica de Ciencia Penal y Criminología* 1 (1999), p. 4.

121 En ese sentido GONZÁLEZ RUS, J.J. "Protección penal de sistemas, elementos, datos y programas informáticos". *Revista Electrónica de Ciencia Penal y Criminología* 1 (1999), pp. 4 y ss. También GUTIÉRREZ FRANCÉS, Mª. L., "Delincuencia económica e informática en el nuevo Código penal". *Ámbito jurídico de las tecnologías de la información. Cuadernos de Derecho Judicial*. Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, p. 295.

pio, es decir, de titularidad del mismo autor de los hechos. Para dilucidar esta titularidad debemos acudir a la normativa civil de propiedad intelectual que determina justamente la atribución a una persona o personas de la capacidad jurídica de uso y disposición de tales elementos.

En relación a este elemento del delito pueden plantearse casos problemáticos como el que relata CORCOY.[122] Se trata de aquellas situaciones en las que el propietario del programa lo distribuye de tal manera que el mismo tiene prevista su inutilización o destrucción ante la realización por parte del titular del derecho de uso de alguna maniobra ilícita (copia no autorizada) o no dé el mantenimiento acordado. En estos casos no concurre la ajenidad reclamada por el tipo por lo que desde la óptica de los daños la conducta no resulta abarcada. En ocasiones se ha planteado acudir al delito de realización arbitraria del propio derecho, hoy en el art. 455 CP, pero tal posibilidad queda impedida desde el inicio pues tal delito requiere siempre el empleo por parte del sujeto activo de medios físicos (violencia, intimidación o fuerza en las cosas).

En vía penal la única opción es la apreciación, de concurrir en los datos, programas o documentos electrónicos una relevante utilidad social o cultural para la comunidad, del hecho punible que castiga la sustracción de cosa propia a su utilidad social o cultural (art. 289). En otro caso el hecho debe reconducirse a la vía civil en la que será necesario determinar los deberes y obligaciones de las partes, así como la eventual aplicación de la figura del abuso de derecho.

En el Derecho comparado de daños informáticos se observa la tendencia a especificar un concreto objeto material. Así en legislaciones como la suiza o italiana se incorporan previsiones específicas para el caso de los virus informáticos (*Computerviren*).[123] Estos virus se consideran microprogramas preparados para, en determi-

122 "Protección penal del sabotaje informático. Especial consideración de los delitos de daños". *La Ley,* vol. 1, nº 2400 (1990), p. 1015.

123 De este modo en el apartado segundo del & 144 StGB Suizo y el art. 615 quinto del CP italiano.

nadas condiciones, causar alteraciones bien en el funcionamiento, bien en determinados elementos del sistema informático. Como se ha dicho, no dejan de representar un particularizado objeto material que quizás por su mayor difusión y amplia repercusión en los medios de comunicación ha recibido una mayor atención. En todo caso la no mención expresa no quiere decir, naturalmente, que los supuestos cometidos mediante virus no estén previstos por la legislación española.

b. La conducta típica de los daños sobre elementos informáticos presenta numerosos aspectos de interés que van a ser expuestos a continuación.

— En primer lugar cabe señalar que no existe previsión legal en cuanto a los medios de ejecución del supuesto típico. Quiere esto decir que la concreta forma de realización del delito es indiferente, por cuanto lo relevante es la producción de la destrucción, alteración o inutilización de los datos, programas o documentos electrónicos. Los estudios criminológicos en este campo nos muestran la variedad de métodos empleados en este tipo de comportamientos. Así aparecen constantemente en esta clase de análisis de la realidad criminal y en los medios de comunicación la propagación de virus a través de las redes informáticas que pueden producir efectos perniciosos sobre un sinnúmero de terminales en todo el planeta.

Precisamente por la indeterminación típica en los medios de comisión del delito ya se ha mencionado que pueden reconducirse al mismo tanto los daños realizados mediante virus, bombas lógicas, caballo de Troya, etc., como los de destrucción o deterioro de datos o programas a través de comportamientos físicos sobre su soporte. Incluso se ha puesto acertadamente de relieve las dificultades e inconvenientes que introducen la tipificación de estos comportamientos mediante la fijación de unos precisos medios de ejecución a través de una técnica legislativa casuística.[124]

124 CORCOY BIDASOLO, M., expone detalladamente el conjunto de modalidades de destrucción lógica en "Protección penal del sabotaje informático. Especial consideración de los delitos de daños". *La Ley,* vol. 1, nº 2400 (1990), p. 1012.

La no determinación legislativa de los medios típicos de ejecución permite también plantear la duda sobre si estamos ante un supuesto activo en sentido estricto, o bien cabría admitir el sabotaje informático conseguido mediante omisión. Cabe descartar la punibilidad de hechos que representen una omisión pura o simple, en el sentido de un mero dejar de hacer, pues el tipo requiere como hemos visto la producción de un resultado y además no existe tipificación expresa del caso. Sin embargo es posible todavía plantear la hipotética sanción de conductas de comisión por omisión, en las que el autor se encuentra en una posición jurídica (posición de garante) que le obliga a actuar en defensa del bien jurídico protegido, siendo sin embargo que el mismo omite la conducta debida dirigida a salvaguardar tal interés.

Con el Código Penal de 1995 los requisitos generales para la punibilidad de la comisión por omisión se recogen en el art. 11 del CP. A este respecto CORCOY[125] ha señalado, ya antes del vigente Código Penal, que "son posibles también realizaciones típicas a través de comportamientos omisivos, cuando un operador, como garante, no impide alguna de las destrucciones previstas, cuando tiene conocimiento de ello y puede hacerlo".

— Respecto a la acción típicamente constitutiva de los daños informáticos, la regulación legal del art. 264.2 CP incorpora las mismas conductas propias de los daños genéricos. Así se castiga "al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas…" De manera que en cuanto a la conducta desenvuelta por el autor no representa este nuevo supuesto ninguna especialidad.

Otras conductas punibles de daños informáticos previstas en algunas legislaciones o admitidas por la doctrina resultan difícilmente asumibles para el caso español. PICA,[126] en el ámbito italiano, entiende que cualquier modificación que comporte la alteración de la secuencia y registro de los datos constituye delito de daños, al afec-

125 "Protección penal del sabotaje informático. Especial consideración de los delitos de daños". *La Ley,* vol. 1, nº 2400 (1990), p. 1011.

126 *Diritto penale delle Technologie Informatiche*, Utet, Torino, 1999, pp.92 y ss.

tar a la función atribuida a su titular. De este modo no encuentra reparo en castigar como daños la conducta de incluir nuevos contenidos en un documento electrónico junto a los ya existentes, como alteración del original, que a su juicio supone un hecho penalmente relevante respecto a la regulación del art. 635-bis CP italiano.

En el Derecho comparado se observan algunas particularidades en este campo de las conductas constitutivas de los daños, especialmente en lo relativo a las especificaciones legislativas sobre virus informáticos. Así para este caso de los virus suelen recogerse conductas punibles tanto en relación al estadio o desarrollo del hecho como respecto al tipo de efecto producido. Como conductas que especifican los distintos momentos del desarrollo de los virus se incriminan tanto su fabricación, puesta en circulación, propagación, introducción de los mismos, hacerlos accesibles de cualquier forma e, incluso, el mero dar indicaciones para su fabricación.[127] Según el tipo o clase de efectos o consecuencias se pueden encontrar previsiones incriminando tanto el daño efectivo como la alteración en el uso o funcionamiento del sistema.

Algunas de estas conductas encuentran difícil acomodo en nuestro sistema jurídico-penal. Por una parte la estructura del delito de daños, que se mantiene en el tipo agravado del art. 264.2 de daños informáticos, un resultado de alteración efectiva de datos o programas incompatible con ciertas conductas del derecho comparado que constituyen auténticos delitos de peligro abstracto (fabricación, establecer instrucciones para su fabricación). Igualmente el tipo de lesión del delito de daños requiere una alteración permanente de datos o programas, cosa que no sucede necesariamente en las meras alteraciones en el funcionamiento o uso del sistema informático. Problemático resulta si este tipo de alteraciones en el uso del sistema puede entenderse incluida en el ámbito de las previsiones del art. 256 del CP español, que castiga el hacer uso de un terminal de telecomunicaciones sin consentimiento de su titular y ocasionando determinados perjuicios.

---

127 Véase SCHMID, N., *Computer- sowie Chech- und Kreditkarten-Kriminalität*, Zürich, 1994, pp. 199 y ss., en relación a la regulación del & 144 apartado 2 del StGB suizo.

— Otro aspecto hace referencia al efecto que la acción desenvuelta por el autor debe producir en el objeto material del delito, es decir, la determinación del efecto recibido por los datos, programas o documentos electrónicos. Problemática que posee ya incidencia en el mismo tipo general del delito de daños. La redacción del supuesto se refiere "al que por cualquier medio destruya, altere, inutilice, o de cualquier otro modo dañe datos, programas o documentos electrónicos", precisamente como estado que sigue al medio empleado para llevar a cabo el hecho. Esta destrucción, alteración o inutilización constituye así el resultado típico reclamado por el delito.

En relación a este resultado del delito se ha planteado si el mismo implica necesariamente la lesión de la sustancia del objeto, en el sentido de algún tipo de alteración de la estructura material del objeto. En lo que afecta al tipo básico del delito parece que la inclusión de la modalidad de inutilización hacía inevitable excluir la necesidad de lesión de la sustancia, abarcando, por tanto, el precepto los supuestos de lesión del mero valor de uso.

Sin embargo, para el caso concreto que estudiamos, GONZÁLEZ RUS[128] mantiene la exigencia de lesión de la sustancia de la cosa de acuerdo a distintas razones. En primer lugar –apunta este autor– por el carácter restrictivo de la punición en el Código de las meras lesiones de uso de los bienes, lo que es cierto, pero nada decide sobre el caso concreto. Señala también que la exigencia de ajenidad de los objetos sobre los que recae el comportamiento no se corresponde bien con la admisión de las lesiones de uso. Esta característica puede entenderse como un presupuesto acertado, pues lo único que excluye es que el propietario pueda ser sujeto activo, en cuanto aquí se tutela la capacidad de uso de los bienes que es una de las facultades que reúne el derecho de propiedad. Además se trata de una exigencia presente anteriormente en los otros supuestos punibles de mera afectación en el uso de la cosa (robo y hurto de uso de vehículos del art. 244 CP y uso de equipos de telecomunicaciones del art. 256 CP) en los que no resulta problemática tal exigencia.

128 "Protección penal de sistemas, elementos, datos y programas informáticos". *Revista Electrónica de Ciencia Penal y Criminología 1 (1999)*, pp. 5 y ss.

Frente al reparo de que incluida la inutilización queda claro que los daños abarcan los déficits de funcionalidad ocasionados al objeto, GONZÁLEZ RUS entiende que en realidad el supuesto de inutilización es congruente con la incidencia material del comportamiento dañoso sobre el objeto. Esto es cierto si se entiende que una lesión de uso puede sobrevenir por un comportamiento que represente alteración material de la cosa, lo que sucede es que, también puede darse el mismo efecto sin que se produzca tal alteración de la estructura material, lo que en Italia se conoce como identidad física del objeto.

Incluso el mantenimiento de la exigencia de la lesión de la sustancia en este supuesto en el que se trata de cosas incorporales puede provocar incerteza y resultados poco deseados. En primer lugar no sabemos bien en estos casos de cosas incorpóreas en qué consista la lesión de la sustancia. Y, además, según se entienda puede conducir a algún despropósito. Puesto que el legislador admite como objeto material del delito los elementos lógicos de los sistemas informáticos, se haría necesario distinguir entre los casos de daños con incidencia material (lesión de la sustancia) –punibles– y aquellos otros sin lesión de la sustancia –impunes. Cosa nada clara y que podría abocar a entender punibles sólo los producidos mediante ataques físicos, cuando el peso de la construcción penal parece tenerlo el resultado que debe acaecer y no los modos de ejecución del hecho.

Sin embargo GONZÁLEZ RUS[129] señala que no es necesaria la lesión física del soporte ¿entonces cómo debe entenderse la afectación de la sustancia en el caso de los elementos lógicos de los sistemas informáticos? Quizás la referencia novedosa a la alteración de la cosa como modalidad expresamente recogida en la regulación de los daños informáticos permita contribuir a reforzar la idea de que no se exige una afectación material de la cosa.[130]

---

129 "Protección penal de sistemas, elementos, datos y programas informáticos". *Revista Electrónica de Ciencia Penal y Criminología 1 (1999)*, p. 6.

130 No digamos si incluimos como daños el supuesto de deslucimiento del art. 626, como hace BAJO en la exposición de la parte especial en su *Compendio de Derecho Penal (Parte Especial), volumen II*, Ceura, 1998, p. 510. También lo hace MUÑOZ CONDE, F., *Derecho Penal, Parte Especial*, Tirant lo blanch, 1996, p. 417.

– Por otra parte parece pacífico que el delito de daños no es un hecho punible que requiera la causación de un perjuicio para el titular del bien dañado. Ha sido también un problema clásico para el delito de daños en general, resuelto con anterioridad a la aparición de los daños informáticos.[131] Y no habiendo razones diferenciadoras la solución debe ser la misma, es decir, el hecho punible de daños no protege el contenido económico del derecho de propiedad, por lo que no es preciso constatar en el hecho la producción de un determinado perjuicio sobre el bien.

Otra cosa es la exigencia de una cantidad mínima para que el hecho pueda ser castigado como delito (en sentido estricto) y no mera falta como infracción penal leve. En realidad el hecho es punible en todo caso, aún cuando la cuantía del daño sea inferior a las 50.000 ptas. exigidas por el art. 263, lo que sucede es que lo será con pena leve como corresponde a las faltas del Libro III del CP.

No parece tan problemático el hecho de que la cuantía de los daños causados directamente sobre los elementos lógicos puede ser menor y, sin embargo, mayor los causados sobre la funcionalidad del sistema informático, como pone de relieve GUTIÉRREZ FRANCÉS.[132] En realidad no tiene porqué dejarse de computar en la evaluación económica de los daños los derivados de la no funcionalidad del sistema informático, entre otras cosas porque se admite expresamente la modalidad de inutilización que justamente abarca la lesión del valor de uso de la cosa.

---

131 Así, BAJO FERNÁNDEZ, M. *Compendio de Derecho Penal (Parte Especial)*, volumen II, Ceura, 1998, p. 505. También MUÑOZ CONDE, F. *Derecho Penal, Parte Especial*, Tirant lo blanch, 1996, p. 414. Igualmente en otros sistemas jurídicos, SCHMID, N., *Computer- sowie Chech- und Kreditkarten-Kriminalität*, Zürich, 1994, p. 193.

132 "Delincuencia económica e informática en el nuevo Código penal". Ámbito jurídico de las tecnologías de la información. Cuadernos de Derecho Judicial. Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, p. 294 y MATELLANES, "Algunas notas sobre las formas de delincuencia informática en el Código Penal". *Hacia un Derecho Penal sin fronteras* (DIEGO DIAZ-SANTOS, Mª R./ SÁNCHEZ LÓPEZ, V., Coordinadoras), Colex, 2000, p. 143. Piénsese en los desajustes y retrasos para una empresa en la que su actividad se gestiona y organiza a través de un sistema informático.

– En lo tocante a los grados de ejecución del delito se presentan aspectos complejos y de gran interés. Como indica GONZÁLEZ RUS[133] la consumación de los daños informáticos vendría a exigir la desaparición completa y definitiva de los datos, ficheros o programas almacenados en cualquier tipo de soportes. Es pues necesario que el comportamiento sea irreversible, produciendo la pérdida o menoscabo definitivo de los mencionados elementos informáticos. Por ello señala este mismo autor[134] que los casos en los que el procedimiento de destrucción no llega de manera efectiva a llevar a cabo su misión o cuando existan copias de seguridad deberemos entender presente un supuesto punible de tentativa. Existe, sin duda, un comienzo de ejecución del tipo con hechos que deberían ser suficientes para producir el resultado delictivo, pero éste no se produce por causas independientes de la voluntad del autor, como exige la regulación del art. 16 del CP para el castigo de la tentativa.

De los dos casos mencionados, el de la copia de seguridad creo que permite adentrarnos en la singularidad de los hechos punibles relacionados con la informática. Y ello pues en principio pudiera parecer poco acertado la exclusión de la punibilidad cuando se destruye un determinado archivo de la memoria central pero se cuenta con una copia de seguridad. En realidad concurren todos los requisitos del comportamiento típico de los daños: un objeto material admitido por el propio legislador y la destrucción de esos mismos datos, programas o documentos electrónicos. De forma que al igual que ocurre cuando se destruye un valioso jarrón del que su propietario posee una o más copias idénticas, el hecho parece punible. Ahora bien, para el caso de los elementos lógicos es posible introducir un elemento diferencial. Los datos o programas tienen siempre un valor instrumental y gozan de la posibilidad de ser reproducidos indefinida y rápidamente por la propia naturaleza de los procedimientos informáticos. Creo que es una argumentación de este tipo la que permite justificar la no punibilidad de la destruc-

133 "Protección penal de sistemas, elementos, datos y programas informáticos". *Revista Electrónica de Ciencia Penal y Criminología 1 (1999)*, p. 7.

134 "Protección penal de sistemas, elementos, datos y programas informáticos". *Revista Electrónica de Ciencia Penal y Criminología 1 (1999)*, pp. 7-8.

ción de datos o ficheros existentes otras copias, frente a casos como el mencionado del jarrón aún contando con al existencia de réplicas idénticas.

En realidad, el caso de destrucción de datos o ficheros cuando en otros soportes se cuenta con copias de los mismos habría que calificarlo como de tentativa imposible, pues dado el carácter de repetibilidad expansiva de estos objetos el auténtico objeto material del delito lo constituirían la totalidad de copias o archivos idénticos existentes. La destrucción real de archivos o datos informáticos únicamente se logra si se acaba con las réplicas que pudieran encontrarse como copias de seguridad o respaldo en cualquier tipo de soporte. Sólo a este tipo de hipótesis podemos llamar destrucción o desaparición completa y definitiva de datos, programas o documentos electrónicos. Por ello sólo estaríamos ante una tentativa idónea, es decir, punible, si la acción se dirige a ocasionar la destrucción de todos los archivos y datos idénticos que existan en cualquier tipo de soporte y, por cualquier motivo ajeno a la voluntad del autor esto no sucede.

Una situación singular a los grados de ejecución del delito lo representan aquellos casos en los que el procedimiento de menoscabo de datos, programas o documentos no entran en funcionamiento en el momento en el que el autor lo introduce, sino pasado un tiempo ante la presencia de determinadas circunstancias (una fecha predeterminada, la aparición de algunos datos en el sistema o la eliminación de ciertos datos del sistema). Se produce así un distanciamiento temporal entre la introducción del programa agresivo y la ejecución misma del hecho que hace necesario determinar el momento de comienzo de la tentativa y la producción de la consumación del hecho.

Para CORCOY[135] la tentativa comienza en el momento en el que el autor pierde el control del instrumento, de manera que si el mismo autor tuviera la oportunidad posterior de intervenir para evitar

135 "Protección penal del sabotaje informático. Especial consideración de los delitos de daños". *La Ley,* vol. 1, nº 2400 (1990), pp. 1014-15.

el resultado lesivo nos encontraríamos ante el desistimiento. Parece que la tentativa debe afirmarse igualmente si el autor introduce las órdenes en el sistema que posteriormente deben producir los daños y sigue manteniendo sobre las mismas, permanentemente, la posibilidad de evitar su activación. La consumación se producirá, aunque medie un lapso temporal amplio, en el momento en el que los elementos lógicos del sistema informático resultan efectivamente dañados.

Se ha indicado por tanto como se entiende en la doctrina española y para nuestra legislación la problemática referida al momento de la consumación de este tipo de hechos delictivos. La misma no está presente sino con la destrucción o alteración definitiva de los datos o programas informáticos. En otros contextos doctrinales, sin embargo, la consumación parece concebirse de modo menos exigente. En otros sistemas y con relación a supuestos particularizados respecto a virus informáticos se estima punible la perturbación temporal de la operatividad del sistema por lo que de ninguna manera puede entenderse presente un efecto irreversible o definitivo.[136]

– Hasta el momento hemos estado presuponiendo un comportamiento doloso por parte del autor. Es decir, contando con que el sujeto activo dirige su comportamiento consciente y voluntariamente a la destrucción o inutilización de ciertos elementos lógicos de un sistema informático. Pero, sin embargo, el legislador no sólo concede relevancia en este campo a los comportamientos dolosos, sino que también para los casos de destacada gravedad cometidos por imprudencia hace intervenir al Derecho Penal.

En efecto la regulación del art. 267 CP admite el castigo de los daños imprudentes con carácter general –no sólo para los daños informáticos– aunque supeditado siempre a condicionamientos de distinta naturaleza. Así se exige, en primer lugar, que el comportamiento pueda ser calificado como de imprudencia grave, esto es, como comportamiento que desatienda las normas de diligencia más

136 Véase PICA, G., *Diritto penale delle Technologie Informatiche*, Utet, Torino, 1999, pp. 98-9.

elementales. Cualquier otro tipo de imprudencia que pudiera ocasionar los daños quedaría al margen de la persecución penal. Además, necesariamente el hecho debe originar unos perjuicios superiores a diez millones de pesetas.

Por otra parte, y ahora desde un punto de vista procesal, se condiciona la persecución de estos hechos a que medie denuncia de la persona agraviada o de su representante legal, excluyéndose, por tanto, la iniciación de la investigación penal de oficio por los órganos de la Administración de Justicia. Finalmente, incluso, se concede una amplia eficacia al perdón del ofendido, que puede paralizar la acción penal y extinguir la pena. Desde estas dos últimas ópticas se procede a convertir a los daños imprudentes en un delito semipúblico.

La admisión por el legislador de la imprudencia en este campo puede tener trascendencia en determinados campos. Así en aquellos supuestos de sabotaje consistentes en introducir una serie de órdenes que provocan su autoreproducción, el resultado final escapa al control y a la previsión incluso del autor o en los procedimientos llamados caballo de Troya,[137] por lo que la imputación subjetiva de este tipo de comportamientos se moverá en la zona fluida entre el dolo eventual y la imprudencia con representación.

Lo cierto es que pese a los condicionantes de no escasa importancia exigidos para que los daños imprudentes –en cualquiera de sus modalidades– alcancen relevancia penal, sin embargo no deja de representar su punibilidad un cierto desajuste desde la óptica político-criminal. El castigo de hechos imprudentes debe reservarse –como exigiría una ponderada aplicación del principio de intervención mínima– para los hechos que amenacen bienes jurídicos del más alto rango y que no puedan ser salvaguardados mediante otros procedimientos jurídicos menos lesivos.

137 Comportamientos de sabotaje descrito por CORCOY BIDASOLO, M. "Protección penal del sabotaje informático. Especial consideración de los delitos de daños". *La Ley,* vol. 1, nº 2400 (1990), pp. 1004-5.

La protección de intereses patrimoniales lesionados imprudentemente, por legítimos que sean y pese a su reconocimiento como bien penalmente tutelado cuando de comportamientos dolosos se trata, pueden ser adecuadamente defendidos a través de los instrumentos que aportan otras normas no penales y las cuales representan consecuencias menos gravosas. La reparación civil a través de un proceso de esa naturaleza se presenta como la vía jurídica idónea de protección de estos intereses, sin que pueda apreciarse con carácter general la necesidad de acudir a las medidas jurídico-penales como última *ratio* del Ordenamiento Jurídico en la protección de intereses básicos de las personas y de la sociedad.

IV. EL BIEN JURÍDICO PROTEGIDO

En último lugar cabe plantear la determinación del bien jurídico protegido en el supuesto de los daños informáticos. Frente a las habituales exposiciones en las que la referencia al bien jurídico se realiza en los primeros momentos para luego poder aplicar el contenido del mismo sobre los aspectos de dudosa interpretación en el hecho punible de que se trate, aquí la situación es diversa. El método antes señalado corresponde a aquellas figuras en las que el bien jurídico ha sido objeto ya de una atención detenida y existe una posición sólida sobre el mismo, por lo que interesa que despliegue su función de criterio interpretativo en los elementos de mayor imprecisión en la determinación del alcance del delito.

Sin embargo, en nuestro caso se trata de una figura de reciente incorporación a la legislación penal cuyo bien jurídico no ha podido, por tanto, ser analizado con detenimiento, e incluso puede resultar discutido. Así resulta metodológicamente necesario realizar previamente el estudio de su configuración legislativa para poder extraer consecuencias sobre la finalidad de protección que cabe asignarle. Además, naturalmente de la contemplación del interés jurídico-penal protegido desde la perspectiva político-criminal.

El delito como es notorio se encuentra regulado en el ámbito del tradicional delito de daños. Por ello cabe sin mayores diferenciaciones, como una de las opciones interpretativas, identificar el

bien jurídico con el general de los daños.[138] Se acepta generalmente como bien jurídico-penalmente relevante en el tipo básico del delito de daños la propiedad. En este caso el menoscabo del bien jurídico propiedad se produce por desaparición física o disfuncionalidad práctica del objeto material en el que se plasma y sobre el que se pueden verter los contenidos jurídico-económicos del derecho de propiedad. De esta manera se puede adoptar el mismo bien penalmente protegido en los daños informáticos, lo que en muchas ocasiones cabe entender en las exposiciones de este nuevo supuesto delictivo cuando no se hace mención a ninguna alteración en este campo del régimen general del delito de daños.

Sin embargo, en ocasiones se apunta una visión distinta respecto al concreto interés jurídico penalmente relevante para los daños informáticos, de forma no coincidente con lo establecido para los daños en general. Así GUTIÉRREZ FRANCÉS[139] en un análisis dedicado exclusivamente a la perspectiva empresarial del sabotaje informático, señala la presencia de intereses de contenido económico no necesariamente identificables con el patrimonio *strictu sensu*. Se refiere con ello la autora a la particular trascendencia de los sistemas informáticos en la organización y gestión de la actividad empresarial, cuya disfuncionalidad puede ocasionar graves problemas y lesión de intereses económicos que van mucho más allá de la destrucción o inutilización del propio sistema de organización y gestión de la empresa.

De esta aproximación particularizada al problema del bien jurídico, MATELLANES[140] hace una generalización, entendiendo que únicamente se contemplan los perjuicios que afecten a la capacidad competitiva de la empresa. Parece que la confusión arranca con la

138 También en otros sistemas jurídicos. Así PICA, G., *Diritto penale delle Technologie Informatiche*, Utet, Torino, 1999, pp. 87 y ss.

139 "Delincuencia económica e informática en el nuevo Código penal". *Ámbito jurídico de las tecnologías de la información. Cuadernos de Derecho Judicial*. Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, p. 297.

140 "Algunas notas sobre las formas de delincuencia informática en el Código Penal". *Hacia un Derecho Penal sin fronteras* (DIEGO DÍAZ-SANTOS, Mª R./ SÁNCHEZ LÓPEZ, V., Coordinadoras), Colex, 2000, p. 142.

forma de concebir el perjuicio para este hecho delictivo. Se señala bien por estas autoras que el perjuicio no sólo hace referencia a la destrucción misma del *software* sino a los derivados para la actividad de la empresa al no poder hacer empleo del mismo.

Esto es correcto pero sucede que el perjuicio no es un auténtico elemento del tipo, pues el delito de daños no reclama que necesariamente con el comportamiento típico se produzca finalmente un perjuicio patrimonial al titular del bien.[141] Hay que tener en cuenta que el bien jurídico o interés penalmente relevante que pretende tutelar esta figura delictiva no hace referencia a una cuantía económica como forma de menoscabo patrimonial, sino que éste consiste en la incapacidad de disposición del propietario sobre sus bienes en todas sus dimensiones jurídico-económicas.

Es verdad que en este campo ha resultado perturbador la tradicional división en escalas, que permitía según la concepción del momento el establecimiento de penalidades diferenciadas según la cuantía del hecho. En esa situación resultaba fácil entender que el perjuicio constituía un elemento más del tipo, aunque en realidad no formaba parte de la materia de prohibición, sino que lo estrictamente necesario era que el objeto poseyera un valor económico[142] –mayor o menor– que se situaba así como una auténtica condición objetiva de punibilidad.

Por eso el problema respecto a las dificultades en la cuantificación del perjuicio no posee relevancia en el campo estrictamente penal.[143] Otra cosa será a la hora de determinar la posible indemnización de naturaleza civil que resultara también del hecho delictivo.

---

141 Por todos BAJO FERNÁNDEZ, M., *Compendio de Derecho Penal, volumen II*, Ceura, 1998, pp. 504 y ss.

142 Así MUÑOZ CONDE, F., *Derecho Penal, Parte Especial*, Tirant lo blanch, 1996, p. 415.

143 Me refiero fundamentalmente a la posibilidad de computar en tal perjuicio la lesión misma sobre los elementos del sistema informático sino además las repercusiones económicas que pudiera generar la inoperancia de esos datos, programas o documentos electrónicos. También puede poseer trascendencia la necesidad de establecer la cuantía del perjuicio a los efectos de situar el hecho típico entre las faltas del Libro III, en el tipo básico del art. 263.

De todas maneras el que para el caso de la gestión empresarial se presenta en estos comportamientos de forma singular, es una cuestión de hecho que no puede ser tomada como criterio general pues ni siquiera los daños informáticos se producen necesariamente en ámbitos empresariales.

MARCHENA[143bis] plantea la posible concurrencia de otros bienes jurídicos para determinados casos. En determinadas acciones destructivas en el campo de las comunicaciones, el patrimonio puede no ser el único bien jurídico afectado. De forma que si el propósito del autor busca en sí mismo la interrupción o destrozo de los sistemas de telecomunicaciones –y no el aspecto económico– resultará aplicable el art. 560.1 del CP.

Confirmación de que el bien jurídico tutelado por la norma de los daños informáticos sigue siendo el mismo que para los daños en general es también la exigencia de ajenidad respecto al objeto material del delito, que siempre se ha recogido por el legislador penal en relación a la protección de la propiedad en su perspectiva jurídico-penal. Igualmente cabe recordar cómo con carácter general se ha entendido la inclusión de los daños informáticos como una simple forma de evitar dudas en la extensión del delito de daños a este tipo de comportamientos como se ha puesto de relieve anteriormente y no por la necesidad de incorporar una nueva regulación que tuviera una finalidad de tutela diversa.[144]

---

143 bis "Sabotaje informático: ¿una forma de desórdenes públicos?", *Actualidad Informática Aranzadi*, 10/2001, pp. 11-12.

144 Dogmáticamente los daños informáticos representan una determinación específica del objeto material del delito, precisamente para evitar dudas en la aplicación del delito a lo que criminológicamente se denomina sabotaje informático. El resto de elementos de la figura permanecen inalterados, salvo que los mismos se aplican, dada la regulación particularizada, en relación siempre a estos concretos elementos informáticos. Criminológicamente las diferencias son más acusadas, aunque esto no influye en la construcción legislativa de la figura criminal.

SECCIÓN TERCERA

Regulación penal de la Propiedad intelectual relacionada con ficheros de datos y programas de ordenador

I. INTRODUCCIÓN

Con carácter general la tutela penal de la propiedad intelectual protege frente a los ataques más graves para el conjunto de facultades que el creador tiene sobre su obra literaria, artística o científica (derechos de autor). La regulación penal se refiere a las conductas de reproducción, distribución, comunicación pública o plagio de las obras sobre las que recaen derechos de autor. Es lo que desde un punto de vista genérico y extrajurídico se conoce como piratería.[145]

La tutela jurídica de los programas de ordenador, después de un primer debate se ha reconducido a las instituciones de la propiedad intelectual, excluyéndose incluirlos entre los derechos relativos a la propiedad industrial, de acuerdo a la perspectiva de las Instituciones europeas.[146] Por tanto también los hechos de relevancia penal en este ámbito se incluyen entre los delitos relativos a la propiedad intelectual.

Desde 1987 se ha abandonado la técnica de las leyes penales en blanco, pues ahora el tipo penal recoge expresamente las conductas atentatorias a la propiedad intelectual que acabamos de mencionar. Ello, naturalmente, no quiere decir que se deje de tener en cuenta la regulación civil de la LPI, pero sí que no se da un automatismo a la hora de rellenar de contenido las conductas incriminadas, de forma que el intérprete y aplicador del Derecho posee una mayor capacidad al integrar tales comportamientos desde su inicial configuración civil en la técnica y fines de la tutela penal.

---

145 SEMINARA, S. "La pirateria su Internet e il diritto penale*", Rivista Trimestrale di diritto penale dell´economia* 1,2 (1997), p. 73.

146 Véase PANSIER/JEZ *La criminalité sur l´Internet*, PUF, 2000, pp. 35 y ss. También PICA, G.*, Diritto penale delle Technologie informatiche*, Utet, Torino, 1999, pp. 188 y ss.

En este sentido todas las causas de exclusión de la ilicitud de una conducta en la regulación civil tienen aplicación en el ámbito penal. Por lo tanto deben aplicarse y poseer plena eficacia para el Derecho Penal los límites generales temporales y espaciales relativos a los derechos de propiedad intelectual (art. 98 con relación al Capítulo I del Título III de la LPI, en cuanto a la duración). Sin embargo, todos los aspectos de la regulación civil que amplíen o agraven la responsabilidad pueden ser objeto de revisión para su integración en las conductas penalmente relevantes.

II. SUJETOS PASIVOS DEL DELITO

Interesa ahora destacar los sujetos pasivos del delito, tema que en este hecho punible posee alguna complejidad por el buen número de variantes que pueden presentar tales sujetos, que van a coincidir con los posibles titulares de los derechos de autor o de propiedad intelectual. Nos referimos por tanto a todos los titulares de los derechos de propiedad intelectual o sus cesionarios. Para esto debemos atenernos a la regulación de la LPI. Tiene gran trascendencia la determinación de estos sujetos pues son los que pueden consentir válidamente la cesión a terceros de los derechos de explotación de la obra y por tanto determinan el sujeto pasivo del concreto hecho delictivo.

GONZÁLEZ GÓMEZ[147] distingue entre sujetos pasivos principales y secundarios de acuerdo a las formulaciones legales para ser titular de los derechos de propiedad intelectual sobre una obra, e incluso señala distintos grados en cada uno de esos grandes grupos de sujetos.

Como sujetos pasivos principales de primer grado se consideran a los titulares originarios de los derechos de autor. Es en definitiva el creador de la obra, como sujeto pasivo por excelencia. En cuanto a alguna de las modalidades es irreemplazable, como sucede para el plagio. Así lo sería por ejemplo el creador de un programa informático (art. 7 L 16/1993).

147 *El tipo básico de los delitos contra la propiedad intelectual*. Tecnos, Madrid, 1998, pp. 138 y ss.

Dentro de este mismo grupo se incluyen los sujetos pasivos principales de segundo grado: titulares originarios de "otros derechos" de propiedad intelectual. Son los derechos afines o conexos a los de los autores, distintos a los relativos a la creación misma de la obra, y que suponen una actividad de mediación entre el autor y el público.

El segundo gran grupo de sujetos pasivos viene representado por los llamados sujetos pasivos secundarios, en el que se reúnen a los cesionarios de los derechos de propiedad intelectual *–latu sensu–*, entre los que cabe considerar a quienes reciben mediante contrato los derechos de explotación de la obra, la cesión presunta (según disposición de la LPI) y los cesionarios *mortis causa*.

La regulación legal se refiere a "los titulares de los correspondientes derechos de propiedad intelectual o sus cesionarios", fórmula en la que cabe integrar a todos los que acabamos de mencionar. Para el caso de los programas de ordenadores los titulares de los correspondientes derechos de propiedad intelectual figuran en el art. 97 LPI.

III. OBJETO MATERIAL DEL DELITO

1. El objeto material en general en estos delitos

En cuanto al objeto físico sobre el que debe recaer materialmente la acción delictiva, el legislador hace mención en primer lugar a las distintas clases de obras. Así el tipo penal se refiere a las obras literarias, artísticas o científicas. Pero también admite como posible objeto material del delito la transformación, interpretación o ejecución artística de cualquiera de las obras antes mencionadas.

Generalmente se entiende que son exigibles distintos requisitos de las obras para su consideración a los efectos de la propiedad intelectual. Por una parte debe tratarse de creaciones originales y también que tal obra haya sido exteriorizada de alguna manera: expuesta a través de cualquier medio o soporte que permita su percepción a terceros.

2. Objeto material de los delitos informáticos relativos a la propiedad intelectual: el concepto jurídico de programa de ordenador

a. El concreto objeto material del delito lo constituye en nuestro caso los programas de ordenador, definidos en el art. 96.1 LPI como "toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuera su forma de expresión y fijación".

En la definición legal que se acaba de reproducir se tocan distintos aspectos del mencionado objeto material. En primer lugar el modo característico de funcionamiento del mismo, que consiste en una secuencia de instrucciones. Tales secuencias de instrucciones tienen como destino un ordenador o sistema informático. Y, finalmente, la misión de tales secuencias de órdenes incluidas en un sistema informático es la de realizar una función u obtener resultado determinado.

En otros sistemas jurídicos, como el italiano se prefiere no efectuar una definición legal de este objeto para evitar los problemas que pudieran surgir con la evolución técnica, exigiéndose en todo caso que la obra sea de carácter creativo y original.[148]

En un sistema informático se distinguen dos partes, como señala ROMEO:[149] lo referente al soporte del programa, que es tangible (el disco en el que se encuentra registrado) y, por otra parte, el medio de expresión consistente en unos impulsos (instrucciones) eléctricos intangibles.

b. La protección de los derechos de autor sobre programas de ordenador se efectúa a través de su asimilación a estos efectos a las obras literarias (así art. 1 L 16/1993, de 23 de diciembre, que incorpora la Directiva 91/250/CEE de 14 de mayo –art. 1.1–). A estos

148 En este sentido PICA, G. *Diritto penale delle Technologie informatiche*, Utet, Torino, 1999, pp. 196-7.

149 "La protección penal del software en el Derecho español", *Actualidad Penal* 35/1988, pp. 1832-3. Sobre la distinción entre la obra misma y el soporte físico en relación a la teoría del agotamiento, véase PANSIER/JEZ, *La criminalité sur l´Internet*, PUF, 2000, p. 42.

efectos la protección de los derechos de autor sobre programas informáticos comprende tanto el *software* como la documentación técnica, los manuales de uso y la documentación preparatoria (art. 96.1 LPI). Como en España, en otros países la noción extrapenal de programa de ordenador incluye estos materiales preparatorios y complementarios. Sin embargo es dudoso que puedan ser incluidos en el objeto material del hecho punible, dadas las garantías propias del principio de taxatividad, pues el legislador penal podía haberlos mencionado de haber sido esa su intención conociendo las exigencias del principio de legalidad en la construcción de las infracciones punibles.

IV. ESTRUCTURA DE LA REGULACIÓN LEGAL Y PRESUPUESTOS GENERALES DE LAS CONDUCTAS PUNIBLES

1. Estructura de la regulación legal

La regulación legal de la protección penal de la propiedad intelectual se sitúa en un apartado del Código penal que posee independencia sistemática (sección 1ª del capítulo XI), dentro del grupo de delitos patrimoniales y contra el orden socioeconómico (Título XIII). En la concreta regulación se contiene un tipo básico (art. 270), unos tipos agravados (art. 271), así como referencias a aspectos relativos a la responsabilidad civil y la publicidad de la sentencia condenatoria (art. 272).

El tipo básico, que reúne las conductas más elementales contrarias a la tutela penal de la propiedad intelectual, incluye las de reproducción, distribución, comunicación pública y plagio de la obra concreta. Un segundo párrafo, de este mismo precepto, se refiere a las conductas de importación, exportación y almacenaje de las obras que se entienden asimiladas a la previamente señalada conducta de distribución como acciones específicas dentro de ésta. Todavía dentro del tipo básico un tercer párrafo se refiere a la tutela de un concreto objeto: los dispositivos de protección de los programas de ordenador, lo que no deja de suscitar algunos problemas que intentaremos destacar.

Según lo que hemos visto en la estructura de la regulación legal, en cuanto al comportamiento típico, se distingue, según la naturaleza de las facultades de los derechos de autor menoscabadas entre comportamientos que afectan a los derechos morales del autor y los que se relacionan con la explotación económica de la obra.[150]

2. Elementos comunes a los distintos comportamientos punibles

Con la nueva regulación del Código Penal de 1995 el legislador incorpora a la redacción del tipo básico –y por tanto también para los tipos agravados– dos nuevos elementos que restringen el ámbito de la punibilidad: el ánimo de lucro y que el autor actúe en perjuicio de tercero. Además el hecho, como sucedía con anterioridad debe llevarse a cabo sin el consentimiento del titular de los derechos de propiedad intelectual. El conjunto de estos elementos exigibles para todo supuesto punible reduce el campo de aplicación de estos delitos y los orientan hacia contenidos netamente patrimoniales.

a. Cualquier ilicitud en el campo de la tutela de la propiedad intelectual queda supeditada a que el titular de los derechos no preste su acuerdo a la utilización de su obra en cualquiera de las distintas formas posibles. Esta necesaria ausencia del consentimiento del titular de los derechos se debe hacer todavía más patente en el ámbito de las infracciones penales. Por ello en el campo penal se exige la ausencia clara e indudable de permiso suficiente objetiva y subjetivamente, como señala QUINTERO.[151]

El efecto indudable de la prestación de consentimiento válido por el titular de los derechos de autor será la irrelevancia penal de la conducta. Ahora bien siendo esto claro, sin embargo resulta discutida la naturaleza jurídica que deba otorgarse a tal exención de responsabilidad. Para unos constituye una causa de atipicidad. Así según la mayoría de la doctrina con el consentimiento del titular se

150 En este sentido véase PANSIER/JEZ *La criminalité sur l´Internet*, PUF, 2000, pp. 40 y ss.

151 *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 1999, p. 611.

excluye el tipo mismo.[152] Otros, sin embargo optan por considerar, al menos parcialmente, el consentimiento una auténtica causa de justificación. ROMEO,[153] en este sentido, considera que para algunos casos, cuando entren en juego los llamados derechos morales, entiende que únicamente se excluye el carácter ilícito de la conducta pues se trata de derechos irrenunciables e inalienables.

En todo caso los sujetos que pueden prestar válidamente el consentimiento serán los titulares de los derechos de propiedad intelectual, conforme a la regulación jurídico-privada de la LPI a la que se ha hecho mención a la hora de hablar de los sujetos pasivos del delito.

b. El ánimo de lucro, como dirección subjetiva que necesariamente debe guiar el comportamiento del autor se presenta en la nueva regulación como un auténtico elemento del tipo básico, que por tanto también deberá aparecer en los tipos agravados.[154] En la regulación anterior únicamente hacía surgir su presencia una las posibles formas de agravación del tipo básico, es decir, que tal tipo podía presentarse y ser punible la conducta sin que el autor actuara movido por el ánimo de lucro.

Como se sabe en cuanto a la determinación del concepto de ánimo de lucro existen dos posibilidades conceptuales.[155] La primera, más restrictiva, vincula tal elemento a la búsqueda por el autor de un enriquecimiento con la realización del comportamiento. La segunda opción mantiene un concepto sumamente amplio que permite extender el mismo a cualquier tipo de ventaja perseguida por el autor. Esta segunda fórmula, que prácticamente desdibuja el elemento, es mantenida por la jurisprudencia en los distintos ámbitos

---

152 JORGE BARREIRO, A. *Comentarios al Código Penal*, Civitas, 1997, p. 773.

153 "La protección penal del software en el Derecho español", *Actualidad Penal* 35/ 1988, p. 1841.

154 Componente subjetivo en el ámbito de la responsabilidad penal frente a lo que sucede en el campo de la responsabilidad civil que no lo exige, al menos para el caso francés. Así PANSIER/JEZ, *La criminalité sur l´Internet*, PUF, 2000, p. 53.

155 Sobre ello puede verse MATA y MARTÍN, R.M., El delito de robo con fuerza en las cosas, Tirant lo blanch, 1995, pp. 218 y ss.

típicos de presencia de este elemento. También en el caso de los delitos relativos a la protección de la propiedad intelectual los Tribunales aplican esta noción amplia, como sucede en la sentencia de la AP de Zaragoza de 14-11-95.[156] En todo caso el lucro perseguido con el comportamiento puede revertir en el propio autor o en un tercero.

c. Como mayor novedad el legislador de 1995 ha introducido el requisito de que el autor del hecho delictivo obre en perjuicio de tercero. Elemento sobre el que pesa cierta indeterminación, pues puede ser completado en sentido subjetivo o bien desde una perspectiva objetiva, naturalmente con desiguales consecuencias.

En sentido subjetivo se entiende este elemento como tendencia interna del autor que dirige su comportamiento a provocar determinados resultados lesivos al titular de los derechos de autor. Se trataría de una tendencia interna del autor que debe verificarse mediante su conexión con otros datos externos revelados en los hechos. De otra manera, en sentido objetivo, se representa como idoneidad material de la conducta para causar perjuicios a los titulares de los derechos.[157] Así la presencia del mismo resulta verificable directamente en cuanto debe tratarse de una conducta capaz de conseguir la lesión de estos derechos.

En relación al problema del posible perjuicio derivado de este tipo de comportamientos la sentencia de la AP de Barcelona de 3-6-98[158] en aplicación de la regulación anterior, considera que se trata de un delito de mera actividad, que no precisa para su consumación un resultado, por lo que es irrelevante que exista perjuicio o no. Esto resulta coherente con la regulación legal del hecho punible pues aun cuando se entienda el requisito de que el autor actúe en perjuicio del tercero en sentido objetivo, el mismo no reclama un perjuicio efectivo y real, sino la tendencia objetiva (idoneidad, posibilidad) de conseguirlo.

---

156 La Ley-Actualidad a52/1996, Marginal, 115.

157 En este sentido GONZÁLEZ RUS, J.J., *Curso de Derecho Penal Español, Parte especial I*, Marcial Pons, 1996, p. 779 quien excluye por ello la tipicidad de la copia privada.

158 A. 3586.

V. INFRACCIONES DE LOS DERECHOS MORALES DEL AUTOR: EL PLAGIO

1. Contenido de los ataques a los derechos morales del autor

Tales infracciones referentes a los derechos morales sobre la obra vienen constituidos por el comportamiento de plagio. Fundamentalmente se protege la paternidad, integridad, respeto a la esencia y contenido de la obra (la enumeración de las particulares facultades del autor afectadas por el plagio se encuentran en el art. 14 LPI).

Se puede distinguir, como hace en ocasiones la doctrina, entre un concepto amplio y otro estricto de plagio.[159] El primero abarca tanto la usurpación de la condición de autor como la imitación fraudulenta, mientras que la versión restringida distingue entre ambos campos. Se entiende que con la regulación del CP de 1995, que reunifica ambos aspectos en el tipo básico, se asume por el legislador la concepción amplia.

2. Requisitos del comportamiento punible de plagio

Los requisitos del comportamiento punible de plagio vienen definidos por la exteriorización de una obra que posea similares características a la original. La exteriorización consiste en la difusión de carácter público de la obra en cualquier modo. Es necesario además la manifiesta similitud con la forma de presentación de las ideas y contenidos en la obra original

Sin embargo no cualquier similitud o parecido entre las obras integra este requisito del tipo penal. Por eso no es la mera falta de originalidad de la obra sino la usurpación de la obra mediante la presentación de otra con identidad sustancial. En este sentido QUINTERO[160] señala que al Derecho Penal sólo le puede corresponder los

159 Así GONZÁLEZ GÓMEZ, *El tipo básico de los delitos contra la propiedad intelectual*. Tecnos, Madrid, 1998, pp. 192-3.

160 *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 1999, pp. 609-10.

supuestos de identidad sustancial entre las obras. También en otros ámbitos geográficos se pone el acento en estas limitaciones. Así PANSIER/JEZ[161] señalan que únicamente la copia servil o quasiservil, en nuestro caso del programa de ordenador, puede ser objeto de protección.

3. Problemas particulares

En el conjunto de la regulación sobre esta materia existen problemas o circunstancias particulares que van a incidir en la relevancia de algunos hechos. Así hay que tener en cuenta que según la legislación mercantil no constituye plagio la realización de versiones sucesivas de un programa por el cesionario de los derechos de explotación, salvo que mediara pacto en contrario.

Otro problema singular hace mención a la posible coincidencia entre autor de la obra y autor de un delito relativo a la propiedad intelectual: ¿El autor del programa, autor del delito? Circunstancia que se plantea en el caso de la sentencia de la AP de Barcelona de 3-6-98.[162] En este supuesto un Informático al servicio de una empresa interviene junto con otro programador en la creación y desarrollo del programa GQ de control de calidad. Antes de dejar de prestar servicios en la empresa efectuó una copia del código fuente y de la aplicación del mencionado programa. Posteriormente creó una nueva empresa que aprovecha el mencionado programa y efectúa pequeñas modificaciones sobre el mismo.

El Tribunal entiende cometido un plagio con irrelevante modificaciones. El acusado señala que siendo titular de una parte del derecho de propiedad intelectual, no cabe entender su conducta como plagiaria. El Tribunal responde que el programa fue creado en virtud de una relación laboral con una empresa, a la cual se ha de entender transmitido el derecho de explotación de la obra… sin que tenga relevancia el derecho moral del autor.

---

161 *La criminalité sur l´Internet*, PUF, 2000, p. 39.

162 A. 3586.

VI. INFRACCIONES DE LOS DERECHOS DE EXPLOTACIÓN DE LA OBRA

El segundo grupo de comportamientos los constituyen los hechos relativos a los derechos de explotación de la obra, con contenidos ya nítidamente patrimoniales. Entre estas infracciones se encuentran las de reproducción, distribución y comunicación pública. Veremos el sentido de la previsión legislativa referente a la importación, exportación y almacenaje con especiales repercusiones para el tráfico internacional de programas de ordenador.

1. La conducta punible de reproducción

a. La reproducción, primera de las conductas punibles mencionadas, consiste en la fijación de la obra en un medio que permita su comunicación y obtención de copias de toda o parte de ella (art. 18 LPI).

Un supuesto de reproducción lo recoge la sentencia de la AP La Coruña de 27 junio 1995. El acusado antiguo empleado de la empresa P acudió a solicitud de otra empresa cliente de P para el arreglo de determinados problemas informáticos ante la imposibilidad de contactar con P. El autor realizó un cambio del sistema operativo, con reproducción del sistema operativo sin licencia y gracias a una copia clandestina de los programas de P hizo diversas modificaciones en el programa de P, dificultando que P pudiese cumplir sus funciones de asistencia y mantenimiento y consiguiendo que las mismas se encargaran a su propia empresa.

También la sentencia de la AP de Alicante de 3-11-98[163] presenta otro caso de reproducción en el que se produce la copia de unos planos realizados por otro arquitecto para la realización de una urbanización ante la falta de acuerdo económico final del primer arquitecto con la constructora.

En el ámbito de este concreto comportamiento punible se distingue dos clases: la reproducción efectiva y la llamada reproduc-

163 A. 5604.

ción potencial. La reproducción efectiva se concibe como la obtención de copias o ejemplares de la obra, naturalmente sin contar con el consentimiento del titular de los derechos. Por su parte la reproducción potencial se entiende en el sentido de fijación o incorporación de la obra en un soporte distinto del que sirvió para crearla o expresarla por primera vez.

En el texto de la sentencia de la AP de Castellón de 18-5-98[164] aparece un nuevo caso de reproducción de programas de ordenador con relevancia penal. Un establecimiento comercial dedicado a la informática vendió a un cliente un ordenador al que previamente se le había introducido un sistema operativo sin contar con el paquete de autenticidad de dichos paquetes informáticos de la empresa Microsoft. No sólo se castiga al empleado que realizó materialmente la instalación sino a los dos directivos del establecimiento, pues no podía obrar con independencia de las indicaciones de aquellos.

Habitualmente se distingue entre un elemento cualitativo y otro de naturaleza cuantitativa necesarios para la presencia de esta modalidad delictiva. El elemento cualitativo consiste en la identidad relativa entre las obras, copias, por una parte, y original, por otra. De esta identidad entre las obras debe excluirse los casos en los que las obras se refieran a ideas o aportaciones que forman parte del dominio público.

En este sentido se pronuncia la sentencia de la AP de Lugo 31-12-98, relativo a la comercialización de un programa informático de cálculo rápido para efectuar reformas en los vehículos. No existe infracción pues la obra del denunciante forma parte del acervo de conocimientos común a los técnicos en esta materia y su utilización viene a ser consustancial al trabajo técnico de aquellos. Se trataba por tanto de un programa de contenidos de uso constante en aplicaciones prácticas como las llevadas a cabo por el inculpado. No consta acreditada la exclusividad del trabajo del autor, por tratarse de ideas o aportaciones técnicas que han entrado en el dominio público, por lo que el comportamiento no puede poseer entidad penal, sin perjuicio de las acciones que pudieran existir en la vía ordinaria.

164 A. 1850.

El aludido elemento cuantitativo consistirá en la reproducción plural de la obra, aunque no necesariamente masiva o muy numerosa. Queda por tanto como elemento indeterminado que deberán fijar los Tribunales penales en atención a las circunstancias particulares de los casos que lleguen a enjuiciar.

b. La consumación de la modalidad de reproducción se producirá con la mera obtención de las copias, sin necesidad de que se avance más en la cadena comercial (distribución, venta).

Así la sentencia de la AP de Barcelona de 20-6-95[165] estimó delito no consumado cuando lo único que le era imputable al acusado es la posesión de las copias, pero no existe prueba de ningún acto de tráfico o comercialización de las mismas, que si bien puede vulnerar lo dispuesto en el art. 99.2 LPI no entraña el tipo penal reservado para los supuestos más grave. Naturalmente en estos casos lo que sí cabe apreciar es tentativa delictiva que, aunque no de igual manera al delito consumado, sí que resulta punible.

Un caso problemático puede ser la puesta en línea de un programa en un sitio de Internet para la posible copia de quienes tengan acceso al mismo. Este hecho ha sido castigado en Francia como supuesto de reproducción.[166] Resulta, sin embargo, muy complejo admitir como reproducción este supuesto, desde luego no como hecho consumado, en el sentido de programa cargado en el ordenador propio o en el servidor.[167] Únicamente podría verse aquí un acto preparatorio que, a falta de incriminación expresa resulta impune.

Tampoco resulta penalmente relevante desde esta perspectiva el mero uso del programa, sin transferencia estable del mismo.[168] Otra cosa será lo que se pueda decir desde el punto de vista de la conducta de distribución. Incluso en este terreno resultaría proble-

---

165 A. 707.

166 PANSIER/JEZ, *La criminalité sur l´Internet*, PUF, 2000, p. 45.

167 Así entiende la conducta de reproducción en estos casos SEMINARA, S. "La pirateria su Internet e il diritto penale*", Rivista Trimestrale di diritto penale dell´economia* 1,2 (1997), p. 81.

168 En este sentido PICA, G.*, Diritto penale delle Technologie informatiche*, Utet, Torino, 1999, pp. 201-2.

mático la determinación del sujeto activo, pues quien realizaría la copia sería el usuario de Internet y no quien ofrece el programa, quien a lo sumo podría ser calificado como cooperador necesario.

c. La reproducción de obras queda ya excluida como hecho ilícito en la regulación privada en determinados casos. Así no se comprende la introducción del programa en la memoria interna para utilización del usuario (99.3 LPI) ni la copia de seguridad (99.2).[169] Por tanto carecen igualmente de relevancia penal estos comportamientos que ni siquiera la tienen en vía civil.

El problema se presenta de forma más compleja respecto a las copias privadas de programas de ordenador. Como uno de los límites generales a las facultades de explotación de los titulares de los derechos de autor o cesionarios, tradicionalmente se ha mantenido el de la copia para uso privado. De manera que la copia de una obra para mero uso privado se ha excluido generalmente por nuestro ordenamiento jurídico del conjunto de acciones ilícitas contrarias a tal derecho. Así el art. 31.2 LPI permite, con carácter general la reproducción para uso privado del copista.

Sin embargo nos encontramos con que la propia regulación civil excluye de este régimen general el caso de las copias privadas de los programas de ordenador,[170] quizá en atención a esa protección cualificada que desde distintas instancias se quiere dispensar a estas nuevas herramientas que para el desarrollo social de todo tipo representan los programas de ordenador. El art. 99 a) LPI incluye la reproducción total o parcial, incluso para uso personal, como contenido de los derechos de explotación del autor del programa de ordenador. Coherentemente la misma regulación civil (art. 25.3 LPI) señala que no será de aplicación el derecho de remuneración por copias privadas a los programas de ordenador. Con ello queda clara la ilicitud civil de las copias privadas de programas

169 También para el caso francés, PANSIER/JEZ, *La criminalité sur l´Internet*, PUF, 2000, p. 43.

170 PANSIER/JEZ señalan también la prohibición general en la legislación francesa de las copias de uso privado de elementos lógicos, sin autorización del titular de la licencia, incluso con fines meramente pedagógicos. *La criminalité sur l´Internet*, PUF, 2000, pp. 42-3.

de ordenador, pero, sin embargo, no está dicha la última palabra sobre la trascendencia penal de las mismas.

Ya hemos señalado que desde la reforma del Código Penal de 1987 la regulación de los delitos contra la propiedad intelectual dejan de construirse como leyes penales en blanco, conforme a las cuales las conductas prohibidas por la propia norma penal se describen en la regulación extrapenal y no describiéndose de otra manera tales comportamientos, se produce una mayor adherencia a lo previsto en la regulación civil.

Conforme a la regulación vigente la situación cambia. Cuando el propio Código señala las conductas penalmente relevantes, aun cuando resulta necesario tomar como punto de partida las nociones civiles, pues en esa sede es donde nace y se construyen las categorías jurídicas de la propiedad intelectual, todavía es posible efectuar sobre ellas consideraciones jurídico penales relativas a la misión genérica que se asigna el conjunto del Derecho penal y al sentido concreto de la regulación penal de la propiedad intelectual, siempre, naturalmente, con los límites que imponga el precepto penal.

Desde la perspectiva general del Derecho Penal puede señalarse, de acuerdo al principio de subsidiariedad, como poco adecuado el empleo de los medios penales si resultan suficientes para restablecer el Derecho, como en principio parece, los medios menos gravosos para las personas, del Derecho Civil. También dentro de esta misma área general puede entenderse que en realidad estos hechos relativos a una copia para simple uso privado no representan el umbral mínimo de gravedad que exige el principio de fragmentariedad, conforme al cual no cualquier hecho lesivo para un determinado derecho (bien jurídico) tiene cabida en la regulación penal, sino exclusivamente aquellos especialmente lesivos y graves.

En cuanto a aspectos relativos a la concreta incriminación no deja de ser asombroso que la copia privada en general no resulte ilícita ni siquiera civilmente y la de *software* pudiera constituir delito. También se señala como en realidad, incluso de acuerdo a los principios generales del Derecho penal antes mencionados, la relevancia penal de las copias privadas resulta insignificante siendo que el interés penal debería centrarse en los negocios ilícitos masivos de reproducción y distribución de *software*.

El argumento a mi modo de ver definitivo viene dado por las condiciones concretas de la regulación penal. El nuevo Código Penal de 1995 introduce como requisitos generales para la persecución penal de estos hechos que el autor actúe en perjuicio de tercero y con ánimo de lucro, elementos que no se actualizan –al menos de manera suficientemente relevante– para el caso de realización de una copia privada de programa de ordenador.

Semejantes problemas respecto a la copia para uso privado se presentan en otras legislaciones. También en esos casos pese a una regulación poco clara se apunta el criterio del fin de lucro como el que puede aportar la solución. Así PICA[171] estima que la solución interpretativa pasa por el elemento del fin de lucro que se exige en la conducta punible, conforme al cual el autor debe perseguir un enriquecimiento patrimonial en dinero. Así "cualquier manipulación o duplicación del *software* de otro efectuada en el ámbito privado, siendo cedida gratuitamente a terceros, sin fines de lucro o de comercio, es penalmente irrelevante".

2. La conducta penal de distribución

En el ámbito de esta modalidad interesa distinguir entre distribución propiamente dicha y otro supuesto con especial incidencia para lo relativo a los programas de ordenador, que se menciona en la regulación de manera diferenciada pero que cabe asimilar a la distribución.

a. Distribución, *strictu sensu,* según lo dispuesto en el art. 19.1 LPI, cabe entenderla como "puesta a disposición del público del original o de copias de la obra mediante su venta, alquiler, préstamo o de cualquier otra forma".

Entre los requisitos que permiten afirmar la presencia de una conducta penal de distribución se incluyen generalmente los de puesta a disposición de la obra al público, publicidad, identidad entre las obras.

171 *Diritto penale delle Technologie informatiche*, Utet, Torino, 1999, pp. 207 y ss.

La puesta a disposición consistiría en colocar al alcance de los destinatarios, ofrecimiento o puesta en circulación. Así nos encontramos con ofertas de *software* a través de los periódicos o de otros medios publicitarios. La sentencia de la AP de Orense de 16-II-98[172] nos relata un caso de reproducciones de programas de ordenador sobre discos vírgenes para la posterior comercialización mediante un específico apartado de correos abierto a estos efectos. Naturalmente se trataba de una oferta de estos productos a precio muy inferior al de mercado.

De atenernos a una integración literal de la regulación civil podríamos llegar a la conclusión de que el mero ofrecimiento, antes de cualquier inicio de una auténtica distribución, constituye una conducta típica de las que estamos considerando.

Sin embargo, es posible y necesario efectuar algún tipo de consideraciones desde la óptica penal que permitan una adecuación de la comprensión de este comportamiento a la técnica y fines penales.[173] Desde el tratamiento penal general de las conductas, la mera oferta u ofrecimiento del *software* constituye en realidad un acto preparatorio de la conducta típica de distribución. Es decir por su naturaleza, la mera comunicación pública de la posibilidad de conseguir determinados objetos se sitúa como un antecedente material necesario para la posterior y efectiva distribución, pero que todavía no implica un inicio de ejecución de la conducta típica. Incluso la práctica habitual de este tipo de negocios ilícitos se desarrolla de manera que mientras el distribuidor no recibe un pedido efectivo no lleva a cabo la reproducción del *software*. Por todo ello, puede decirse que para el Derecho penal la mera oferta no constituye la realización de la conducta típica de distribución, sino que resulta preciso que se produzca de manera efectiva el envío de la mercancía.

El caso ya mencionado antes de la puesta en línea en Internet de *software* para que, sin licencia, sea copiado por cualquiera incide en la conducta de distribución en este momento. Como se acaba de exponer, el mero ofrecimiento –como constituye la puesta *on*

---

172 A. 523.

173 Véase al respecto GONZÁLEZ GÓMEZ, A., *El tipo básico de los delitos contra la propiedad intelectual*. Tecnos, Madrid, 1998, pp. 174 y ss.

line o un anuncio en un periódico– no realiza plenamente la conducta de distribución. Sin embargo estos hechos pueden ser calificados como tentativa punible pues cabe apreciar un inicio de ejecución del tipo que desborda los actos meramente preparatorios.

La publicidad como requisito de esta conducta se entiende en el sentido de un, en principio, destino generalizado de la obra. Es decir, que tal distribución esté abierta a una pluralidad, al menos hipotética, de destinatarios. Con ello se entienden no abarcados, como señala la regulación civil, supuestos de ofrecimiento en ámbitos restringidos, como sería el doméstico.

La identidad reclama, como requisito general a todas las conductas punibles en este ámbito, la coincidencia sustancial de contenidos entre las obras. La sentencia de la AP de Barcelona de 21-2-90 subraya la necesidad no sólo de identidad material entre las obras sino que la misma se manifieste expresamente en el proceso criminal. Se alude en la misma a unos hechos de distribución de programas de videojuegos semejantes por empresas no titulares de los derechos de explotación. Se afirma en la resolución judicial la ausencia de dolo específico o voluntad defraudatoria. Pero, sobre todo, la absolución se apoya en la no realización de prueba pericial por persona experta en informática que pusiera de relieve las semejanzas para poder hablar de copias. Queda abierta, naturalmente, la posibilidad de acudir a la jurisdicción civil.

b. La distribución en sentido amplio hace referencia a los supuestos de importación, exportación y almacenaje que el legislador incorpora de manera separada en el párrafo segundo del art. 270. Se trata de los únicos comportamientos punibles sin correspondencia inmediata con la regulación de la LPI.

Se entiende que este tipo de conductas se corresponden con conductas de distribución, aunque como actos previos. Así la doctrina señala, como lo hace GIMBERNAT,[174] que el legislador con la

174 GIMBERNAT ORDEIG, E., "Los delitos contra la propiedad intelectual", *Cuadernos de Derecho Judicial*, XV (1995), p. 226. Véase también sobre la vinculación de estas conductas con la de distribución GARCÍA RIVAS, N., en *Comentarios a la Ley de propiedad intelectual* (BERCOVITZ Coordinador), Tecnos, 1997, p. 2385.

referencia a la importación, exportación y almacenaje ha querido incluir en el tipo mediante la técnica de los delitos de peligro abstracto conductas que, en realidad, representan actos preparatorios de las lesiones efectivas de la propiedad intelectual, que se producen con la distribución no autorizada de obras.

La distribución y comunicación pública de programas a través de redes internacionales –de un ordenador a otro rebasando fronteras nacionales– dará lugar a las conductas típicas de importación y exportación.[175] En este ámbito confluyen problemas de aplicación de la ley penal en el espacio y de protección de autores extranjeros no comunitarios de la normativa civil, regulado este último aspecto en los arts. 155 y ss. LPI.

Para todas las modalidades de distribución tal comportamiento se entiende que absorbe la previa reproducción de la obra protegida,[176] pues su desvalor vendría comprendido en el de la acción posterior, en el caso de que sea atribuible a la misma persona.

3. Comunicación pública de la obra como hecho punible

Consiste en la realización de cualquier tipo de actividad que permita el acceso a la obra de una pluralidad de personas sin que medie una distribución material de ejemplares para las mismas. Se debe producir por tanto un acceso a la obra por un conjunto indeterminado de personas, mediante un comportamiento que lo haga posible de manera directa o indirecta, sin que además exista entrega material de la obra.

Se excluye la ilicitud de la conducta ya desde la perspectiva civil cuando la comunicación tiene lugar en ámbitos restringidos como el doméstico no integrado o conectado a una red. En este caso de restricción del ámbito de la ilicitud la exclusión de la antijuricidad de la conducta se traslada automáticamente al campo penal.

---

175 ROMEO CASABONA, C.M., "La protección penal del software en el Derecho español", *Actualidad Penal* 35/1988, p. 1838.

176 GARCÍA RIVAS, N., en *Comentarios a la Ley de propiedad intelectual* (BERCOVITZ Coordinador), Tecnos, 1997, pp. 84-5.

Este concepto civil que se toma como punto de partida se encuentra en el art. 20.1 de la LPI. Por otra parte el número segundo de ese mismo precepto, en su letra i), incluye como específico acto de comunicación pública "el acceso público a bases de datos de ordenador por medio de telecomunicación, cuando éstas incorporen o constituyen obras protegidas", lo que puede –en su caso– tener trascendencia a la hora de su posible inclusión entre los hechos abarcables por la regulación penal.

4. Otras conductas punibles: Transformación, interpretación o ejecución artística

Se puede decir que estamos ante un grupo de conductas accesorias que sobre la base de la obra original la modifican o ponen en práctica para su difusión. Por transformación cabe entender como lo hace el art. 21.1 LPI la traducción, adaptación y cualquier otra modificación de su forma de la que se derive otra obra diferente. En ningún caso es la realizada por el usuario para su uso exclusivo.

La interpretación o ejecución artística también pueden dar lugar a derechos de autor diferentes de los de la obra misma, cuyo titular será el artista ejecutante o intérprete, el director de la interpretación o ejecución o sus cesionarios. Por eso su conculcación puede originar también un hecho punible si estos comportamientos se realizan públicamente sin el consentimiento del titular.

VII. INFRACCIONES MIXTAS

El párrafo tercero del art. 270 castiga un supuesto peculiar: la fabricación, puesta en circulación o tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador. Constituyen así un hecho delictivo esta serie de conductas previas a la lesión misma de la propiedad intelectual sobre programas de ordenador y cuyo objeto material de ataque inmediato en realidad se refiere a los dispositivos técnicos de protección de programas de ordenador.

El origen de la incriminación de esta conducta resulta también peculiar. Esta conducta, incluida en el texto del Código Penal du-

rante la tramitación parlamentaria del mismo, tiene su base en la pretensión de las instancias Comunitarias de dotar de especial protección a los elementos lógicos de los sistemas informáticos, proponiéndose la sanción de estas conductas a los países miembros en la Directiva Comunitaria de 14 de mayo de 1991 (91/250/CEE).[177]

Este hecho delictivo representa por distintos motivos una modalidad de comportamiento punible de carácter excepcional. En primer lugar pues supone el adelantamiento de la protección penal a conductas que no se refieren siquiera al empleo o utilización de estos mecanismos, sino a su mera fabricación, puesta en circulación o tenencia, es decir a momentos siempre previos a lesión alguna de la propiedad intelectual. Se trataría de una modalidad que constituye únicamente un peligro abstracto para la tutela penal de propiedad intelectual, difícil de justificar desde el ángulo del principio de lesividad que preside la construcción del Derecho penal. Por otra parte, se señala cómo esta modalidad tan específica rompe con la sistemática interna de la regulación al referirse a un concreto objeto de propiedad intelectual en las condiciones antes señaladas.[178]

Finalmente esta prohibición posee una mayor amplitud que el ilícito civil (art. 102 letra c LPI) lo que resulta incoherente con la relación característica entre ambos tipos de ilícitos.[179] No resulta acertada la regulación penal superando el radio de acción del ilícito civil al abarcar tanto tenencia como puesta en circulación y fabricación (este último supuesto no previsto en la regulación LPI) de este tipo de desprotectores, cuando además el tipo penal no reclama el fin comercial que debe guiar al autor de los hechos que se exigen en la legislación civil, con el consiguiente ensanchamiento de la zona punible.

---

177 Véase también PICA, G., *Diritto penale delle Technologie informatiche*, Utet, Torino, 1999, p. 194.

178 Así GONZÁLEZ GÓMEZ, A., *El tipo básico de los delitos contra la propiedad intelectual*. Tecnos, Madrid, 1998, pp. 204.

179 En este sentido también JORGE BARREIRO, A., *Comentarios al Código Penal*, Civitas, 1997, p. 775.

En todo caso si parece exigible para la aplicación del supuesto que el medio técnico desprotector de programas posea como única y exclusiva finalidad la de eliminar o evitar los dispositivos de seguridad del programa, excluyéndose entonces aquellos que, además, posean otras funciones o aplicaciones.[180]

VIII. TIPOS AGRAVADOS

Además del tipo básico, en el que se contiene la conducta punible más elemental en relación a los ataques a la propiedad intelectual, ya hemos dicho que la regulación articula otras conductas contra los derechos de autor de carácter agravado.

Los tipos agravados presuponen siempre la concurrencia de los elementos exigidos ya por el tipo básico. Es decir, sólo puede aplicarse si se realizan los requisitos ya previstos en el tipo básico. Además añaden algún elemento o circunstancia particular que les hacen aparecer como hechos de mayor gravedad y que justifica la elevación de la pena asignada al comportamiento.

Suponen por tanto una elevación de la pena a imponer: en nuestro caso la prisión de un año a cuatro años, multa de ocho a veinticuatro meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años. Frente a ello el tipo básico impone la pena de prisión de seis meses a dos años o multa de seis a veinticuatro meses. La diferencia no sólo es de orden cuantitativo, sino visiblemente cualitativa, cuando en el tipo básico la pena privativa de libertad –la más grave del sistema penal– además de inferior en duración no es imprescindible su imposición, sino que resulta alternativa con la de multa. En el caso del tipo agravado la pena de prisión es de obligatoria imposición con independencia de su duración.

Los concretos supuestos agravados se recogen en el art. 271 CP de forma mucho más reducida y simplificada a la regulación anterior. En primer lugar se incluyen entre ellos los casos en los que el

180 GONZÁLEZ GÓMEZ, A., *El tipo básico de los delitos contra la propiedad intelectual*. Tecnos, Madrid, 1998, p. 203.

beneficio obtenido posea especial relevancia económica. Supuestos de evidente naturaleza cuantitativa para el que sin embargo no existen cifras fijas, determinadas por el legislador, sino que esta tarea se abandona a los Tribunales, para que éstos en atención a los hechos concurrentes ponderen su aplicación.

El segundo y último supuesto hacen referencia a que el daño causado revista especial gravedad. De índole aparentemente cualitativa, sin embargo, no deja determinada la naturaleza de la especial gravedad que debe revestir el hecho. Queda descartada la gravedad económica, en cuanto a la cuantía del beneficio económico conseguido con el delito, pues se ha incluido ya en el supuesto anterior. Pudiera, de otra manera, tomarse en consideración a la importancia económica del hecho para la víctima (ruina o grave situación económica). También la trascendencia social del hecho puede apuntar a su posible ataque a intereses colectivos.

SECCIÓN CUARTA

Los medios informáticos en los delitos contra la libertad e indemnidad sexuales de menores e incapaces

El derecho penal relativo a las conductas humanas con significación sexual ha experimentado grandes transformaciones en las dos últimas décadas. Se produce un cambio completo en la sistemática de ordenación de los comportamientos en este grupo de delitos, buscando una mayor coherencia con el nuevo bien jurídico atribuido a este grupo de conductas. Con la reforma introducida mediante la LO 3/1989, de 21 de junio, de actualización del Código penal, los delitos hasta entonces llamados "Delitos contra la honestidad" pasan a constituir los "Delitos contra la libertad sexual". El legislador pretende prescindir totalmente de la naturaleza y significado del acto sexual, tomando como criterio rector únicamente el medio (violencia o intimidación) y la ausencia de consentimiento o los vicios de éste (engaño, prevalimiento) como manifestaciones de la ausencia de libertad de la víctima en su ámbito sexual. Sólo para las agravaciones se toma en cuenta la naturaleza del comportamiento en el ámbito sexual. A través de la reforma mediante la LO 11/1999, de 30 de abril, se incorporan algunas matizaciones

en esta orientación, al hablarse ahora de "Delitos contra la libertad e indemnidad sexuales".

Desde este punto de vista se han producido los mayores logros en el terreno de la regulación de la delincuencia sexual. En lo que afecta a la determinación de las conductas punibles y su reconducción a los principios fundamentales del Derecho Penal (principio de lesividad, principio de intervención mínima, principio de fragmentariedad, etc.), se ha producido una evolución claramente satisfactoria, con contribuciones de la doctrina como las de DÍEZ RIPOLLÉS. Años atrás, en España y fuera de ella, la percepción era bien distinta, de forma que la delimitación de las conductas sexuales que debían ser objeto de castigo representaba el problema más visible. Así, por ejemplo, KLUG[181] trataba justamente de abordar con una metodología más jurídica –sometiendo a las conductas debatidas al análisis de los principios jurídico-constitucionales implicados– y menos emotivista lo que el legislador penal podía disponer en este ámbito y lo que le estaba vedado.

Sin embargo, la justicia criminal en el campo que iniciamos presenta otros aspectos donde la satisfacción no puede sino ser mucho menor, especialmente en lo referente a la criminalidad sexual violenta. Un primer escollo es el de la imputabilidad o capacidad de culpabilidad de los autores de delitos sexuales. Según algunos estudios cerca del 15% de los autores de delitos sexuales pueden ser calificados propiamente como inimputables y un 7% más como semiimputables.[182] Dato nada desdeñable es que un 77% de este tipo de delincuentes tienen antecedentes penales o psiquiátrico-penitenciarios, lo que revela la existencia en todo caso de algún tipo de anomalías psíquicas, al margen ya de la declaración de responsabi-

181 "Problemas filosófico-jurídicos y político-jurídicos del Derecho Penal Sexual". *Problemas de la Filosofía y de la Pragmática del Derecho*. Ed. Alfa, 1989, pp. 107 y ss. Ulrich KLUG aborda el problema con carácter general y en relación a las conductas de prácticas homosexuales, aborto y otro tipo de hechos en el marco de la discusión del proyecto de Código Penal Alemán de 1962.

182 Véase GARCÍA ANDRADE, J.A., *Psiquiatría Criminal Forense*. Centro de Estudios Ramón Areces, 1993, p. 128.

lidad o no del autor.[183] En relación a este problema se presenta otro, cual es el de la respuesta jurídico-penal más adecuada a este tipo de hechos delictivos.

Las consecuencias jurídicas impuestas a los autores de este grupo de hechos son fundamentalmente la privación de libertad y la pena de multa. No parece que en este campo se hayan aportado grandes novedades y se echa en falta una mayor flexibilidad con más altas posibilidades de aplicación de medidas de seguridad con un carácter educativo y terapéutico.[184] No obstante están previstas las posibilidades que otorgan en este campo la regulación de los arts. 95 y ss. del Código Penal. Además se producen dificultades, sobre todo de tipo práctico, en la aplicación en el medio penitenciario del tratamiento al delincuente sexual.[185]

Pasamos ahora a tratar aquellos comportamientos de este grupo delictivo que, desde el punto de vista de los nuevos medios tecnológicos de comunicación y difusión, posean alguna relevancia. Naturalmente no se trata de realizar una exposición exhaustiva de estos comportamientos sino de incidir especialmente en aquellos elementos o aspectos del delito que guarden una mayor relación con el empleo de las nuevas tecnologías. En todos los comportamientos punibles que van a ser objeto de desarrollo aparece como punto en común la figura del menor como víctima del delito. La

---

183 GARCÍA ANDRADE, J.A. *Psiquiatría Criminal Forense*. Centro de Estudios Ramón Areces, 1993, pp. 124 y 140-1.

184 La mayor presencia de estas medidas no está exenta de riesgo, pues como señala KLUG "la entrega incontrolada del paciente social al libre arbitrio de los médicos y psicólogos, por mejor intencionados que ellos sean, conduce finalmente a la arbitrariedad". "Problemas Filosófico-jurídicos y político-jurídicos del Derecho Penal Sexual". *Problemas de la Filosofía y de la Pragmática del Derecho*. Ed. Alfa, 1989, p. 115. Sin embargo en la actual regulación española los límites a estas medidas impiden sustancialmente estos efectos perversos.

185 Los distintos métodos de tratamiento del delincuente sexual en MARSHALL, W.L. *Agresores sexuales*, Ariel, 2001. SCHORSCH, E. Sexualkriminalität, Kleines Kriminologisches Wörterbuch, Heidelberg 1993, pp. 47-6. Véase también GARRIDO GENOVES, V. *Técnicas de Tratamiento para Delincuentes*, Centro de Estudios Ramón Areces, 1993, pp. 233 y ss. También CLEMENTE, M./NÚÑEZ, J. (Coordinadores), *Psicología Jurídica Penitenciaria I*, Fundación Universidad-Empresa, 1997, pp. 257 y ss.

nueva orientación del Derecho penal sexual, conforme a los principios de lesividad e intervención mínima, produce una especial presencia del menor en este campo (al reducirse notablemente la presencia del adulto).

Estamos ante hechos punibles previstos para sujetos pasivos menores o incapaces. Por eso se entiende que se trata de proteger el proceso de formación y maduración de los menores en el ámbito sexual (evolución o desarrollo de su personalidad) frente a conductas que pretenden involucrar al menor o incapaz en actos de naturaleza sexual que pueden incidir negativamente es su indemnidad sexual.

I. DELITOS DE EXHIBICIONISMO Y PROVOCACIÓN SEXUAL (Capítulo IV)

En el ámbito del capítulo IV del grupo delictivo que comentamos se incluyen los delitos de exhibicionismo y provocación sexual, en los que también se manifiesta la nueva orientación legislativa respecto a este campo. La reforma de la Ley LO 5/1988 de 9 de junio sustituyó los anteriores delitos de escándalo público por los de "exhibicionismo y provocación sexual", buscando una mayor certeza y seguridad jurídica en la regulación, así como huir de connotaciones morales en la protección dispensada por el Derecho Penal.

1. Exhibicionismo (art. 185)

En este precepto se castiga la realización de actos exhibicionistas obscenos ante menores o incapaces. Cabe interrogarse sobre su posible vinculación a los medios informáticos.

La conducta del autor puede ser desenvuelta por sí mismo, "Ejecutar por sí" (referencia expresa a la autoría directa) o a través de un tercero ("hacer ejecutar"), referencia legal entendida generalmente como la previsión expresa de la autoría mediata para este comportamiento. En cuanto al contenido de la acción desplegada por el autor, directamente o a través de un tercero, la regulación menciona los actos de exhibición obscena. Elemento que genera cierta indeterminación y no consigue por ello eliminar la vaguedad e imprecisión que pesaba sobre este tipo de conductas. Así se conci-

be generalmente como un elemento normativo del tipo de valoración cultural, es decir, precisado de acudir a las pautas sociales en este terreno para determinar su alcance. En todo caso se entiende que debe concurrir una acción con contenido erótico idónea para lesionar el bien jurídico: la indemnidad sexual de los menores o incapaces. No se trata por tanto de acciones relevantes en sí mismas por su obscenidad o inmoralidad. Igualmente se señala que no necesariamente debe despertar deseos sexuales para que nos encontremos ante la conducta típica.[186]

La regulación parece construida sobre la imagen de un determinado tipo de autor o criminológico: el del exhibicionista. Básicamente se caracteriza por la tendencia a la exhibición de los órganos genitales ante determinadas personas con el fin de alcanzar la propia excitación sexual. Como ya se ha mencionado la conminación penal únicamente alcanza a los supuestos realizados ante menores de edad o incapaces. Es decir, en la actualidad, menores de 18 años. Debe destacarse coherentemente con la naturaleza de los hechos recogidos en el tipo que se castigan en este preciso ámbito los actos realizados ante y no sobre menores.

Como se ha indicado, procede señalar la posible aplicación de este hecho punible a conductas verificadas a través de los medios telemáticos. Las enormes posibilidades que abren este tipo de medios no excluye que los actos de exhibición obscena a los que alude el precepto puedan ejecutarse por estos medios. Por otra parte, la formulación típica de este hecho no parece impedir que, concurrentes actos de exhibición obscena ante menores según el sentido del tipo, resulte aplicable el mismo. No creo que pueda oponerse a tal aplicación el que los hechos deban realizarse ante el menor, en el sentido de una presencia física directa de los sujetos, pues tal interpretación no aparece en el texto y no se desprende del fin de tutela perseguido por esta norma. En estos casos los menores o incapaces únicamente aparecen como sujetos pasivos o víctimas del hecho delictivo.

186 Sobre todos estos aspectos MUÑOZ CONDE, F., *Derecho Penal, Parte Especial*, Tirant lo blanch, 1999, pp. 224 y ss.

2. Difusión o exhibición de material pornográfico entre menores

a. El artículo 186 castiga la puesta en circulación entre menores de material con contenido pornográfico. En el ámbito del art. 186, con relación a los hechos punibles relativos a material pornográfico, el menor únicamente desempeña el papel de víctima o sujeto pasivo del delito. A diferencia de lo que sucede en otros hechos típicos, que veremos a continuación, en los que además se sitúa como protagonista o actor de los objetos calificados como pornográficos.

Las conductas prohibidas se refieren a materiales con contenido pornográfico.[187] El concepto de material pornográfico no deja de –en alguna medida– resultar problemático. En principio tal material se entiende extensible a cualquier tipo de soporte en el que pueda recogerse la producción pornográfica, sea esta escrita, hablada, gráfica (cine, video) o de cualquier otro género, pues en realidad lo decisivo es el contenido y no la forma de presentación a la que la regulación legal no impone ninguna restricción, al menos en cuanto a su naturaleza.

Respecto al contenido del material generalmente se acude a la configuración que del mismo ha realizado la jurisprudencia del Tribunal Supremo de los EE.UU. de Norteamérica. En este sentido CARMONA[188] entiende que se pueden mantener los dos criterios fundamentales elaborados por la mencionada doctrina del TS Americano: que el contenido global de la producción sea de índole exclusivamente libidinoso (encaminado a provocar la excitación sexual, según se señala) y, por otra parte, que carezca por completo de cualquier otro valor justificante (de índole literario, artístico, científico, educativo, etc.).

---

187 DÍEZ RIPOLLÉS habla más que de materiales pornográficos de representaciones pornográficas. *La protección de la libertad sexual*, Bosch, 1985, p.151, lo que a juicio de algunos autores permitiría evitar interpretaciones extensivas. Así MORALES PRATS, F. /GARCÍA ALBERO, R., *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi 1999, p. 279.

188 CARMONA SALGADO, C. *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons, 2000, p. 239. También ORTS BERENGUER, E., *Derecho Penal. Parte Especial*, Tirant lo blanch, 1999, p. 254. MORALES PRATS, F. /GARCÍA ALBERO, R., *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 1999, p. 279.

En relación a estos materiales de contenido pornográfico se castigan conductas que vienen a representar actos de inmediación del material con el sujeto pasivo, es decir posteriores a la elaboración misma del material y de su puesta en circulación, momentos que por tanto resultan excluidos de la tipicidad. La regulación se refiere a la venta, difusión o exhibición de los posibles objetos pornográficos, en situaciones por tanto de inmediación con el destinatario final o intermedio.

b. El problema fundamental para el tema que nos interesa viene representado por la exigencia típica de que el autor obre "por cualquier medio directo" en la conducta de difusión de este tipo de materiales. Para un grupo de autores este requisito tiene como consecuencia ineludible la puesta en contacto directo del autor con la víctima.

El menor o incapaz así como el sujeto activo, según esta orientación, deben estar físicamente presentes en cualquiera de las conductas comprendidas por la prohibición, con una confrontación directa entre ambos.[189] Es decir, que no quedarían abarcadas por la descripción típica las conductas de difusión de material pornográfico cuando se entendiera que estaban dirigidas a un conjunto indeterminado de personas y no a un singular sujeto pasivo, lo que llevaría a excluir conductas como las de exposición al público de pornografía en un Kiosco.[190] También a juicio de alguno de estos autores obliga tal presupuesto a descartar la posibilidad de aplicar el precepto a los hechos que se realicen a través de Internet, como indica TAMARIT,[191] aun a pesar de considerar que estas restricciones podrían no cumplir con las condiciones básicas de protección de los menores en el ámbito internacional.

---

189 CARMONA SALGADO, C., *Compendio de Derecho Penal Español (Parte Especial),* p. 238.

190 MORALES PRATS, F. /GARCÍA ALBERO, R., *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 1999, pp. 278-9. También TAMARIT SUMALLA, J.M., *La protección penal del menor frente al abuso y la explotación sexual*. Aranzadi, 2000, p. 140.

191 TAMARIT SUMALLA, J.M., *La protección penal del menor frente al abuso y la explotación sexual*. Aranzadi, 2000, p.141.

Esta opción tiene su origen en las propuestas de DÍEZ RIPOLLÉS que fueron seguidas por el Código penal de 1995, con la idea de traducir en la configuración legislativa del delito la exclusiva protección de la víctima desde el punto de vista de la libertad sexual del individuo y no tomando en consideración otros aspectos. DÍEZ RIPOLLÉS concibe el conjunto de acciones provocadoras (exhibicionismo y difusión de material pornográfico entre menores) como atentados a la libertad sexual, en sentido estricto, y trata de conseguir una redacción del precepto acorde con ese punto de partida. Así señala este autor: "En realidad lo coherente con el bien jurídico protegido en estos preceptos es penar únicamente la confrontación directa de la víctima con la pornografía…"[192] Estima que no debe castigarse cualquier tipo de acción realizada con objetos pornográficos, "sino exclusivamente la acción que tiende de modo directo a involucrar a otra persona en un contexto sexual… a través de una representación pornográfica".[193]

Cuando se interroga por el bien jurídico protegido en las conductas sexuales provocadoras, estima que, aunque de menor entidad que otras, suponen un "ataque a la libertad de la víctima, en concreto, un menosprecio de su voluntad". "Se tratará de conductas en las que el autor inserta a la víctima en una acción sexual sin su consentimiento… como ocurre en la confrontación no deseada con pornografía…"[194] De todo ello parece deducirse la necesidad de la presencia física de ambos sujetos que permita una efectiva imposición de la voluntad del autor sobre la de la víctima y, por tanto, una genuina lesión de la libertad del sujeto pasivo en el ámbito de su comportamiento sexual.

---

192 DÍEZ RIPOLLÉS, J.L., *La protección de la libertad sexual*, Bosch, 1985, p. 156. Véase también la p. 155 en la que frente a la situación legislativa anterior a la reforma de 1989 señala como posibilidad la de interpretar el "difundir" el material pornográfico como confrontar de modo directo a la víctima con representaciones pornográficas.

193 DÍEZ RIPOLLÉS, J.L., *La protección de la libertad sexual*, Bosch, 1985, p. 151. También, del mismo autor, aunque de manera no tan explícita, en *Exhibicionismo, pornografía y otras conductas sexuales provocadoras*, Bosch, 1982, pp. 391 y ss.

194 DÍEZ RIPOLLÉS, J.L., *La protección de la libertad sexual*, Bosch, 1985, p. 144.

Por ello el autor pasa a examinar la manifestación de voluntad del sujeto pasivo o la configuración de la voluntad de la víctima. Señala que el elemento que hace que una conducta sexual sea desvalorada por el Derecho penal lo constituye la voluntad del sujeto pasivo respecto a la realización de tal acción, lo que debe manifestarse en la redacción del tipo. Las fórmulas tradicionales de la legislación penal española en los delitos que toman en consideración la voluntad del sujeto pasivo, "contra la voluntad" o "sin la voluntad" del mismo, adolecen de ciertas deficiencias por lo que se propone una fórmula mixta que abarque ambos tipos de situaciones e incluso aquellas situaciones en las que no se dé oportunidad a la víctima de manifestar su voluntad: "sin darle oportunidad de manifestar su voluntad, o en contra de ella".[195]

En una obra posterior[196] el autor va a distinguir y proponer tres hipótesis legislativas sobre la configuración de la voluntad de la víctima en estos supuestos: caso de realización de la acción sexual "sin darle a la víctima oportunidad para manifestar su voluntad o en contra de ella", los supuestos en los que en atención a la cualidad del sujeto pasivo se pena con independencia de su manifestación de voluntad y, finalmente, el supuesto de prevalimiento en relación con determinados sujetos pasivos. Considera que las conductas realizadas sobre menores de doce años se incluyen entre los casos previstos con independencia de la manifestación de voluntad de la víctima, mientras que los recaídos sobre sujetos con edades entre los doce y dieciocho años pertenecen a los supuestos de prevalimiento.

Tras la reforma de 1999 en el ámbito de la delincuencia sexual, DÍEZ RIPOLLÉS ha reafirmado su convicción de que la libertad sexual constituye el único bien jurídico que justifica las intervenciones jurídico-penales en las prácticas sexuales de los ciudadanos, incluso en el caso de menores e incapaces. Así señala que "se interviene

195 Hasta aquí las citas y la exposición de este aspecto se refieren a lo señalado por el autor en su obra *Exhibicionismo, pornografía y otras conductas sexuales provocadoras*, Bosch, 1982, pp. 402-413.

196 *La protección de la libertad sexual*, Bosch, 1985, pp. 156-159.

con la pretensión de que toda persona ejerza la actividad sexual en libertad. Ello explica que no haya obstáculo en hablar de que el derecho penal tutela también la libertad sexual de aquellos individuos que no están transitoriamente en condiciones de ejercerla... En suma pasa a ser objeto de atención del derecho penal todas aquellas conductas que involucren a otras personas en acciones sexuales sin su voluntad".[197]

Desde el punto de vista de la protección de la libertad en este ámbito del ser humano, expone este autor la clasificación de las distintas modalidades: conductas que se realizan venciendo la voluntad contraria de la víctima, comportamientos que se realizan contando con un consentimiento viciado de la víctima, conductas que cuentan con un consentimiento inválido de la víctima y, finalmente, conductas sexuales que se realizan sin el consentimiento de la víctima.[198] Entre las conductas con consentimiento inválido se incluirían las sufridas por las víctimas que carecen de la capacidad para comprender el sentido y la trascendencia de su decisión en este ámbito.[199]

Todo este análisis, por sus implicaciones para el tema concreto que nos interesa, debe ser objeto de reconsideración cuando el castigo de la difusión de material pornográfico queda exclusivamente reducido a lo efectuado frente a menores. La presencia de infracciones cuyo único destinatario son los menores obliga a preguntarse si el bien jurídico tutelado lo es todavía la libertad sexual –ahora del menor–. Respecto a ello MUÑOZ CONDE[200] entiende que la libertad sexual queda desplazada en estos casos "…ya no se puede hablar de la libertad sexual como bien jurídico específicamente protegido…, dado que los sujetos pasivos sobre los que recaen son personas que carecen de esa libertad, bien de forma provisional (menores), bien de forma definitiva (incapaces). Si algo caracteriza a las personas

197 "El objeto de protección del nuevo Derecho penal sexual*", Revista de Derecho Penal y Criminología 6 (2000)*, p. 69.

198 "El objeto de protección del nuevo Derecho penal sexual", *Revista de Derecho Penal y Criminología 6 (2000)*, pp. 75 y ss.

199 "El objeto de protección del nuevo Derecho penal sexual", *Revista de Derecho Penal y Criminología 6 (2000)*, pp. 76-78.

200 *Derecho Penal, Parte Especial*, Tirant lo blanch, 1999, p. 196.

que se encuentran en esa situación… es carecer de autonomía para determinar su comportamiento en el ámbito sexual".

De manera, vendrá a indicar el mencionado autor, que se hace necesario acudir a otro fundamento para esta intervención "si se quiere prohibir algo más…, aún sin ser contrarias a la voluntad del afectado, entonces hay que acudir a otros criterios que están más allá de lo que se entiende por libertad sexual. Este es, en definitiva, lo que ha venido a reconocer la nueva rúbrica del Título VIII al incluir la referencia a la indemnidad sexual…". También CARMONA[201] entiende que en el capítulo IV al que estamos haciendo referencia se viene a tutelar un conjunto global de intereses, relativos al ámbito sexual, de los que resulta ser titular el sujeto pasivo menor o incapaz y que pueden reconducirse a la noción general de indemnidad sexual.

Lo que parece cierto es que el sujeto pasivo menor o incapaz introduce una variable distinta de la mera libertad sexual. La propia clasificación que efectúa DÍEZ RIPOLLÉS, incluyendo los supuestos relativos a menores entre los que el legislador no toma en consideración el consentimiento, hace notorio que no es este el fundamento de la incriminación. Si bien a efectos de la clasificación de las distintas modalidades delictivas puede ser útil la referencia al consentimiento, sin embargo, desde el punto de vista del contenido y justificación debe hacer referencia a otros aspectos. Incluso hablar de "consentimiento inválido", como hace DÍEZ RIPOLLÉS, presuponiendo que en todos los supuestos existiría un consentimiento del menor que, sin embargo, la ley no valida, parece hacer entender que en el caso de una voluntad contraria del menor el hecho no sería abarcado de acuerdo a lo previsto en el art. 186. Consecuencia que parece debe ser descartada, pues lo que subyace es una irrelevancia de la voluntad del menor o incapaz, justamente porque se toman en consideración otras perspectivas.

En realidad el propio DÍEZ RIPOLLÉS ha destacado que el Derecho penal sexual –alejándose de concepciones generales de la sexua-

201 *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons, 2000, pp. 232-3.

lidad– debe tutelar únicamente los intereses fundamentales de los ciudadanos que pueden verse afectados por comportamientos con significación sexual, entre los que se encuentra la libertad y –por qué no, se puede añadir– la indemnidad sexual de los menores. De hecho ya hace tiempo la protección de la juventud fue señalada como uno de los bienes jurídicos protegibles en este ámbito. Así KLUG[202] indica que: "Al igual que en el Derecho penal en general, especialmente en el Derecho penal sexual el legislador puede imponer penas sólo allí donde ello es indispensable para la protección de bienes jurídicos reconocidos en general, como en el caso de la protección de la juventud".

Este detenido estudio sobre el bien jurídico para el caso de los menores tiene su fundamento en que la exigencia de que la difusión de material pornográfico se realice a través de un medio directo tiene su anclaje en la pretensión de proteger la libertad sexual del menor, que obliga a verificar un efectivo contraste de voluntades. Siendo más que discutible, e incluso inconveniente, la afirmación de la libertad como objeto jurídico para el caso de menores e incapaces, no se ve la necesidad de que el hecho se desarrolle a través de un medio directo que permita establecer la lesión efectiva de la libertad.

Pero es que incluso atendiéndonos al bien jurídico libertad sexual, y puesto que el precepto lo que hace es apartarse completamente de lo que la voluntad del menor pudiera revelar, tampoco resulta preciso especificar la naturaleza del medio empleado. No se puede entender que se trate de construir el tipo penal sobre la base del contraste de voluntades y la lesión efectiva de la libertad del menor si al tiempo se admite que pertenece al grupo de modalidades de comportamiento en las que el legislador incluye las sufridas por las víctimas que carecen de la capacidad para comprender el sentido y la trascendencia de su decisión en este ámbito.[203]

---

202 "Problemas Filosofico-jurídicos y politico-jurídicos del Derecho Penal Sexual". *Problemas de la Filosofía y de la Pragmática del Derecho.* Ed. Alfa, 1989, pp. 126-7.

203 Lo que sí afirma DÍEZ RIPOLLÉS, J.L., "El objeto de protección del nuevo Derecho penal sexual*", Revista de Derecho Penal y Criminología 6 (2000)*, pp. 76-78.

Incluso la necesaria confrontación a la que se alude puede ser vista de otro modo. No como contraste entre ambos sujetos, sino del sujeto pasivo con el contenido pornográfico del material de que se trate. En este sentido algunas de las expresiones utilizadas por DÍEZ RIPOLLÉS se refieren más a esta posibilidad que a la presencia directa de los dos sujetos en el hecho. Así este autor, como ya se ha tenido ocasión de señalar, entiende que lo coherente con el bien jurídico protegido "… es penar únicamente la confrontación directa de la víctima con la pornografía…"[204] Lo cual resulta más razonable y evita posibles interpretaciones extensivas. Si se admite la perspectiva de la indemnidad sexual del sujeto pasivo como objeto de tutela no cabe duda que se puede alcanzar y dañar la indemnidad sexual del menor por Internet, por ejemplo.

Otras consecuencias que hipotéticamente parecen derivarse de este requisito relativo al empleo de un medio directo tampoco parecen acertadas. Así para algunos autores, como ya se ha manifestado, la difusión del material pornográfico hacia destinatarios inespecíficos excluye la presencia de un medio directo, como sería el caso de Internet o las de exposición al público de pornografía en un Kiosco.[205] Creo que en este punto se producen algunos equívocos errores. Identificar la inmediación o carácter directo del medio con un destinatario preciso no puede estimarse correcto. Pero es que, inversamente, las distintas posibilidades que ofrece Internet permiten, desde luego, la difusión de cualquier contenido hacia masas indeterminadas (páginas *Web*), pero también hacia concretos destinatarios, como sería el caso de mensajes de correo electrónico de contenido pornográfico enviados a determinados menores o comunicación con éstos a través de chats.

---

204 DÍEZ RIPOLLÉS, J.L., *La protección de la libertad sexual*, Bosch, 1985, p. 156. Véase también la p. 155 en la que frente a la situación legislativa anterior a la reforma de 1989 señala como posibilidad la de interpretar el "difundir" el material pornográfico como confrontar de modo directo a la víctima con representaciones pornográficas.

205 MORALES PRATS, F. /GARCÍA ALBERO, R. *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 1999, pp. 278-9. También TAMARIT SUMALLA, J.M. *La protección penal del menor frente al abuso y la explotación sexual*. Aranzadi, 2000, p. 140.

En este sentido ORTS[206] señala que "también puede hablarse de relación directa cuando se utiliza la distribución, difusión o envío a través del correo, incluido el electrónico, u otro procedimiento, por medio del cual se contacta con menores o incapaces, premeditadamente". En realidad ORTS/SUÁREZ-MIRA[207] parece que orientan este elemento en sentido subjetivo al tratarse de un delito de provocación sexual por lo que el mismo no consiste en la oferta de artículos pornográfico a todo el que pueda estar interesado, incluidos los menores, si está ausente el ánimo de involucrarlos en sus designios sexuales. Por ello los comportamientos han de estar encaminados a enredar al menor o incapaz en los planes trazados por el autor con una finalidad sexual. De forma que, señalan estos autores precisando el alcance de este elemento, aunque el carácter directo del medio empleado exigido por el tipo implica un contracto inmediato, una relación personal entre autor y víctima, no se hace preciso la entrega en mano del material por el autor, bastando con que se lo haga llegar. Tampoco es preciso que el sujeto activo conozca al destinatario o que consiga o desee dárselo a una persona concreta, sino que el tipo se cumple también con el envío del material a través de un tercero o cuando la persona siendo indeterminada resulta determinable.

II. CONDUCTAS DE EXPLOTACIÓN SEXUAL RELATIVAS A MENORES O INCAPACES (Capítulo V)

Entre las conductas del capítulo V destacamos aquellas que más estrecha relación poseen con hechos punibles de posible ejecución a través de los medios telemáticos. En éstos el menor o incapaz no sólo constituye el sujeto pasivo de las infracciones sino que alcanza un papel añadido, como es el de objeto sexual de los distintos comportamientos. Se trata de hechos en los que el menor o incapaz como víctima posee una posición singular, en el sentido de la utili-

206 *Derecho Penal. Parte Especial*. Tirant lo blanch, 1999, p. 253.

207 *Los delitos contra la libertad e indemnidad sexuales*, Tirant lo blanch, 2001, pp. 196 y ss.

zación del mismo como objeto sexual frente a terceros. Se produce entonces una explotación del menor en un determinado contexto sexual, en hechos dirigidos al enriquecimiento patrimonial del autor que pueden lesionar la indemnidad sexual del menor o incapaz, aun cuando estos dos últimos aspectos no aparezcan explícitamente en la regulación.

1. Conductas sobre menores o incapaces relativas a materiales pornográficos ("pornografía infantil")

a. En primer lugar podemos señalar los comportamientos relativos al empleo de menores en relación con conductas sobre materiales pornográficos (art. 189.1 letras a y b). Así se castiga la elaboración de los mencionados materiales (art. 189.1 letra a, en su segundo inciso). Estamos en un primer momento de creación del material pornográfico, en el cual se emplean menores o incapaces, previsiblemente para su posterior comercialización por cualquier medio, como sería la Red de redes.[208] Puesto que en la producción de material pornográfico con menores no se ha establecido limitación alguna en cuanto al procedimiento, pueden incluirse la vía informática y cualquier otra que pudiera surgir en el futuro.[209]

En la letra b del mismo precepto se incluye un conjunto de conductas relativas a material pornográfico –en el que intervengan menores o incapaces–, fundamentalmente con carácter posterior a la elaboración del material (excepto la inicial referencia a la producción del material).[210] Así el tipo se refiere a producir, vender,

208 Véase CARMONA SALGADO, C. *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons, 2000, p.249.

209 ORTS BERENGUER, E./SUÁREZ-MIRA RODRÍGUEZ, C. *Los delitos contra la libertad e indemnidad sexuales*, Tirant lo blanch, 2001, p. 254.

210 Esta referencia legal a la producción impide que se pueda aceptar la tesis de RODRÍGUEZ PADRÓN ("Los delitos de utilización de menores o incapaces con fines o espectáculos exhibicionistas o pornográficos o para la elaboración de material pornográfico". *Delitos contra la libertad sexual 21, Estudios de Derecho Judicial*, CGPJ, 1999, pp. 38-39) que entiende que no se incluyen los momentos de producción o creación. En realidad existe ya la previsión de la letra a de mismo precepto que alude a "elaborar", con lo que estamos ante una duplicidad legislativa innecesaria.

exhibir, o facilitar la producción, venta, difusión o exhibición. Las conductas de difusión o exhibición propiamente o las de facilitación de estas mismas conductas serán las que mayor relieve posean respecto a la utilización en Internet de este tipo de materiales, dada la naturaleza de la actividad que se lleva a cabo en la Red. Así se incluyen en este ámbito la difusión de imágenes, sonidos, etc., desde determinados servidores con acceso directo o a través de servidores.[211] También la realización de cualquier material pornográfico en soporte papel, magnético o digital.[212]

En la actualidad se constata el uso con enorme frecuencia de estos nuevos medios para la distribución del material pornográfico y se detecta la evolución que dentro de la propia Red se ha producido en este tipo de actividades.[213] La difusión de pornografía infantil comienza en Internet mediante la creación de páginas web ofreciendo este tipo de material, almacenando todo tipo de material en la misma. Después se pasa a los chats o programas de conversación en los que se produce venta directa por parte de traficantes de pornografía infantil. En la actualidad cada vez se estima más frecuente que sean los propios consumidores de pornografía infantil los que mediante estos mismos chats se comuniquen e intercambien el material, pues resulta más rápido, barato y permiten una mayor adecuación a lo que se busca concretamente.

Por esta mayor relación de las conductas de difusión con la actividad en Internet el CP italiano (art. 600 párrafo tercero) castiga específica y expresamente "al que por cualquier medio, incluso por vía telemática, distribuye, divulga o publica" el material porno-

211 RODRÍGUEZ PADRÓN, C., "Los delitos de utilización de menores o incapaces con fines o espectáculos exhibicionistas o pornográficos o para la elaboración de material pornográfico". *Delitos contra la libertad sexual 21, Estudios de Derecho Judicial*, CGPJ, 1999, p. 39.

212 Así MORALES PRATS, F. /GARCÍA ALBERO, R., *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 1999, p. 288.

213 Véase ROJO GARCÍA, J.C. "Pornografía infantil en Internet". *Boletín Criminológico* 52/2001. Otros aspectos criminológicos sobre materiales pedopornográficos en POMANTE, G., *Internet e Criminalità*, Torino, 1999, pp. 219 y ss.

gráfico (realizado mediante la explotación de menores).[214] También el Ordenamiento Jurídico Británico castiga expresamente la transmisión de material obsceno almacenado electrónicamente, entendiéndose como distribución del mismo la puesta a disposición de los usuarios de Internet de imágenes digitales con este contenido.[215]

Se castiga de manera indiferenciada –lo que puede conllevar problemas desde el punto de vista material– la intervención en la realización de tales comportamientos así como, por otra parte, conductas de mera facilitación de las mismas. Con la pretensión de abarcar todo el ciclo relacionado con el material pornográfico se incluye todos los momentos del mismo, pero además cualquier tipo de intervención en tales hechos, sin que se permita –conforme a las reglas generales de la teoría de la codelincuencia– distinguir entre las conductas propias de los autores y las de los meros partícipes. Desde el punto de vista práctico debería permitir diferenciarse, al menos, el caso de los cómplices, que son los que pueden obtener una respuesta penal menos intensa.

En el ámbito de las conductas relacionadas con material pornográfico en el que se emplean menores o incapaces, se castiga, finalmente, la posesión del material para realizar cualquiera de las conductas descritas anteriormente (párrafo segundo letra b). Por su naturaleza el hecho mismo posesión se corresponde con actos preparatorios con relación a las posteriores conductas de tráfico o venta del material.[216] Con este carácter, por sí mismos, los hechos resultarían impunes, aunque la intervención del legislador incriminando expresamente tal conducta los transforma en punibles, bien que como tipo atenuado frente a la conducta básica.

---

214 Véase ZENO-ZENCOVICH, V. "Il corpo del reato: pornografia minorile, libertad di pensiero e cultura giuridica". *Politica del diritto 4 (1998)*, p. 641. También CORRIAS LUCENTE, G., *Il diritto penale deimezzi di comunicazione di massa*. CEDAM, 2000, p. 266.

215 Véase USTARAN, E. "Pornografía en Internet: la respuesta legal". *La Ley* vol. I (1997), pp. 2130 y ss.

216 En este sentido CARMONA SALGADO, C. *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons, 2000, p. 249.

Hay que tener en cuenta además que la incriminación concreta no castiga simplemente la mera posesión, sino que se refiere "a quien poseyere dicho material para la realización de cualquiera de estas conductas". Se vincula así la posesión a la futura realización de las acciones ya mencionadas con el material pornográfico.[216 bis] Queda todavía pendiente establecer la naturaleza objetiva o subjetiva de esa vinculación entre posesión y posterior tráfico o venta del material. Por otra parte, las dificultades de prueba en esa tendencia de la posesión hacia los posteriores actos se adivinan considerables.

b. En todos los anteriores casos el punto de partida es el del material pornográfico, en este caso concreto la pornografía infantil. Hay que tener en cuenta que en el campo de la pornografía infantil son cada vez más numerosas y concluyentes las declaraciones y compromisos internacionales tendentes a evitar este tipo de explotación sexual, en particular para la difusión de la misma en Internet y desde las instancias europeas.[217] En este sentido el Convenio sobre cyber-criminalidad incluye como uno de los supuestos a castigar en las legislaciones internas de los Estados firmantes distintas conductas relativas a la pornografía infantil (art. 9).[218]

En algunos casos puede resultar problemático la precisa determinación del concepto de pornografía infantil, en especial, con el avance de las técnicas de producción de material visual, en lo referente a la llamada "pornografía técnica" que en algunos países se tiende a criminalizar.[219]

---

216 bis Por eso no se hace preciso distinguir entre el mero acceso a Internet y el construirse un archivo propio para uso particular, frente a lo señalado por MARTÍN-CASALLO LÓPEZ, J., "Internet y pornografía infantil", Actualidad Informática Avanzada, 10/2001, pp. 6-7.

217 Así la Decisión CE 2000/375/JAI de 29 mayo 2000, relativa a la lucha contra la pornografía infantil en Internet (DOCE 9 junio 2000). Sobre este tema en general DE LA CUESTA ARZAMENDI, J.L., "Las nuevas corrientes internacionales en materia de persecución de delitos sexuales a la luz de los documentos de organismos internacionales y europeos". Delitos contra la libertad sexual 21. Estudios de Derecho Judicial, CGPJ, 1999, pp. 323 y ss.

218 Convenio redactado en el marco del Consejo de Europa y pendiente de ratificación por los Estados.

219 MORALES PRATS, F. "Pornografía infantil e Internet: la respuesta en el Código penal español". *Problemática jurídica en torno al fenómeno de internet*. Cuadernos de Derecho Judicial, IV/2000, p. 199.

Existe acuerdo generalmente en cuanto a que el material pornográfico debe determinarse por su contenido exento de cualquier otro valor literario, artístico, científico, pedagógico, etc., y dominado fundamentalmente por una dirección que persigue la excitación o satisfacción del instinto sexual.[220] En la llamada pornografía infantil o de menores, el material en que se realice debe contar con la presencia de algún menor con los contenidos antes señalados. Ocurre que en la denominada "pornografía técnica" los procedimientos técnicos permiten incorporar con el mencionado sentido pornográfico a mayores con apariencia de menores (mediante fotografías o imágenes superpuestas o retocadas, utilizando elementos propios de menores –como ropa– sobre los mayores, etcétera).

MORALES[221] señala que la incriminación no alcanza estos supuestos de mayores que se hacen pasar por menores en su utilización en el material pornográfico, pues no basta que se trate de pornografía relativa o alusiva a menores, sino que la tutela penal se asienta sobre la idea de utilización del menor. En este sentido, se podría hablar de una falta de lesividad de estas conductas.[222] Sin embargo, este autor, entiende que en los casos de inserción de imágenes de menores reales en escenas pornográficas en las que realmente no ha participado *sí* existe tal utilización del menor que permite estimar punible la conducta.

Esta posición, para el caso de menores reales que se utilizan posteriormente para la producción de material pornográfico sin participación del menor en el contexto sexual, resulta problemática. Se trata entonces de casos en los que se incluye al menor en el material pornográfico desde fuera, sin participar propiamente en su desarrollo y sin que necesariamente se vea afectado por los con-

---

220 ORTS BERENGUER, E./SUÁREZ, *Los delitos contra la libertad e indemnidad sexuales*. Tirant lo blanch, Valencia, 2001, p. 255.

221 "Pornografía infantil e Internet: la respuesta en el Código penal español". *Problemática jurídica en torno al fenómeno de internet*. Cuadernos de Derecho Judicial, IV/2000, pp. 187-8.

222 MORALES PRATS, F. "Pornografía infantil e Internet: la respuesta en el Código penal español". *Problemática jurídica en torno al fenómeno de internet*. Cuadernos de Derecho Judicial, IV/2000, p. 199.

tenidos pornográficos. Entiendo que el bien jurídico tutelado de la indemnidad sexual de ese menor no necesariamente se ve dañado, pues el menor por si mismo –que es la conducta que realmente le afecta– no constituye ese material pornográfico, sino que posteriormente se produce su inclusión en tal material.

Deben en este sentido descartarse los casos en los que el hecho total se escinda claramente en dos partes, una la obtención de imágenes o cualquiera otros aspectos del menor y otra la confección o realización del material, sin que además conozca su utilización en tal producción pornográfica. Más dudosos, como afirman ORTS/SUÁREZ-MIRA,[223] serán los casos en los que el menor sea advertido de su utilización para tal material. De todas formas, como ya se ha mencionado, toda esta materia está cada vez más vinculada a los compromisos internacionales de los Estados que repercutirán en la solución legislativa. Así el Convenido sobre cyber-criminalidad incluye entre los hechos que los Estados firmantes deben recoger en su legislación interna la representación visual de una persona que aparezca como un menor desarrollando un comportamiento sexual explícito.[224]

Otro aspecto es el de la posible relación concursal de estos hechos con los delitos contra la intimidad. Este problema se plantea con ocasión de la discusión sobre el tratamiento jurídico-penal de la elaboración de material pornográfico con menores, ante la duda –anterior a la reforma de 1999–, sobre su inclusión en los supuestos típicos de los delitos contra la libertad sexual en la primera redacción de éstos en el Código penal de 1995.

MORALES,[225] ya después de la mencionada reforma, distingue, dos posibilidades para el caso de producción del citado material. Si

223 *Los delitos contra la libertad e indemnidad sexuales*. Tirant lo blanch, Valencia, 2001, p. 255 nota 122.

224 Letra b) del art. 9.2 del Convenio del Consejo de Europa todavía pendiente de ratificación por los Estados.

225 "Pornografía infantil e Internet: la respuesta en el Código penal español". *Problemática jurídica en torno al fenómeno de internet*. Cuadernos de Derecho Judicial, IV/2000, pp. 189 y ss.

el menor no advierte el uso pornográfico del material con él realizado (utilización clandestina del menor), su incriminación debería realizarse –según propone este autor– a través de lo regulado en el número 5 del art. 197 CP como hecho punible atentatorio a la intimidad del menor. Esta opción descarta, creo que acertadamente y en coherencia con lo aquí señalado para la pornografía técnica, que la utilización no conocida por el menor pueda menoscabar su indemnidad sexual.

Sin embargo, por otra parte, mayores dificultades va a presentar la aplicación de los delitos contra la intimidad cuya regulación expresamente requiere que el autor actúe con un especial elemento subjetivo del injusto: "El que, para descubrir los secretos o vulnerar la intimidad de otro…" Esta particular finalidad del hecho no parece en principio compatible con lo que podría considerarse –inicialmente– como una finalidad económico-pornográfica de quien realiza este tipo de comportamientos.

c. Un último inciso introduce una especificidad en cuanto al ámbito espacial alcanzado por esta conducta, lo que posee una gran trascendencia para los hechos cometidos a través de redes de telecomunicación. La regulación señala como punible esta conducta incluso cuando "el material tuviera su origen en el extranjero o fuere desconocido", según la redacción que incorpora la LO 11/1999, de 30 de abril. Aparece así la pretensión del legislador de evitar problemas de aplicación de la ley penal a hechos cometidos fuera de nuestras fronteras, a través de la introducción de este inciso que constituiría una auténtica excepción al principio de territorialidad, que con carácter general rige la aplicación de la ley penal española.

La propia exposición de motivos de la mencionada reforma de 1999 señala la trascendencia de esta nueva regulación para la competencia de los Tribunales penales: "el Consejo de la Unión Europea, sobre la base del art. K.3 del Tratado de la Unión Europea ha adoptado, el día 29 de noviembre de 1996, una acción común relativa a la lucha contra la trata de seres humanos y la explotación sexual de los niños como consecuencia de la cual los Estados miembros se comprometen a revisar la legislación nacional vigente relativa, entre otros extremos, a la explotación sexual o abusos sexuales cometidos con niños y a la trata de niños con fines de explota-

ción o abuso sexual, considerando tales conductas como infracciones penales, previendo para las mismas penas eficaces, proporcionadas o disuasorias, y *ampliando los fundamentos de la competencia de los Tribunales propios más allá del estricto principio de territorialidad*".[226]

Esta pretensión lleva incluso hasta la reforma de la LOPJ en lo relativo a la exigencia del principio de doble incriminación para facilitar la persecución de estos hechos,[227] lo que también se refleja en la exposición de motivos ya recordada. Siendo ésta la pretensión del legislador de 1999, sin embargo puede que encuentre algunos problemas en la realización práctica de la misma. La redacción dada al precepto se refiere a la excepción mencionada con la expresión "aunque el material tuviere su origen en el extranjero o fuere desconocido". Se refiere, por tanto, el legislador al origen del material y no tanto a la realización misma de las conductas punibles. Es decir que el origen del material no determina la competencia más que para el caso de producción del mismo, pero lo relevante para la venta, distribución, difusión o exhibición es el lugar desde el que se lleva a cabo tales conductas.[228] Ello salvo que se quiera entender que el origen del material es lo mismo que el lugar de la venta del material, el lugar de exhibición del material, etc.

---

226 La cursiva del último inciso del texto entrecomillado es nuestra, pues se quiere destacar especialmente lo relativo a la superación del principio de territorialidad en este ámbito.

227 Nueva redacción del art. 23 LOPJ de acuerdo a la disposición final única de la LO 11/1999, de 30 de abril.

228 Por eso mismo no representa dificultad alguna el que se puedan perseguir hechos relativos a un material de origen desconocido, como sí afirma RODRÍGUEZ PADRÓN, C., "Los delitos de utilización de menores o incapaces con fines o espectáculos exhibicionistas o pornográficos o para la elaboración de material pornográfico". *Delitos contra la libertad sexual 21, Estudios de Derecho Judicial*, CGPJ, 1999, p. 39. Si el origen resulta desconocido, pero su exhibición o difusión se ha detectado, esto último constituye por sí mismo una de las conductas incriminadas.

2. Participación con fines o en espectáculos exhibicionistas o pornográficos de menores o incapaces

También se castiga la utilización de menores o incapaces con fines o en espectáculos exhibicionistas o pornográficos (art. 189.1 en su letra a). Ahora ya no se trata de conductas relativas a la elaboración o tráfico con determinados materiales calificados de pornográficos, sino de hechos al margen de la realización o comercialización de tales materiales. Por ello cabe la inclusión de espectáculos o representaciones exhibicionistas o pornográficas de menores en directo a través de las redes de telecomunicación, supuestos en los que no cabría entender presente la realización o exhibición de ningún tipo de material. Supone esta incriminación la utilización de menores o incapaces "con fines o en espectáculos exhibicionistas o pornográficos". Lo relevante por tanto es la instrumentalización del menor o incapaz en un determinado contexto exhibicionista o pornográfico, no necesariamente en un espectáculo, pues la referencia a "con fines o en espectáculos" admite otras posibilidades.

La calificación como exhibicionista o pornográfico del contexto en el que se inserta al menor o incapaz puede realizarse con los mismo criterios señalados para los supuestos de los arts. 185 y 186. En todo caso parece que la tipicidad de la conducta no depende exclusivamente del papel que directamente juegue el incapaz o menor en el espectáculo, sino de una valoración de conjunto del hecho en atención al bien jurídico protegido. En este sentido MORALES/GARCÍA ALBERO[229] señalan la ausencia de determinación legal sobre el grado de implicación que cabe exigir del menor, entendiendo que no se limita la punición a los casos en los que el menor es parte activa de conductas de contenido obsceno. La regulación señala la indiferencia respecto al carácter público o privado de la actividad en la que de alguna manera participa el sujeto pasivo, es decir, no es relevante típicamente que el acceso sea abierto o restringido a las conductas realizadas por menores o incapaces.

229 MORALES PRATS, F. /GARCÍA ALBERO, R., *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 1999, p. 289.

Por último, tras la reforma de 1999, es posible aplicar a este tipo de hechos el reintroducido delito de corrupción de menores. El mencionado tipo del art. 189.3, como formulación genérica y residual de los posibles ataques a la indemnidad sexual de los menores, aparece como posible destinatario de aquellas conductas que por distintos motivos no encuentren fácil acomodo en los tipos que venimos comentando. El hecho punible consiste en este caso en hacer participar al menor o incapaz en un comportamiento de naturaleza sexual que perjudique la evolución o el desarrollo de la personalidad del mismo. Tan amplia formulación ha encontrado enseguida críticas por su falta de precisión y la difícil calculabilidad de las conductas a las que puede afectar,[230] de forma que ORTS/SUÁREZ MIRA[231] llegan a decir que se trata de un tipo penal del que "se lo mire por donde se lo mire, nada bueno puede decirse".

III. ELEMENTOS TÍPICOS GENERALES

En este último apartado relativo a los delitos contra la libertad e indemnidad sexuales, nos referimos sintéticamente, a aquellos elementos que se presentan en la tipicidad de todos los comportamientos punibles ya descritos, o bien, sin ser elementos típicos en sentido estricto resultan extensibles a cada una de las conductas que hemos expuesto precedentemente.

Empezando por los mencionados en primer lugar, el tratamiento unitario de los elementos constantes en los diversos comportamientos punibles objeto de nuestra atención nos evita la repetición de su exposición. Entre los aspectos válidos para todos los hechos punibles que nos interesan en este ámbito, vamos a señalar funda-

230 Sobre ello GARCÍA ALBERO, R., "El nuevo delito de corrupción de menores". *Delitos contra la libertad sexual 21, Estudios de Derecho Judicial*, CGPJ, 1999, pp. 111 y ss. También DÍEZ RIPOLLÉS, J.L., "El objeto de protección del nuevo Derecho penal sexual", Revista de Derecho Penal y Criminología 6 (2000), p. 88. RODRÍGUEZ PADRÓN, C. "Los delitos de utilización de menores o incapaces con fines o espectáculos exhibicionistas o pornográficos o para la elaboración de material pornográfico". *Delitos contra la libertad sexual 21, Estudios de Derecho Judicial*, CGPJ, 1999, pp. 42 y ss.

231 *Los delitos contra la libertad e indemnidad sexuales*, Tirant lo blanch, 2001, p. 260.

mentalmente lo concerniente a la exigencia de que los hechos hagan referencia a un menor o incapaz, los posibles problemas en torno al error sobre la edad o incapacidad de la víctima por parte del autor y la pretensión de incorporar a los tipos determinados aspectos subjetivos no previstos legalmente.

La exigencia legal de un determinado sujeto pasivo hace que como víctimas de estos hechos sólo puedan considerarse a los menores de edad penal y a los incapaces. La minoría de edad penal, tras la entrada en vigor de la Ley de responsabilidad penal del menor se ha situado en los dieciocho años –en un sentido puramente biológico o cronológico–, coincidentemente con la mayoría de edad civil. En definitiva todas las conductas estudiadas tienen como destinatarios los menores o incapaces, como sujeto pasivo o, además, como objeto sexual frente a terceros.

La presencia del menor o incapaz hace que se suscite un nuevo problema, cual es el del conocimiento que deba poseer el autor sobre este extremo y las posibles consecuencias ante un hipotético error del autor en cuanto a la edad o incapacidad de la víctima. Como se trata de delitos dolosos, es exigible que el autor conozca y quiera la realización de los elementos objetivos de los tipos a los que nos referimos, entre los que se encuentra el estado de minoría de edad o de incapacidad de la víctima. La confusión del autor, que estima lleva a cabo el comportamiento ante o sobre un mayor de edad, cuando, en realidad, es un menor o, bien, estimando normal a la persona, resulta que es un incapaz, en principio, hace aparecer un error de tipo. Conforme a la regulación legal si se aprecia un error vencible (de tipo), el hecho es punible en su forma imprudente (art. 14.1 CP), que como no resulta admitida en este caso, provoca la impunidad del hecho.[232] Igualmente el error invencible aboca a la exclusión de cualquier tipo de responsabilidad penal.

En la práctica, puede ser habitual que el autor no preste excesiva atención a la edad del sujeto pasivo, por lo que se planteará la admisibilidad del dolo eventual a estos casos. Cabe entender en

232 En parte esto es lo sucedido en el caso Arny –sentencia AP Sevilla de 19 de marzo de 1998.

este ámbito que este tipo de hechos cometidos a través de medios de una gran potencialidad de difusión el autor no deja de aceptar la alta probabilidad del acceso de menores o incapaces a los contenidos, con lo que podría afirmarse la comisión de un hecho doloso, en su modalidad de dolo eventual.[233] Aun con ello no dejarán de presentarse dudas sobre este aspecto.

Como elemento subjetivo adicional, al menos para el caso de las conductas provocadoras, se exige por algunos autores la tendencia del autor a involucrar al menor o incapaz en un determinado contexto sexual (tendencia provocadora), sin ningún tipo de respaldo directo o indirecto de la redacción del tipo. Así DÍEZ RIPOLLÉS[234] o MUÑOZ CONDE[235] incluyen este elemento complementario caracterizado como un particular elemento subjetivo del injusto que, pretendidamente, permite dotar al tipo de una ulterior restricción. CARMONA,[236] sin embargo, estima que se trataría de un elemento innecesario.

SECCIÓN QUINTA

Protección penal de la intimidad informática

I. INTRODUCCIÓN

Con el Código penal de 1995 se observa ya la protección específica que el legislador otorga a la intimidad de las personas. Incluso dentro de esta tutela penal de la intimidad del Título X ("Delitos contra la intimidad, el derecho a la propia imagen y la inviolabili-

233 TAMARIT SUMALLA, J.M., *La protección penal del menor frente al abuso y la explotación sexual*. Aranzadi, 2000, p. 140. Autor que, como se ha mencionado no estima punibles, al menos con carácter general, los hechos cometidos a través de Internet en este ámbito.

234 *Exhibicionismo, pornografía y otras conductas sexuales provocadoras*, Bosch, 1982, pp. 497 y ss.

235 *Derecho Penal, Parte Especial*, Tirant lo blanch, 1999, pp. 225 y ss.

236 CARMONA SALGADO, C., *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons, 2000, p. 239.

dad del domicilio"), puede hablarse de una atención particularizada a la intimidad afectada por medios informáticos electrónicos y telemáticos. En el art. 197 el legislador de 1995 ha incorporado distintas referencias a los datos y comunicaciones contenidos en soportes informáticos, electrónicos o telemáticos, en lo que se entiende –en sentido amplio– como tutela penal de la intimidad informática. Se trata de delitos contra la intimidad de las personas mediante el uso de la informática (comprende el acceso o manipulación de datos reservados registrados en soportes informáticos u otros, la interceptación de las telecomunicaciones y el apoderamiento de mensajes de correo electrónico).

La regulación referente a la intimidad informática se contiene en el art. 197 del Código Penal, de la forma que luego se verá. Encontramos ámbitos conexos con ataques a la intimidad con participación de elementos electrónicos en el número primero y segundo del mismo precepto, por lo que será preciso abordar y distinguir todas las modalidades que de distintas maneras enlacen con la tutela penal de la intimidad informática. Por otra parte no conviene olvidar la confluencia en alguna medida de la regulación administrativa de esta materia a través de la nueva Ley de Protección de Datos Personales.[237]

Hoy se entiende que la intimidad y su tutela jurídica se corresponde con dos grandes bloques.[238] En primer lugar hace referencia a aquellas facultades jurídicas que le proporcionan al titular la capacidad de excluir a terceros de determinados ámbitos a los que se extiende la intimidad de la persona. Así los supuestos relativos al

---

237 Ley orgánica 15/1999, de 13 de diciembre. Sobre ella puede verse el trabajo de TÉLLEZ AGUILERA, A., *Nuevas Tecnologías. Intimnidad y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*. Edisofern, 2001.

238 Desarrollado fundamentalmente en nuestra doctrina jurídico-penal por MORALES PRATS, F., La tutela penal de la intimidad: privacy e informática, Ediciones Destino, 1984, pp. 45 y ss. También en *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 1999, pp. 336 y ss. También MARCHENA GÓMEZ, M. "Intimidad e informática: la protección jurisdiccional del *habeas data". Boletín de Información. Ministerio de Justicia e Interior nº 1768 (1996)*, pp. 742 y ss. En la doctrina italiana una referencia a estos aspectos en PICA, G. *Diritto penale delle technologie informatiche*, Utet, Torino, 1999, p. 5.

acceso a los secretos documentales, la interceptación de telecomunicaciones, el control ilícito de sonido o imagen de las personas o el allanamiento de morada se entienden como violación de esas facultades de exclusión frente a terceros en determinados espacios jurídicos de carácter restringido.

Pero además hoy también se considera que la intimidad proporciona en determinados casos, singularmente los que afectan a datos obrantes en sistemas informáticos, poderes de control sobre determinados datos y aspectos relativos a la intimidad de las personas. La eclosión en la sociedad moderna de los sistemas informáticos y las enormes potencialidades lesivas para la intimidad de las personas aconsejan que en este territorio se disponga de mecanismos jurídicos apropiados para conocer y vigilar los datos de las personas contenidos en ficheros o archivos automatizados. A este segundo bloque pertenece la regulación del número segundo del art. 197, en cuanto castiga distintas conductas relacionadas con abusos sobre datos personales incluidos en ficheros automatizados.

La potencialidad lesiva para los ámbitos reservados de las personas que generan los medios informáticos es tan importante que hace preguntarnos si no estaremos camino de convertirnos en "ciudadanos transparentes" en muchas facetas de nuestra vida.[239]

Corresponde ahora ver en concreto cómo se tutela en las distintas modalidades de comportamientos previstas en la intimidad informática. Distinguiremos en el conjunto del capítulo I del Título XI los supuestos relativos a los secretos documentales, la interceptación de telecomunicaciones y, sobre todo, los supuestos de privacidad informática con relación a los ficheros automatizados.

II. PROTECCIÓN DE LA INTIMIDAD INFORMÁTICA EN CUANTO SECRETOS DOCUMENTALES

En el contexto del Capítulo I del Título X se castigan las acciones de apoderamiento de documentos o efectos personales lleva-

239 ROMEO CASABONA, C. M., *Poder informático y Seguridad Jurídica*, Fudesco, 1987.

dos a cabo por el autor para descubrir los secretos o vulnerar la intimidad de otro. Entre los posibles objetos de apoderamiento que pueden lesionar la intimidad del sujeto pasivo se menciona expresamente por el legislador los mensajes de correo electrónico. La incorporación de este particular objeto fue consecuencia de una enmienda del Grupo Parlamentario de CiU en la tramitación parlamentaria del Proyecto de Código Penal, sumándose a los otros objetos ya enumerados, con la justificación de "Proteger el cada vez más extendido correo electrónico".[240]

La perspectiva de este primer inciso del art. 197 es la de la tutela de aspectos de la intimidad recogidos documentalmente o en efectos personales. Así el legislador ejemplifica con "papeles, cartas, mensajes de correo electrónico" y finaliza la referencia al objeto material del delito con una fórmula genérica de recogida –"o cualesquiera otros documentos o efectos personales"– en la que se manifiesta la concreta dimensión de la intimidad a la que afecta la conducta punible.

1. El apoderamiento documental

La acción del sujeto activo sobre los elementos documentales o personales que guardan relación con la intimidad se describe como un apoderamiento. De acuerdo a las características de los elementos y documentos como el correo electrónico resulta complejo una absoluta identificación de esta conducta con la de los clásicos delitos de apoderamiento en el campo patrimonial.[241]

Hay que tener en cuenta que –dada la naturaleza de los elementos informáticos fácilmente repetibles– no siempre se producirá la desposesión del titular del mensaje o documento, lo que no es óbice alguno pues el bien jurídico no es la propiedad sino la intimidad, que ya resulta menoscabada con la aprehensión del objeto. En el ámbito de los delitos contra la propiedad la desposesión viene

240 *Ley Orgánica del Código Penal. Trabajos Parlamentarios, vol I*, Cortes Generales, 1996, p. 299.

241 Véase sobre estos aspectos MATA y MARTÍN, R.M., *El delito de robo con fuerza en las cosas*, Tirant lo blanch, 1995, pp. 198 y ss. y 140 y ss.

demandada por el hecho de que la lesión del bien jurídico consiste en la privación al titular del bien del conjunto de facultades jurídico-económicas que el Ordenamiento Jurídico le atribuye sobre el objeto. Sin tal desposesión queda claro que no puede darse el menoscabo efectivo del bien jurídico. En lo concerniente a la intimidad, sin embargo, basta con la apropiación del contenido para que la misma se vea menoscabada.

Lo que sí parece requerir en definitiva el apoderamiento en este campo de la intimidad es algún tipo de materialización instrumental del mensaje de correo electrónico o del objeto de que se trate, de forma que permita al autor la aprehensión del mismo. Con ello se excluyen del ámbito de la tipicidad las conductas que no lleven asociadas algún tipo de materialización.

Desde la perspectiva de este primer inciso del número primero del art. 197, el de los secretos o aspectos de la intimidad documentalmente recogidos, resulta coherente la exigencia de un plus en la acción delictiva, como representa la apropiación del documento o efecto personal. Este plus, que puede entenderse como el desvalor de acción específico del comportamiento, se correspondería con el exigido en el caso del control audiovisual ilícito (art. 197.2 segundo inciso) cuando se requiere legalmente el empleo de medios técnicos en las conductas relativas al sonido o imagen ajenos. Por ello no puede incluirse en el tipo que estamos analizando los comportamientos de mera captación intelectual del mensaje de correo electrónico, visualizado en pantalla, como –sin embargo– si admiten MORALES[242] y SEGRELLES.[243] Paralelamente en el supuesto ya indicado del control audiovisual punible tampoco resulta típico el escuchar una conversación privada parapetado detrás de una puerta.[244]

Si que resultan abarcadas por el tipo, para las conductas que en concreto nos interesan, la impresión del mensaje de correo electró-

242 En *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 1999, p. 339.

243 SEGRELLES DE ARENAZA, I., En *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons, 2000, p. 275.

244 Así MUÑOZ CONDE, F., *Derecho Penal, Parte Especial*, Tirant lo blanch, 1999, p. 247.

nico, apoderándose el autor del contenido mediante esa conversión a papel del mensaje. También puede considerarse incluida la grabación del mensaje en un diskette que le permita posteriormente al autor acceder a su contenido. En ambos casos se produce esa cierta materialización del contenido que exigiría la acción de apoderamiento documental en este primer inciso del art. 197.1.

2. Otras exigencias típicas

Naturalmente el apoderamiento de mensajes de correo electrónico, en el sentido indicado, debe hacer referencia a mensajes con contenido secreto o referencias a la intimidad de las personas para que puedan estimarse como objeto material de este hecho punible. En sentido subjetivo, además, el tipo precisa que el autor que se apodera del objeto en el que determinados contenidos afectan a la intimidad, debe actuar con la intención de descubrir tales secretos o vulnerar la intimidad. Otros fines perseguidos por el autor dejan fuera de la tipicidad esta clase de apoderamientos de mensajes de correo electrónico o de cualquier otro documento, incluso aunque desde el punto de vista objetivo, dado el contenido, puedan peligrar o lesionar los secretos o la intimidad de alguien.

En todo caso, pese a la finalidad exigida al autor, sin embargo, no se requiere desde el punto de vista objetivo que efectivamente se lesione la intimidad o se descubran determinados secretos. Es decir, se produce la consumación de la conducta del art. 197.1 con la acción de apoderamiento del documento o efecto personal en el que se contienen datos secretos o íntimos, sin necesidad de ulteriores consecuencias como la de una auténtica vulneración de la intimidad o real descubrimiento del secreto. O lo que es lo mismo sin que sea preceptivo que el sujeto activo llegue al conocimiento del contenido del mensaje o documento.

Por eso cabe calificar estos hechos delictivos como delitos de peligro, pues no exigen sino la amenaza al bien jurídico y no el menoscabo real. Este sería el caso, por ejemplo, de quien se apodera de un mensaje de correo electrónico cifrado por lo que finalmente no puede llegar a conocer lo contenido en el mismo. El delito ha rebasado la mera tentativa y ha llegado a la fase de consumación pues se ha producido el peligro para la intimidad requerido por el

tipo. Menos aún resulta necesario que, una vez conocido el contenido íntimo o secreto, tales aspectos se difundan o trasladen a terceros. Esta situación es objeto de un plus punitivo conforme a lo previsto en el número tercero del art. 197 del CP: "Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos…"

III. INTERCEPTACIÓN DE LAS TELECOMUNICACIONES

En un segundo momento de la descripción de las conductas punibles en el art. 197 se prohíbe y castiga la interceptación de telecomunicaciones. También la intimidad puede verse quebrantada mediante la intromisión ilegítima en los modernos medios de telecomunicación, entre los que se pueden incluir los informáticos, como el correo electrónico. Desde 1994 la original redacción vinculada a las comunicaciones telefónicas se amplía a "cualquier otra señal de comunicación", con lo que el tipo abarca todo tipo de telecomunicaciones.

La interceptación, en cuanto acción típica, se entiende en este ámbito como acceso ilícito al contenido de la comunicación. No se trata, como impone una interpretación teleológica en atención al bien jurídico, de una obstaculización de la comunicación –que nada tiene que ver con la tutela de la intimidad–. Como señala POLAINO estamos ante una interceptación de indiscreción y no ante una interceptación de obstrucción.

Dada la naturaleza de los medios tecnológicos empleados en las modernas telecomunicaciones se presenta como presupuesto necesario el empleo por el autor de medios técnicos que permitan el acceso al contenido de tales comunicaciones. Aun cuando la profusa redacción del número primero del art. 197 pudiera hacer pensar que la exigencia de utilización de "artificios técnicos" únicamente se refiere a las conductas de control ilícito del sonido o imagen, sin embargo, resulta incuestionable la presencia de los mecanismos de acceso a las telecomunicaciones en la conducta punible, aunque sólo fuera como presupuesto fáctico.

En contra de entender el empleo de instrumental técnico como una exigencia típica se ha manifestado SEGRELLES,[245] incluso para el supuesto de captación o reproducción de imágenes o sonidos. El problema está –según este autor– en la confusión entre la intimidad en sí con la percepción de la misma por terceros, lo que se realiza a través de señales. El legislador protege la intimidad, cualquiera sea la señal por la que se pueda manifestar. Entiende que el último inciso del art. 197.1 admite la punición de la percepción de comunicaciones sin ayuda de medios técnicos.

Es verdad que como señala este autor el legislador protege la intimidad propia de cualquier tipo de comunicación, por lo que no exige que ésta se produzca a través de medios técnicos –al menos en algunos de los supuestos. Otra cosa es que sí se exija que el autor en la conducta de ataque a la intimidad penalmente relevante emplee medios técnicos para el acceso al contenido de la comunicación o la captación de imágenes o sonidos. Para algunos supuestos resulta una exigencia típica expresa y para otros un presupuesto fáctico ineludible, como ya se ha indicado. En todos los casos manifiesta un específico desvalor de acción en la conducta del autor, coherente con principios básicos del Derecho penal como el principio de intervención mínima y el principio de fragmentariedad. La necesidad de empleo de instrumental técnico o de apoderamiento documental impone un umbral mínimo para las conductas penalmente relevantes, que se corresponde con la misión propia del Derecho penal y que evita que posea trascendencia penal el hecho de escuchar detrás de una puerta una conversación que pueda afectar a secretos o la intimidad de determinadas personas, distinguiéndose de las meras faltas de educación, por graves que puedan ser.

Ya se ha destacado que este supuesto afecta a cualquier tipo de señal empleada en la telecomunicación. Pero la calificación del comportamiento como interceptación y la tipificación de algunas conductas en el primer inciso del art. 197.1 parece restringir las conductas relevantes penalmente a un determinado momento. Al ha-

245 En *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons, 2000, p. 280.

blarse de interceptación se está sugiriendo ya que la comunicación –al menos desde el punto de vista técnico– se está produciendo en ese momento, es decir, se trata de mensajes en tránsito. Igualmente el que antes se haya incriminado el apoderamiento documental –entre los que se encuentra el correo electrónico– sitúa nuevamente el segundo inciso del número primero del art. 197 –interceptación de las telecomunicaciones– fuera de las fases de recepción y almacenamiento de los mensajes. La exigencia de apoderamiento, con la consiguiente materialización del mensaje ya vista, en las anteriores conductas, harían referencia justamente a los momentos de recepción y almacenamiento. Con ello también se establece una correspondencia con la diferenciación procesal según el momento en el que se encuentre la comunicación para los casos de vigilancia o control ilícito de las telecomunicaciones por las autoridades.[246]

Aquí se reproducen el conjunto de elementos necesarios para la relevancia típica de la conducta del supuesto anterior. Así es necesario que el autor del hecho persiga con su conducta de interceptación de las telecomunicaciones el descubrir secretos o vulnerar la intimidad de otro. Bien entendido que esto no supone la producción de resultado alguno en el sentido de un menoscabo efectivo de la intimidad o descubrimiento real de algún tipo de secreto. Sin embargo, la consumación delictiva *sí* que precisa que, según las circunstancias del caso concreto, el autor, de acuerdo a los medios técnicos empleados, llegue a interceptar de manera efectiva las telecomunicaciones. Interceptada la comunicación pero no descubierto secreto alguno o sin violación de la intimidad, el hecho punible está completo en su descripción típica.

También aquí el supuesto toma como punto de referencia el descubrimiento de secretos o vulneración de la intimidad, como tendencia en la conducta del autor, y no lo referente a la posterior revelación o difusión de los datos que constituyen el secreto o afectan a la intimidad que, como ya se ha mencionado, se castigan

246 Véase PARTE TERCERA de este trabajo y el Documento de la UE sobre "Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos" de 26 de enero de 2001.

independientemente y de forma más severa según las previsiones del número tercero del art. 197.

IV. TUTELA PENAL DE LOS DATOS RESERVADOS DE FICHEROS AUTOMATIZADOS

En el número segundo del art. 197 encontramos lo que puede considerarse la regulación penal más general de la intimidad informática. En el contexto del Título X (que cabe considerar como el lugar sistemático de la tutela de la intimidad) se contiene en el precepto indicado las conductas punible relacionadas con datos reservados contenidos en ficheros automatizados.[247] Ya hemos visto algunas otras conductas vinculadas a la informática de agresión a la intimidad contenidas en el número primero del art. 197 y que, por tanto, deben excluirse del ámbito del número segundo.

A la hora de desarrollar este campo vamos a tratar separadamente los elementos típicos generales y, por otro lado, las conductas en sentido estricto. En realidad vamos a comprobar que guardan una estrecha relación –especialmente en algún caso– y no sólo porque, naturalmente, la punibilidad dependa de la concurrencia del conjunto de requisitos típicos.

1. Elementos o presupuestos típicos generales

a) Un primer aspecto se refiere al objeto material de este hecho punible contra la intimidad. La acción delictiva prevista en el número segundo del art. 197 debe recaer sobre "datos reservados de carácter personal o familiar de otro". Esta determinación legislativa del concreto objeto material del delito no deja de presentar varias dificultades.[248]

---

247 En la legislación italiana se diversifica la regulación efectuada por el Código penal de protección de la intimidad en cuanto reserva de las comunicaciones (reforma introducida en el Código por la Ley 547/1993) de la relativa al tratamiento automatizado de datos personales mediante ley especial 675/1996, de 31 de diciembre. PICA, G. Diritto penale *delle technologie informatiche*, Utet, Torino, 1999, pp. 281 y ss.

248 Véase también sobre estos aspectos PICA, G., *Diritto penale delle technologie informatiche*, Utet, Torino, 1999, pp. 296 y ss.

Así la calificación de los datos que constituyen este objeto de la conducta punible como "reservados" produce cierto desconcierto en la doctrina. Primero porque tal calificación no coincide con la denominación usual en el ámbito de la protección de datos personales. Así la LOPDP habla de datos de carácter personal, que son todos los objetos de la mencionada regulación. Para los datos que se entienden forman parte del núcleo de la intimidad de las personas, la mencionada LOPDP (art. 7) se refiere a "datos especialmente protegidos" con un régimen cualificadamente garantista.

No hay por tanto coincidencia en las denominaciones de estos dos órdenes jurídicos, lo que tampoco debe considerarse definitivamente un inconveniente. Pero es verdad que la calificación como reservados podría llevar a entender que sólo determinados datos personales son abarcados por la regulación penal que estamos viendo, quedando el resto fuera de la tutela jurídico-penal. Según esta primera aproximación deberían considerarse reservados aquellos más estrechamente vinculados al ámbito de la intimidad de las personas, es decir, los referentes a la ideología, religión, creencias, afiliación sindical, origen racial, vida sexual, salud, infracciones penales o administrativas (todos ellos incluidos en el régimen particular establecido para los "datos especialmente protegidos" del art. 7 LOPDP).

Esta posibilidad ha sido acertadamente descartada por MORALES[249] al confrontarla con las previsiones del número quinto del art. 197 CP. El tipo agravado del número quinto del art. 197 eleva las penas cuando los hechos "afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual…" Si se aceptase la interpretación propuesta sobre la calificación como reservados de los datos protegidos, obligaría a dejar total o sustancialmente vacío de contenido del tipo del número segundo del art. 197 CP. Además es conocido que no existen datos sin interés y menos, si como resulta correcto y realista, se valoran los mismos en una visión dinámica (interrelación o combi-

249 En *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 1999, pp. 344-5.

naciones entre los mismos, etc.), y no desde una óptica puramente estática.[250]

Todo ello hace que exista un cierto acuerdo en estimar que no puede entenderse que la tutela penal se dirige únicamente a determinados datos, es decir, que cabe concebir, en principio, todos los incorporados a un fichero automatizado como reservados a efectos penales.[251] Esto puede justificarse no sólo por la lesividad potencial para el bien jurídico de cualquier dato personal incluido en un tratamiento automatizado, sino también porque el carácter de reservados puede entenderse en un sentido descriptivo,[252] como aquellos para los que no se posee un acceso libre por cualquiera. Es decir, se excluirían únicamente los datos contenidos en ficheros de consulta libre por cualquier persona, como las denominadas "fuentes accesibles al público" en la LOPDP, aunque no sólo éstas, dadas las exclusiones de determinados ficheros públicos del ámbito de la mencionada ley.

También produce alguna dificultad la referencia a datos no sólo personales sino incluso familiares, probablemente por el peso de la declaración constitucional reconociendo el derecho a la "intimidad personal y familiar" (art. 18.1 CE). Igualmente esta diferencia con la regulación de la LOPDP causa una inicial incerteza, aunque en la práctica lo más probable es que no tenga gran importancia. Como señala SEGRELLES[253] lo familiar es al final también personal. Los datos familiares poseen significación para la intimidad de los miembros de ese grupo familiar. Quizás la dificultad real estribe en determinar qué grado de parentesco resulta comprendido en el objeto material.

---

250 MARCHENA GÓMEZ, M., "Intimidad e informática: la protección jurisdiccional del *habeas data". Boletín de Información. Ministerio de Justicia e Interior nº 1768 (1996)*, p. 752.

251 En este sentido MARCHENA GÓMEZ, M., "Intimidad e informática: la protección jurisdiccional del *habeas data". Boletín de Información. Ministerio de Justicia e Interior nº 1768 (1996)*, pp. 753-4.

252 Así SEGRELLES DE ARENAZA, I., en *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons, 2000, p. 285.

253 En *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons, 2000, p. 286.

En todo caso, se trata siempre de datos reservados ya registrados en un determinado fichero. El Derecho penal ha renunciado a admitir como hechos relevantes momentos anteriores a la existencia del fichero. Toda la fase anterior, en el ciclo total de un fichero, la fase de formación del mismo (obtención irregular de datos, constitución del mismo fichero[254]) quedaría al margen de los hechos penalmente relevantes.[255] Particular interés puede poseer la formación misma del fichero al margen de la regulación legal prevista para ello, que pudiendo ser considerada atípica,[256] puede dar lugar, sin embargo, a conductas punibles sobre la base de los datos obrantes en el mismo. En todo caso su exclusión del ámbito penal no evita su ilicitud y su consideración como infracción administrativa.

Por último cabe señalar como con carácter general el llamado *habeas data* penal se entiende circunscrito a los ficheros automatizados de datos. Sin embargo, algún autor[257] estima que la regulación abarca tanto ficheros automatizados como no automatizados, pues entiende que el *habeas data* no se limita a la informática, tal y como tampoco hace la LOPDP. Es cierto que la intimidad puede verse amenazada mediante el uso fraudulento de datos pertenecientes a cualquier tipo de archivos o ficheros. De hecho la regulación de este supuesto finaliza con una fórmula general que admite la inclusión de los datos en "cualquier otro tipo de archivo o registro público o privado". Pero también lo es que la trascendencia, al menos *a priori*, de los datos contenidos en ficheros automatizados, para la intimidad de las personas no puede ser equiparada a la de los ar-

254 La constitución clandestina de un fichero, sin embargo, constituye específicamente en la legislación francesa un hecho punible en esta materia. Véase PANSIER, F.J/JEZ, E., *La criminalité sur lÍnternet*, PUF, 2000, p. 70.

255 MARCHENA GÓMEZ, M., "Intimidad e informática: la protección jurisdiccional del *habeas data". Boletín de Información. Ministerio de Justicia e Interior nº 1768 (1996)*, p. 756. MORALES PRATS, F., en *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 1999, p.

256 En ese sentido MARCHENA GÓMEZ, M., "Intimidad e informática: la protección jurisdiccional del *habeas data". Boletín de Información. Ministerio de Justicia e Interior nº 1768 (1996)*, p. 757.

257 SEGRELLES DE ARENAZA, I., en *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons, 2000, p. 281.

chivos no automatizados. El tratamiento automatizado de datos genera sin duda una mayor intensidad de riesgo para la incolumidad de la intimidad. En todo caso en este momento nos interesa únicamente la protección penal de los datos registrados en ficheros automatizados.

b) En las dos secuencias típicas del número segundo del art. 197 CP se hace una mención al perjuicio que deben causar estas conductas. Así en el primer inciso (apoderamiento, utilización o modificación de los datos) se exige que el autor obre "en perjuicio de tercero". Para el segundo ámbito típico (acceso, alteración o utilización) nuevamente el sujeto activo sólo actúa en el sentido requerido por la tipicidad si lo hace "en perjuicio del titular de los datos o de un tercero".

Quedan, sin embargo, por determinar múltiples aspectos relativos a este elemento, como su naturaleza, los sujetos a los que en concreto se refiere el mismo o el cómo debe producirse en el ámbito de la conducta típica. Resulta que todas estas preguntas se encuentran interrelacionadas entre sí.

La exigencia típica de perjuicio puede ser entendida, como sucede generalmente en los numerosos hechos punibles en los que se plantea de igual manera, bien en sentido subjetivo o bien en sentido objetivo. Si se estima que es un elemento subjetivo, como un particular elemento subjetivo del injusto, se viene a requerir que el autor actúe con la tendencia interna de perjudicar, con ánimo de causar perjuicio. Ello comporta las dificultades propias de todos los elementos de naturaleza subjetiva.

JAREÑO/DOVAL[258] entienden que se trata de un elemento objetivo, siguiendo la tesis del TS en la sentencia de 18 de febrero de 1999, por las dificultades que entrañan los elementos subjetivos y por no añadir nada a la conducta específica de acceso que queda fijada ya con su mera consideración objetiva. Consideran que la pers-

258 "Revelación de datos personales, intimidad e informática". *El nuevo Derecho Penal Español. Estudios Penales en Memoria del Profesor José Manuel Valle Muñiz*, Aranzadi, 2001, pp. 1486-90.

pectiva objetiva obliga a entender este elemento como resultado lesivo abarcado por el dolo. La perspectiva objetiva parece acertada, no así su comprensión como resultado lesivo, no congruente con la estructura del tipo ni necesario desde el punto de vista gramatical. De otra manera, en sentido objetivo, cabe vincularlo a la tendencia de la conducta externa del autor, como idoneidad objetiva de la misma para causar un perjuicio. Esta opción descarta aquellos hechos que no pudieran originar perjuicio alguno para el bien jurídico. Parece más acertada esta segunda versión, que además conecta con los postulados de la moderna teoría de la imputación objetiva.

Como se ha dicho, el legislador incluye este elemento del perjuicio en dos momentos distintos. En un primer momento se refiere a la actuación "en perjuicio de tercero" y en un segundo inciso la referencia lo es al comportamiento "en perjuicio del titular de los datos o de un tercero". Como en el primer caso únicamente se menciona al tercero, éste tiene que coincidir necesariamente con el titular del bien jurídico (intimidad), quien ve afectada su intimidad por el comportamiento sobre los datos reservados. No es posible entender que quien se ve afectado en su intimidad sólo se proteja en el segundo inciso. La denominación de tercero responde entonces a su consideración desde el punto de vista del autor de los hechos.

En el segundo momento regulativo el legislador se refiere no sólo al tercero sino también al titular de los datos. Lo que, según la interpretación propuesta, debe corresponder con el titular de la gestión de los datos, es decir, con el titular del fichero o del conjunto de datos cuyo tratamiento está automatizado. En este sentido MARCHENA[259] entiende que en este caso se protege a tal titular frente a un posible desapoderamiento o utilización inconsentida de los datos desde la perspectiva patrimonial. Con ello se decide también el último aspecto concerniente a la naturaleza del perjuicio. Para el denominado tercero se protege la intimidad y para el llamado "titular de los datos" lo relevante es el aspecto patrimonial, cuya

259 MARCHENA GÓMEZ, M., "Intimidad e informática: la protección jurisdiccional del *habeas data". Boletín de Información. Ministerio de Justicia e Interior nº 1768 (1996)*, p. 756. Sobre estos aspectos en la legislación Suiza SCHMID, N., *Computer- sowie Check- und Kreditkartenkriminalität*, Zürich, 1994, pp. 34 y ss.

inclusión en este ámbito sistemático puede considerarse una incongruencia.[260] De todas las maneras, la necesidad político-criminal de una reorganización del precepto se hace ineludible como se hace todavía más patente al analizar más adelante las concretas conductas descritas en el tipo.

c) Las conductas realizadas sobre datos reservados obrantes en ficheros automatizados deben realizarse por el sujeto activo "sin estar autorizado". Es decir, se criminalizan las conductas previstas en este número segundo del art. 197 que no cuenten con la anuencia del interesado o interesados. Se trata pues de un ámbito en el que el legislador admite la disponibilidad del bien jurídico tutelado por su titular. Como al referirnos a los sujetos perjudicados hemos distinguido entre el tercero y el titular, nuevamente aquí debe aplicarse la distinción a los efectos de determinar quien debe prestar el consentimiento válido. La forma concreta de prestación del consentimiento deberá ser aquella en la que quede determinado de manera incuestionable la auténtica voluntad del interesado en relación a la conducta a realizar sobre los datos reservados.

2. Las conductas punibles de ataque a la intimidad informática

Como se viene haciendo mención, las conductas en sentido estricto, desenvueltas por el autor del hecho punible vienen recogidas en el número segundo del art. 197 en dos momentos sucesivos. En un primer inciso el legislador incrimina "al que, sin estar autorizado, se apodere, utilice o modifique" los datos registrados en ficheros. Ya en el segundo inciso prevé las mismas penas para "quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice".

El apoderamiento debe entenderse en el sentido señalado, como aprehensión de algún tipo de materialización de los datos contenidos en el fichero. Ahora se trata de datos consignados en un fiche-

260 MARCHENA GÓMEZ, M., "Intimidad e informática: la protección jurisdiccional del *habeas data". Boletín de Información. Ministerio de Justicia e Interior nº 1768 (1996)*, p. 756.

ro automatizado y no de los datos recogidos documentalmente (según la previsión del número primero del art. 197 en su primer inciso). La descripción de la misma conducta dos veces distintas pudiera hacer surgir problemas concursales, pero la distinción se produce no tanto por la acción misma sino por el objeto del apoderamiento, en un caso de carácter documental y en otro sobre datos registrados en ficheros. La utilización de los datos se entiende como cualquier comportamiento de aprovechamiento posterior de los mismos. La modificación supone el cambio o transformación de los datos almacenados en el fichero. Modificación y alteración son conducta equivalentes a pesar de que el legislador emplee términos diversos. Con el acceso se produce la captación intelectual de la información almacenada en el sistema informático.[261]

Por tanto las conductas típicas incluyen comportamientos que se sitúan en dos segmentos distintos del ciclo total de un fichero automatizado de datos. Por una parte, se incriminan conductas realizadas sobre los datos existentes en el fichero (acceso, modificación y alteración) y, por otra, conductas posteriores cuando el dato ha sido obtenido ya del fichero (utilización). Sin embargo, nada obliga a que quien obtiene el dato del fichero y quien lo utiliza posteriormente sean los mismos sujetos. No se recogen otros supuestos distintos, por lo que quedan excluidos de la zona penalmente prohibida momentos previos a la incorporación del dato al fichero (recogida ilícita de datos o formación misma del fichero).

No deja de señalarse por la doctrina la diferenciación legislativa a la hora de incriminar las conductas punibles, en dos momentos sucesivos, empleando los mismos o equivalentes términos, con lo que se llega a una situación de confusión. Se ha producido algún intento de explicar las divergencias de las dos secuencias típicas. Así CARBONELL/G. CUSSAC[262] sitúan la distinción en torno al objeto de las conductas. De este modo el primer inciso (apoderamiento,

261 La descripción de estas conductas puede verse en CARBONELL/G.CUSSAC., *Comentarios al Código penal de 1995*, vol I, pp. 1000 y ss. También de los mismos autores en *Derecho Penal. Parte Especial*, Tirant lo blanch, 1999, pp. 290-2.

262 *Comentarios al Código penal de 1995*, vol I, p. 1001.

utilización o modificación) se proyectaría sobre los datos reservados, mientras el segundo momento lo haría sobre los ficheros o soportes informáticos, electrónicos o telemáticos. MORALES[263] ha rechazado acertadamente esta posibilidad al desenfocar teleológicamente la regulación, pues la protección de la intimidad hace relación a los datos personales y no se persigue la tutela de los ficheros o sistemas informáticos por sí mismos. Además, señala otras disfunciones como la de adelantar el momento de protección de los ficheros y retrasar la línea de intervención penal para los datos personales, auténtico objeto material del bien jurídico intimidad.

Quizás otra forma de señalar la distinción entre ambos incisos legislativos pudiera correr mejor suerte. Puede entenderse que la distinción responde no al objeto material sino a los sujetos que pueden recibir el perjuicio (potencial) exigido por la regulación. Conforme a lo desarrollado antes para el elemento del perjuicio se ha señalado ya como en un primer momento su destinatario es únicamente el tercero y en el segundo momento también el titular de los datos. Así las conductas de apoderamiento, utilización o modificación se vinculan al sujeto pasivo tercero, entendido como el afectado en su intimidad por las conductas realizadas sobre los datos reservados.

La segunda secuencia típica se refiere al acceso, alteración o utilización, pero para éstas se señala como sujeto pasivo no sólo el tercero, sino también "el titular de los datos" entendido como el propietario del fichero que vería lesionado su poder de disposición sobre el conjunto de datos y organización que constituyen el fichero, archivo o registro. La diferencia está únicamente en la conducta de acceso, no prevista en el primer inciso, como si se quisiera expresar que la misma no constituye atentado a la intimidad y sí de carácter patrimonial para el titular del fichero. De ser ésta la concepción que subyace tras la regulación, ésta constituye un excelente ejemplo de deficiente técnica legislativa.

263 En *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 1999, pp. 346-7.

En realidad el texto del número segundo del art. 197 es fruto de un particular modo de legislar. La redacción definitiva del precepto tiene su origen en una superposición descoordinada de enmiendas sobre la base del texto del proyecto de Código Penal de 1994, sin tener en cuenta lo que cada una de ellas modificaba el sentido del texto.

El Proyecto únicamente incluía la acción de apoderamiento de los datos reservados (art. 188).[264] La enmienda número 606 del GS había incorporado las conductas de utilización o modificación del finalmente primer inciso que debía producirse "en perjuicio de otro".[265] La número 728 del Grupo Federal IU-IC añadía la posibilidad de incluir los soportes electrónicos o telemáticos y, finalmente, la conducta por la que se "accediese por cualquier medio a los mismos sin la citada autorización".[266] La enmienda número 49 del GPV añadía al final "y a quien los alterase o utilizare en perjuicio del titular de los datos o de un tercero".[267] Con alguna reforma de matiz y estilo, ésta fue la redacción definitiva como conjunción de distintas enmiendas que aisladamente poseían cierta coherencia, pero que sumadas todas ellas creaban una gran confusión y desdibujaban el sentido de la regulación.

264 *Ley Orgánica del Código Penal. Trabajos Parlamentarios, vol I*, Cortes Generales, 1996, p. 36.

265 *Ley Orgánica del Código Penal. Trabajos Parlamentarios, vol I*, Cortes Generales, 1996, p. 272.

266 *Ley Orgánica del Código Penal. Trabajos Parlamentarios, vol I*, Cortes Generales, 1996, p. 299.

267 *Ley Orgánica del Código Penal. Trabajos Parlamentarios, vol I*, Cortes Generales, 1996, pp. 124-4. Esta enmienda se redactaba como añadido al apartado 2 de la anterior enmienda 606 del GS.

PARTE TERCERA

ASPECTOS PROCESALES EN LA DELINCUENCIA INFORMÁTICA

I. PROBLEMAS SOBRE LA DETERMINACIÓN ESPACIAL DE LA LEY PENAL APLICABLE

Uno de los condicionantes de la ley penal es saber qué ley es aplicable o si resulta aplicable una determinada ley penal a ciertos hechos con relevancia jurídico penal. Es decir si el hecho delictivo puede ser alcanzado por la legislación penal de un país por razón del lugar de ejecución del delito. En lo que nos afecta hay que tener en cuenta la naturaleza del medio de ejecución delictiva que ahora abordamos. Es decir que para el autor de hechos delictivos a través de Internet las fronteras nacionales son irrelevantes.[268] Sólo si se entiende extensible la ley penal a un determinado lugar los Tribunales penales que se rigen por esa ley podrán declararse competentes y llevar a cabo el enjuiciamiento de los hechos.

1. Espacio jurídico en el que se entiende cometido el hecho

El primer paso consiste en establecer el lugar en el que jurídicamente se declara realizado el delito, es decir, la determinación espacial del hecho delictivo desde el punto de vista jurídico.[269] Este

268 SCHWARZENEGGER, CH., "Der raümliche Geltungsbereich des Strafrechts im Internet". *Schweizerishes Zeitschrift für Strafrecht* 2/2000, p. 110.

269 Es la cuestión previa a la que se refiere MARCHENA GÓMEZ, M., "Algunos aspectos procesales de Internet", en *http://www.fiscalia.org/*, p. 27. *También en Problemática jurídica en torno al fenómeno de internet*, Cuadernos de Derecho Judicial, CGPJ IV/2000.

problema puede parecer sencillo y lo será en muchos casos en los que la ejecución delictiva no presente diferencias temporales ni espaciales entre el comportamiento (acción delictiva en sentido estricto) y el resultado delictivo. El disparo sobre la víctima causando la muerte se produce generalmente en un mismo contexto espacio-temporal evitando así dudas sobre el lugar de realización del hecho delictivo.

Pero, sin embargo, es posible, y será lo propio de los hechos ilícitos cometidos con ocasión de transacciones electrónicas y otros muchos casos, que la acción desenvuelta por el autor suceda en un lugar físico, y en otro –más o menos alejado– el resultado del delito. Así quien lleva a cabo la manipulación informática puede encontrarse en una ciudad distinta de la del terminal de la empresa que recibe un perjuicio patrimonial en el ámbito de su actividad negocial electrónica. Si ambos puntos espaciales, aunque en poblaciones diversas, se encuentran en un mismo país, no se produce duda sobre la ley penal aplicable, que en todo caso es la misma, pero sí un problema de competencia de los concretos Tribunales penales que deberán perseguir los hechos.

En la actualidad no contamos en España con ninguna norma positiva que señale el lugar en el que se entiende cometido el delito, ya que la referencia del art. 7 CP lo es únicamente al problema de la determinación temporal de la ley penal. Para la solución de este problema Doctrina y Jurisprudencia conocen tres posibles alternativas. La teoría de la acción sitúa el lugar de producción del delito allí donde el autor desenvuelve el comportamiento que dará lugar al delito. Por otra parte la teoría del resultado señala como lugar de realización del delito allí donde ha sucedido el resultado exigido por el tipo penal particular.

Finalmente la teoría de la ubicuidad, la mayoritariamente seguida en doctrina y jurisprudencia permite fijar el lugar de realización del delito tanto en el lugar de la acción como en el del resultado. Dadas estas alternativas posibles queda claro que no es posible fundamentar el lugar de comisión del hecho sobre la base de los lugares de tránsito en los lugares en los que se sitúen los nodos que permiten el recorrido telemático, como acertadamente recoge MAR-

CHENA.[270] De manera semejante se establece el debate en otros Ordenamientos Jurídicos.[271]

En estos casos de posible competencia de dos Tribunales penales españoles en la persecución de un mismo hecho punible, la Jurisprudencia mantiene la determinación de la competencia territorial con arreglo a la teoría de la ubicuidad, de forma que por aplicación analógica del art. 15 LECrim. entiende que debe declararse competente, con carácter general, al Juzgado que incoó en primer término las diligencias.[272] Para los casos de delito de estafa, la jurisprudencia sostiene, sin embargo, que la competencia corresponde al Juzgado del lugar donde se produce la consumación, que es aquél en el que se produce el efectivo desplazamiento patrimonial.[273]

Mayores dificultades se producen cuando la diferencia espacial entre acción y resultado delictivo supone traspasar las fronteras nacionales. Esto nos sitúa ya ante problemas nuevos que vamos a tratar a continuación.

2. Ámbito espacial de la ley penal nacional

Con ello nos preguntamos ya por el espacio al que se extiende la aplicación de la ley penal de un país. Es decir, a qué lugares en los

---

270 MARCHENA GÓMEZ, M., "Algunos aspectos procesales de Internet", en *http://www.fiscalia.org/*, p. 27. *También en Problemática jurídica en torno al fenómeno de internet*, Cuadernos de Derecho Judicial, CGPJ IV/2000.

271 En SCHWARZENEGGER, CH., "Der raümliche Geltungsbereich des Strafrechts im Internet". *Schweizerishes Zeitschrift für Strafrecht* 2/2000, pp. 114 y ss. pueden verse los distintos problemas de cada una de las teorías, las dificultades del concepto de resultado y la clasificación de los distintos tipos penales en cuanto a la exigencia de resultado (delitos de mera actividad o de resultado, delitos de lesión y delitos de peligro abstracto o peligro concreto, delitos a distancia, etc.).

272 Puede verse en este sentido Auto TS de 26-3-98, RJA 3391.

273 Así Auto TS 27-10-98, RJA 10743, en un caso de estafa en una venta a distancia mediante el sistema de televenta. Para los casos de omisión véase Auto TS 21-1-98. RJA 2000. Sobre la evolución jurisprudencial respecto al problema del lugar en el que se entiende cometido el delito puede verse MARCHENA GÓMEZ, M., "Algunos aspectos procesales de Internet", en *http://www.fiscalia.org/*, p. 32. *También en Problemática jurídica en torno al fenómeno de internet*, Cuadernos de Derecho Judicial, CGPJ IV/2000.

que se entiende cometido un hecho delictivo puede entenderse aplicable la ley penal de una nación. Esto naturalmente redunda en la declaración de competencia de los Tribunales penales de un país –en general– para poder perseguir unos hechos penalmente relevantes.

En nuestro país –como sucede generalmente– la regla que rige el ámbito espacial de la ley penal española es la de la territorialidad.[274] En general la ley penal española resulta aplicable a los hechos sucedidos en el territorio jurídico de nuestro país, es decir, tanto el territorio físico, como espacio aéreo y aguas jurisdiccionales. En este caso sí que contamos con declaraciones legales al respecto. Así el art. 8 Cciv., como también el art. 23.1 LOPJ afirman el principio de territorialidad. Este principio general tiene su base en la consideración de la ley penal como emanación de la soberanía nacional, de modo que la misma se extiende a todo el territorio del país.

Sólo excepcionalmente tiene lugar la aplicación extraterritorial de la ley penal, para los casos en los que concurran los presupuestos de los principios de personalidad, de protección de intereses o de justicia universal. De acuerdo al principio de personalidad (art. 23.2 LOPJ) el hecho penal es perseguible según la ley penal correspondiente a la nacionalidad del autor, aun cuando, sin embargo, el hecho se cometa fuera de las fronteras de nuestro país. La LOPJ requiere que el hecho sea punible en el lugar de ejecución (después de las últimas reformas salvo que no lo exija el Derecho Internacional vinculante para España), denuncia o querella del agraviado o del Ministerio Fiscal y que el delincuente no haya sido absuelto, indultado o penado ya en el extranjero.

Por tanto, conforme al principio de personalidad pueden ser perseguidos los delitos informáticos si el autor es español. Eso sí, deben darse los requisitos mencionados: que el hecho sea punible también en el país en el que se lleva a cabo el hecho (principio de

274 Sobre los problemas del ámbito espacial de la ley penal en los casos de Internet y los principios conforme a los que se determina la competencia de los Tribunales penales suizos, SCHWARZENEGGER, CH., "Der räumliche Geltungsbereich des Strafrechts im Internet". *Schweizerische Zeitschrift für Strafrecht* 2/2000, pp. 111 y ss.

identidad o de doble incriminación), previa denuncia o querella de la víctima y a su vez que el autor no haya sido previamente absuelto, penado o indultado en aquél país. De estos requisitos la exigencia que el hecho sea punible igualmente en el lugar de comisión puede plantear problemas especialmente con países no pertenecientes a nuestro círculo geográfico-cultural, con los cuales las diferencias en la legislación penal son más acusadas.

También puede conocer la Jurisdicción española de los hechos cometidos por españoles o extranjeros fuera del territorio nacional cuando los hechos atenten contra el principio de protección de intereses para el propio estado. En el n° 3 del art. 23 LOPJ se recoge el listado de los hechos delictivos que se entienden perseguibles sobre la base de este principio. Será difícil que los hechos delictivos relacionados con la informática puedan ser atribuidos a la Jurisdicción española con el apoyo de este principio dada la naturaleza del elenco de delitos que incorpora de escasa congruencia con la delincuencia informática.[275] Quizás algunas formas de falsificación previstas o los hechos cometidos por funcionarios o autoridades públicas en el extranjero pudieran tener alguna trascendencia a los efectos de los delitos que nos interesan.

Finalmente el n° 4 de este mismo precepto indica expresamente los hechos que resultan perseguibles por la Jurisdicción penal española de acuerdo a los presupuestos del principio de justicia universal. El mismo hace posible que hechos punibles que se entienden lesivos para todos y cualquier Estado puedan ser investigados y juzgados por la jurisdicción nacional pese a no darse los presupuestos anteriores para la declaración de competencia de los Tribunales penales españoles. De los hechos previstos en la relación que afectan al principio de justicia universal, algunos supuestos de prostitución y corrupción de menores (utilización para espectáculos exhibicionistas o pornográficos) pueden guardar relación con la delincuencia informática. En realidad se trata de tipos penales

275 Sobre este aspecto MARCHENA GÓMEZ, M. "Algunos aspectos procesales de Internet", en *http://www.fiscalia.org/*, pp. 34 y ss. *También en Problemática jurídica en torno al fenómeno de internet*, Cuadernos de Derecho Judicial, CGPJ IV/ 2000.

en los que ya existe una previsión –aunque no del todo clara– para su punibilidad "aunque el material tuviere su origen en el extranjero o fuere desconocido" (art. 189 CP).

En ocasiones puede caerse en la tentación de buscar soluciones a la persecución de este tipo de hechos delictivos –u otros– mediante su incorporación generalizada al ámbito del principio de justicia universal. Sin embargo no dejan de señalarse los inconvenientes y dificultades que genera esa pretensión. Así MARCHENA[276] indica que "La incondicionada persecución de toda acción delictiva ejecutada mediante Internet no puede sostenerse con un mínimo rigor. De ahí que la reformulación del principio de universalidad a partir de un criterio puramente instrumental, supondría un verdadero peligro para la coherencia del sistema de delimitación jurisdiccional".

Se hace evidente que la aparición de las nuevas tecnologías ponen en cuestión el sistema de determinación de la ley penal conforme a los principios señalados. De forma que, por una parte, como manifiesta SEMINARA,[277] en Internet una estricta aplicación del principio de territorialidad conduce a la impunidad. Sin embargo no son menores los peligros de otras alternativas, por lo que también señala este autor que la solución opuesta sustituye la anarquía de Internet por una anarquía de Derecho.

3. Mecanismos internacionales de cooperación penal: la extradición

Declarada la aplicabilidad de la ley penal española conforme a cualquiera de los principios que rigen la misma, puede, sin embargo, presentarse otro obstáculo en la persecución del hecho delictivo. Aun cuando los Tribunales penales puedan conocer del hecho según los criterios territoriales o extraterritoriales, si el sospechoso se encuentra fuera del territorio nacional, el mismo no puede ser puesto

276 "Algunos aspectos procesales de Internet", en *http://www.fiscalia.org/*, p. 35. También en *Problemática jurídica en torno al fenómeno de internet*, Cuadernos de Derecho Judicial, CGPJ IV/2000.

277 "La pirateria su Internet e il diritto penale". *Rivista Trimestrale di Dirritto penale dell´economia*, 1-2 (1997), p. 111.

a disposición de los Tribunales para que éstos lleven a cabo la investigación y enjuiciamiento de los hechos. Para superar estos obstáculos existen diversos mecanismos internacionales de cooperación penal entre los Estados, entre los que sobresale el de la extradición.

Como sabemos la extradición consiste en una institución de larga tradición que permite poner a disposición de los Tribunales a aquellas personas refugiadas en país distinto de aquel que pretende procesarle. El Estado que se declara competente en el enjuiciamiento de los hechos solicita (Estado requirente) la entrega de los sospechosos al país de refugio (Estado requerido) para proceder a declarar las responsabilidades penales a que hubiera lugar. De esta forma si determinados hechos relacionados con la informática hubieran sido cometidos desde el exterior y los Tribunales penales españoles pudiesen declararse competentes, podrían solicitar la extradición de los imputados de haberse refugiado en otro país.

Sin embargo la institución de la extradición presenta en su regulación legal una serie de requisitos que pueden dificultar su aplicación. La LECrim. en sus arts. 824 y ss. regula la conocida como extradición activa –en la que España solicita la entrega de un acusado refugiado en otro país– y determina los supuestos de posible solicitud de extradición.

Además de darse alguno de los supuestos de extradición previstos, otros principios que informan esta institución poseen especial significación en este campo. Así el principio de identidad o de doble incriminación exige, para proceder a la extradición, que el hecho perseguido sea punible tanto en el país que solicita la extradición como en aquél en el que se encuentra refugiado el acusado. En muchos casos las legislaciones penales poseen la suficiente homogeneidad para que no exista problema en este terreno, pero en otros casos –singularmente países no pertenecientes a nuestro ámbito jurídico-cultural– la vigencia de este principio puede representar un freno a la posibilidad de poner a disposición de los Tribunales al autor de los hechos.

Así por ejemplo, la pornografía infantil introducida en Internet desde los países asiáticos vería dificultada la entrega de los autores de darse los elementos del delito y la extradición fuera solicitada por España, al no existir normalmente previsiones legales para este

ámbito delictivo en aquellas latitudes.[278] Únicamente la existencia de alguna norma internacional vinculante para España en sentido contrario permitiría eludir este requisito de acuerdo a la nueva redacción del n° 2 del art. 23 LOPJ (Redacción conforme a la LO 11/1999 de 30 de abril en su disposición final única n° 1).

Otras limitaciones a la extradición lo constituye el principio *non bis in idem*, según el cual no se concede la extradición si el delito ya ha sido objeto de enjuiciamiento en el Estado requerido, y, por otra parte, en los Tratados y leyes de extradición suele señalarse las penas mínimas a partir de las cuales los delitos pueden ser objeto de extradición, excluyéndose el resto de hechos punibles por considerarse de escasa gravedad. Por ello habrá de estarse a los convenios bilaterales o multilaterales sobre esta materia en los que participen los Estados requirente y requerido.

El escenario se complica cuando expresamente se elige situar el servidor en determinados países antes conocidos como Paraísos fiscales y ahora convertidos en Paraísos informáticos, pues al no participar los mismos en ninguna clase de Convenio Internacional que permita a otros países que sufran consecuencia de hechos realizados desde aquellos no pueden reclamar la entrega de quienes llevan a cabo determinadas actividades como la venta ilegal de *software*, pero también otras como venta de productos farmacéuticos no autorizados y de drogas, blanqueo de capitales, bancos de datos personales, etc.[279]

Frente a este tipo de situaciones se propone interponer acciones legales ante los tribunales norteamericanos para que éstos se dirijan a la IANA, organismo con sede en EEUU y encargado de asignar los llamados *Internet Protocol* (IP) –número que identifica a un servidor a lo largo de toda la Red– a los propietarios de un ser-

278 Sobre ello BLANCO CORDERO/SÁNCHEZ GARCÍA DE PAZ, "Principales instrumentos internacionales (de Naciones Unidas y la Unión Europea) relativos al crimen organizado: la definición de participación en una organización criminal y los problemas de aplicación de la ley penal en el espacio", *Revista Penal* 6/2000, p. 9.

279 Casos mencionados por J. RIBAS ALEJANDRO. *Aspectos jurídicos del Comercio electrónico*. Aranzadi, 1998, pp. 139 y ss.

vidor. La suspensión o retirada del IP hace que deje de ser visible el servidor para los usuarios de la Red.

II. MEDIOS ELECTRÓNICOS Y PROCESO PENAL

El esclarecimiento de los hechos ilícitos relacionados con la informática tropieza con no escasas dificultades de muy variada índole (desde las puramente técnicas, las de orden jurídico y otras).[280] Por ello, para comenzar, resulta sumamente aconsejable la adopción de medidas de precaución, en especial en empresas y en la Administración pública.[281]

1. Dificultades en la investigación

Como se ha dicho estos procedimientos representan particulares dificultades en el descubrimiento de los hechos y su persecución. En el ámbito de la delincuencia informática se presentan sin duda importantes complicaciones para el descubrimiento y la investigación de los hechos en y mediante el ordenador, de forma que puede en ocasiones no ser raro que muchos de los casos no lleguen nunca a detectarse. Según datos del FBI sólo se llegan a descubrir un 1% de los casos, de éstos únicamente el 14 se ponen en conocimiento de las autoridades y, finalmente, tan sólo un 3% de estos últimos acaba en una sentencia condenatoria. De forma que de cada 22.000 autores de estos hechos, solamente 1 de todos ellos resultaría condenado por los Tribunales, según menciona el

280 Sobre algunos de los problemas procesales en la persecución de la delincuencia transnacional por Internet, con propuesta de reorganización del sistema jurídico-procesal VASSILAKI, I.E., "Strafverfolgung der grenzüberschreitenden Internet-Kriminalität, *Computer und Recht* 9/1999, pp. 574 y ss.

281 Para estos aspectos en general y en relación a todo lo que sigue en cuanto a las medidas de precaución en empresas y Administración para evitar la vulneración de sus sistemas informáticos, puede verse SIEBER, U., "Criminalidad informática: peligro y prevención". *Delincuencia informática*. (MIR PUIG Comp.). PPU, Barcelona 1992, pp. 34 y ss. Y del mismo autor "Documentación para una aproximación al delito informático". *Delincuencia informática*. (MIR PUIG Comp.), PPU, Barcelona, 1992, pp. 83 y ss.

propio SIEBER,[282] con lo que se evidencian los graves problemas que –desde muchas ópticas– se ciernen sobre la lucha contra este tipo de hechos.

Desde el punto de vista técnico se aprecian problemas de envergadura en la investigación, pues el rastreo informático de la ejecución delictiva se entorpece con la característica falta de visualización inmediata de los pasos lógicos ejecutados y la numerosa acumulación de procesos individuales que se ejecutan diariamente y a lo largo del tiempo en un sistema informático.[283] Así señala MARCHENA[284] cómo "Internet facilita el anonimato y permite que el seguimiento de la huella telemática que va dibujando la ejecución del delito, tropiece con saltos territoriales provocado mediante una hábil utilización de los nodos que hacen posible la comunicación telemática".

Una de las características de los medios de comunicación electrónicos es justamente la necesidad de contar con un intermediario (el ordenador y sus programas) que facilite el acceso a la información. Incluso puede añadirse el cifrado de los accesos y contenidos lo que dificulta todavía más su conocimiento. Con ello la individualización del concreto proceso de ejecución del hecho delictivo alcanza cotas elevadas de complejidad técnica, duración y coste económico. No es despreciable este aspecto de la carga económica de la investigación. Si se trata de una empresa privada puede en ocasiones llegar a considerar que es más rentable el abandono de la investigación que su finalización. Si son los poderes públicos esto requiere la dotación de partidas presupuestarias suficientes para contar con personal especializado y material adecuado y eso, en ocasiones, no será posible.

---

282 Datos aportados por SIEBER, U., "Criminalidad informática: peligro y prevención". *Delincuencia informática*. (MIR PUIG Comp.). PPU, Barcelona, 1992, pp. 31-32.

283 Véase al respecto CONSENTINO, G. y otros. "Tras los pasos de la seguridad perdida. Delitos informáticos". *Informática y Derecho* 23,26 (1998), p. 1198.

284 "Algunos aspectos procesales de Internet", en *http://www.fiscalia.org/*, pp. 25 y ss. También en *Problemática jurídica en torno al fenómeno de internet*, Cuadernos de Derecho Judicial, CGPJ IV/2000.

Además todo ello se ve agravado desde el momento en que, precisamente para esquivar la investigación, el acceso a la red o los contenidos introducidos pueden ser trasladados convenientemente a otros servidores.[285] El cambio permanente de la ubicación del servidor con contenidos ilícitos, que puede lograrse con gran facilidad, impide evitar la continuidad de la realización delictiva y tiende a alargar indefinidamente la investigación. Si se decide la colocación del servidor por el autor de los hechos en uno de los llamados paraísos fiscales, las dificultades vienen del lado jurídico, al imposibilitarse la investigación y detención de los delincuentes en aquél país.

Por otra parte, también en atención a la perspectiva jurídica, hay que señalar que la investigación obliga a trabajar con datos sensibles, por lo que puede entrar en conflicto la aportación de elementos relevantes para la investigación con el anonimato y la protección de la intimidad del "ciudadano electrónico".[286] Respecto a la colaboración necesaria de los operadores de la red en la investigación criminal tampoco se cuenta con una definición suficiente de estos deberes de colaboración de operadores y titulares de servidores que permitan a las autoridades obtener pruebas suficientes de los hechos.

No hay que desdeñar tampoco en la valoración de los escasos resultados que muestran las estadísticas lo relativo a los posibles menoscabos en la imagen pública de una empresa. En muchas ocasiones los empresarios pueden optar por no perseguir los hechos ilícitos relacionados con el sistema informático propio por temor a las repercusiones sobre la imagen pública de la marca comercial o de la empresa.[287] Lo cierto es que bien con una mera investigación interna o incluso sin ningún tipo de averiguaciones sobre los he-

285 En este sentido MORON LERMA, E. *Internet y Derecho Penal:* Hacking *y otras conductas ilícitas en la red*. Aranzadi, 1999, p. 122.

286 Véase MORON LERMA, E. *Internet y Derecho Penal:* Hacking *y otras conductas ilícitas en la red*, Aranzadi, 2000, p. 31.

287 Véase TIEDEMANN, K., "Computerkriminalität und Strafrecht". *Internationalen Perspektiven inKriminologie und Strafreht II. Festschrift für Günther Kaiser zum 70. Geburtstag*. Berlin, 1998, p. 1374.

chos queda cortada de raíz la posibilidad de esclarecimiento de los hechos al poner en el primer escalón del orden de prioridades el miedo a la pérdida de confianza de clientes y ciudadanos. Con lo cual, además, se proporciona una amplia sensación de impunidad a los autores de este tipo de delitos.

2. Posibilidades y necesidades de la investigación criminal

a) La investigación de este tipo de hechos delictivos se aparta mucho del procedimiento habitual. Aunque existen otros hechos y datos ajenos a los sistemas informáticos, son aquellos los que pueden proporcionar las evidencias más relevantes, incluso en algunos casos sólo los datos procedentes del sistema informático resultan definitivos. Pese a todos los inconvenientes señalados para la persecución de estos hechos, sin embargo, no dejan de existir recursos que posibilitan el rastreo de las "huellas electrónicas" de un delito informático.

Las alteraciones de datos y programas y los accesos a sistemas informáticos no dejan huellas semejantes a la de la delincuencia tradicional, de forma que las "huellas digitales" introducen una gran novedad y complejidad. Existe la posibilidad de identificar quienes de manera ilícita introducen y procesan datos mediante *loggins* y otros registros.[288]

Los ordenadores se identifican por el número IP (*Internet Protocol*) establecido mundialmente y que queda registrado en todos los accesos a la red. Así en lo que concierne al correo electrónico la cabecera del mismo proporciona el número IP, salvo en los casos de correo electrónico anónimo que ofrecen determinadas empresas o para los teléfonos móviles con sistema de prepago. En los pasos de la comunicación por Internet la identificación del servidor queda registrada en los *logs* o registro de sucesos de los ordenadores, de los que se puede obtener, por tanto, datos de sumo interés.

288 SIEBER, U., "Documentación para una aproximación al delito informático". *Delincuencia informática*. (MIR PUIG Comp.), PPU, Barcelona, 1992, pp. 94 y ss.

Sin embargo queda pendiente de fijar jurídicamente la obligación de los titulares de los servidores de almacenar durante un determinado periodo tales datos. Otra alternativa en la investigación, frente los posibles obstáculos ya indicados, consiste en seguir la pista al dinero mismo y que de ahí se deriven otros extremos válidos para la indagación propiamente electrónica, en el caso de que se trate de un asunto con contenido económico.[289] También en el caso de intervenciones de las comunicaciones telemáticas se presenta un alto índice de ineficacia debido a los sistemas de encriptación utilizados, por lo que las fuerzas policiales de todos los países entienden necesario la creación de puertas traseras en estos sistemas.

b) En el ámbito policial se centra uno de los puntos decisivos para la eficacia en la lucha contra la criminalidad informática.[290] Así la creación de unidades especializadas constituye un presupuesto necesario para afrontar este fenómeno. Por otra parte la característica mundialización del fenómeno, con el desbordamiento de las fronteras nacionales mediante estos sistemas, impone una progresiva cooperación policial internacional en este terreno, sobre la base de una más amplia y general cooperación internacional en esta materia.[291] Cooperación que ya ha dado lugar a la creación de sistemas de información intercomunicados, con trasvase de información policial entre los distintos países, fundamental a la hora de componer el mapa total de los hechos que pueden encontrarse fragmentariamente en distintos países. Incluso puede llegarse a crear cuerpos policiales internacionales con agentes propios que realicen funciones en el campo de la delincuencia informática (EUROPOL).

---

289 Así SIEBER, U., "Documentación para una aproximación al delito informático". *Delincuencia informática*. (MIR PUIG Comp.), PPU, Barcelona, 1992, pp. 94 y ss.

290 Véase al respecto lo señalado por HERNÁNDEZ GUERRERO, F.J./ÁLVAREZ DE LOS RÍOS, J.L., "Medios informáticos y proceso penal", *en Estudios Jurídicos, Ministerio Fiscal IV*, 1999, pp. 544 y ss. También en MARCHENA, "Algunos aspectos de internet", en http://www.fiscalia.org/, p. 4

291 Sobre la necesidad de esta cooperación internacional y los distintos trabajos llevados a cabo en el marco de la cooperación internacional, puede verse la Resolución de la Association International de Droit Penal sobre "Infractions informatiques et autres crimes contre la technologie informatique". *International Review of Penal Law 66 (1995)*, pp. 27 y ss. También en TIEDEMANN, K., "Computerkriminalität und Strafrecht". *Internationalen perspektiven in Kriminologie un Strafrecht II. Festschrift für Günther Kaiser zum 70. Geburtstag*. Berlin, 1998, pp. 1379-80.

Para la eficaz investigación de los hechos relacionados con la criminalidad informática resulta decisivo la aportación de quienes de distintas maneras intervienen en el conjunto de procesos relacionados con el fenómeno de Internet. La facilitación de datos relativos al uso de la red o el acceso por parte de los investigadores a algún punto de la red para obtener la constancia de determinados extremos, depende de los deberes jurídicos de colaboración que se establezcan para los distintos operadores de Internet y titulares de servidores.

Todas estas necesidades de la investigación criminal en esta materia requieren imprescindiblemente el sustento de instrumentos jurídicos de cooperación internacional. Sin esos cauces formalmente establecidos de cooperación entre las naciones para facilitar la información en el ámbito de la investigación y del proceso penal, los hechos relativos a la criminalidad informática permanecen inaccesibles dado su carácter transnacional. En este sentido el primer medio de cooperación internacional práctico lo constituye el Convenio sobre cyber-criminalidad del Consejo de Europa.[292] El mismo establece la armonización legislativa en materia penal sustantiva y procesal penal, así como medidas de auténtica cooperación internacional para el desarrollo de la investigación y procedimiento penal en esta materia. El propio Convenio declara como fines perseguidos completar la normativa de investigación y procedimiento penal con vistas a su mayor eficacia en la recogida de pruebas electrónicas de una infracción penal en el ámbito de hechos relacionados con sistemas y datos informáticos.

c) Vinculado a lo que se acaba de mencionar se presenta lo relativo a la intervención de comunicaciones electrónicas durante la investigación de los hechos.[293] En España –claramente después

292 Convenio del Consejo de Europa sobre cyber-criminalidad. Convenio todavía pendiente de ratificación. Entrará en vigor a los tres meses de la ratificación de cinco Estados, tres de los cuales al menos deben ser miembros del Consejo de Europa.

293 Una adecuada exposición de esta problemática en HERNÁNDEZ GUERRERO , F.J./ ÁLVAREZ DE LOS RÍOS, J.L., "Medios informáticos y proceso penal", *en Estudios Jurídicos, Ministerio Fiscal IV*, 1999, pp. 496 y ss. que se toma como referencia en los comentarios que siguen. Desde la perspectiva internacional también se ha

de la reforma procesal de 1988– no existe inconveniente legal para la intervención de cualquier tipo de comunicación de acuerdo a lo previsto en el art. 579 LECrim.

Ahora bien al no existir una previsión legal expresa sobre la intervención de comunicaciones electrónicas los problemas se plantean en la asimilación de éstas a determinadas formas de comunicaciones y la posible diferenciación, en cuanto al régimen legal, según el momento en el que se encuentre la comunicación (envío, interceptación, almacenamiento), tal y como se hace en otras legislaciones y parecen patrocinar los documentos e instrumentos de trabajo internacionales en esta materia. Por razón de su mayor semejanza se entiende asimilable el correo electrónico al mensaje telegráfico,[294] aplicándose también el régimen de intervenciones de éste para el caso de apertura y registro de las comunicaciones (especialmente arts. 583-4 y 586 LECrim.).

Debe entenderse que esta asimilación afecta a los mensajes de correo electrónicos almacenados en el servidor de acceso a Internet, lo que implica la observancia de una serie de requisitos muy estrictos y superiores a los de las comunicaciones telefónicas. Así el Auto motivado de la autoridad Judicial debe determinar las comunicaciones que deben ser detenidas o registradas, el interesado debe ser citado para presenciar la apertura y registro y la apertura debe ser practicada directamente por el Juez, seleccionando lo que interese a la causa.

En el caso del correo electrónico este proceso deberá ser practicado previa remisión de las copias de los mensajes almacenados en

---

puesto de relieve la novedad e importancia de este medio de investigación a la vez que la necesidad de su sometimiento a los principios de gravedad y proporcionalidad. Así la Resolución de la Association internationale de Droit Penal sobre "Infractions Informatiques et autres crimes contre la technologie informatique". *International Review of Penal Law 66 (1995),* pp. 32 y 33, puntos 14, 18 y 19.

294 En este sentido HERNÁNDEZ GUERRRO F.J./ÁLVAREZ DE LOS RÍOS, J.L., "Medios informáticos y proceso penal", en *Estudios Jurídicos, Ministerio Fiscal IV*, 1999, p. 497.

el sistema informático.[295] Este régimen legal introduce sin duda problemas prácticos, en perjuicio de la eficacia de la investigación, dado el volumen de comunicaciones que pueden recibirse por este conducto. Por ello se propone la utilización de programas de filtrado de textos, evitando la lectura de mensaje a mensaje por parte del Juez, para no hacer completamente impracticable este tipo de intervenciones.

La regulación legal admite de manera diferenciada "la observación" de cualquier tipo de comunicación de las que se sirvan para la realización de sus fines delictivos las personas sobre las que existan indicios de responsabilidad criminal. Este será el caso de la interceptación de los mensajes de correo electrónico en tránsito, asimilados ahora al régimen de las intervenciones sobre comunicaciones telefónicas, desarrollado en sus detalles por la Jurisprudencia. En este sentido la sentencia de 26 de febrero de 2000[296] señala hasta ocho requisitos en este tipo de intervenciones: "En todo caso, los autos cuestionados, cumplen los requisitos necesarios constitucionales y legales para acordar tal medida judicial, conforme a una reiterada doctrina de esta Sala –cfr. Sentencias de fechas 19 y 20 de enero, 3, 4, 7, l 1 y 20 de febrero, 3 y 22 de abril, 11 de mayo, 29 de julio, 21, 23 y 28 de septiembre, 23, 10 y 16 de noviembre 1999 y del TC 21/1998 de 15 de junio, 49/1999 de 5 abril–, que señalan que en las intervenciones telefónicas son principios básicos, sin cuya observancia se produce la vulneración del derecho fundamental, los siguientes:

1.º la exclusividad jurisdiccional en el sentido de que únicamente por la autoridad judicial se pueden establecer restricciones y derogaciones al derecho, al secreto de las comunicaciones telefónicas.

---

295 HERNÁNDEZ GUERRERO F.J./ÁLVAREZ DE LOS RÍOS, J.L., "Medios informáticos y proceso penal", *en Estudios Jurídicos, Ministerio Fiscal IV*, 1999, p. 497.

296 BDE 361/2000. Sobre ello exhaustivamente la Circular de la FGE 1/1999 "La intervención de las Comunicaciones telefónicas en el seno de los procesos penales". Véase también la Consulta 1/1999, igualmente emitida por la FGE, sobre "Tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones" que, aunque va dirigida principalmente a dirimir sobre la posible capacidad autónoma de investigación de los Fiscales sobre datos personales en el campo de las telecomunicaciones, hace algunas consideraciones interesantes para nuestro tema.

2.º La finalidad exclusivamente probatoria de las interceptaciones para establecer la existencia de delito y descubrimiento de las personas responsables del mismo (sentencia del TS de 12 de septiembre de 1994).

3.º La excepcionalidad de la medida, que sólo habrá de adoptarse cuando no exista otro medio de investigación del delito, que sea de menor incidencia y causación de daños sobre los derechos y libertades fundamentales del individuo que los que inciden sobre la intimidad personal y el secreto de las comunicaciones (auto de 18 de junio de 1992).

4.º Fundamentación de la medida, en el doble sentido de su proporcionalidad y motivación. Desde el primer punto de vista es exigible que (como expresa también la TC S 7/1994, de 17 de enero, que aunque dictada sobre tema distinto establece una doctrina genérica sobre tal principio) exista una proporción entre la intromisión que esa clase de prueba supone en la intimidad de una persona y la finalidad que se busca con ella. Proporcionalidad que el TEDH ha asentado en la satisfacción de una necesidad social imperiosa y "proporcionada a la finalidad legítima perseguida" –SS. TEDH 7 de diciembre de 1976 (caso Handyside); 26 de abril de 1979 (caso "The Sunday Times"); 24 de marzo de 1988 (caso Olsson); 21 de junio de 1988 (caso Berrehab), etc.– y que la sentencia de esta Sala de 25 de junio de 1993 matiza en el sentido de que ha de valorarse poniendo el acento no sólo en la gravedad de la pena fijada al delito investigado, sino también en la trascendencia social del tipo.

En cuanto a la motivación de la autorización judicial que habilita y legitima la intervención, en los términos del art. 18.3 CE, aparte de ser exigencia genérica impuesta a toda resolución judicial por el art. 120.3 CE, resulta mucho más necesaria en los casos en que la decisión del juez afecta a derechos fundamentales, como señaló la TC S 56/1987, de 14 de mayo, al recordar que "cuando se coarta el libre ejercicio de los derechos fundamentales reconocidos en la CE, el acto es tan grave que necesita encontrar una causa especial, suficientemente explicada, para que los destinatarios conozcan las razones del sacrificio de su derecho".

Sin embargo, y sin renunciar a tal exigencia, esta Sala la ha matizado en un doble sentido: primero, que en cuanto la medida no es

posterior al descubrimiento del delito, sino que se dirige a la averiguación y descubrimiento del delincuente (art. 126 CE) el *fumus boni iuris* tiene en tal caso una intensidad menor, en tanto que, como señala la TC S 341/1993, de 18 de noviembre, la autorización judicial es defectiva de la flagrancia, pues en ella queda excusada aquella autorización judicial, precisamente porque la comisión del delito se percibe con evidencia, evidencia no exigible en el otro caso (TS S de 7 de mayo de 1994, ya citada), lo que quiere decir que, como es obvio, de existir ya pruebas y constancia del delito sería superflua tal medida adicional, que si se adopta en fase de investigación es precisamente para comprobar y corroborar la certeza de los indicios no meras sospechas o conjeturas del delito que se investiga y que está por ello en fase de presunción, por lo que sobre él no tiene por qué existir una prueba; y segundo, que aunque lo correcto y deseable es que los fundamentos de la medida se expresen en el auto que la acuerde, no puede negarse la existencia de motivación cuando explícita o implícitamente se conoce la razón y el porqué del acuerdo (TS S de 5 de julio de 1993), con lo que la remisión a las razones de la solicitud, cuando éstas son conocidas y fundadas, complementan e integran la motivación de la resolución judicial.

5.º Especialidad; principio que significa que "no cabe, obviamente, decretar una intervención telefónica para tratar de descubrir, en general, sin la adecuada precisión, actos delictivos" y que "no es correcto extender autorización prácticamente en blanco" (TS A de 18 de junio, citado) exigiéndose concretar el fin del objeto de la intervención y que éste no sea rebasado. Lo que también ha sido matizado en el sentido de que no se vulnera la especialidad y ésta se da cuando no se produce una novación del tipo penal investigado, sino una adición o suma (TS SS de 2 de julio de 1993 y 21 de enero de 1994); así como que no puede renunciarse a investigar la *notitia criminis* incidentalmente descubierta en una intervención dirigida a otro fin, aunque ello hace precisa una nueva autorización judicial específica o una investigación diferente de la que aquélla sea mero punto de arranque (S.TS. 15 de julio de 1993).

6.º Control judicial. Control que como el afectado no conoce la medida y, por ello, no la puede impugnar ha de garantizar sus derechos futuros, por lo que aquél debe ser riguroso. Ello implica que la recepción de las cintas ha de ser íntegra y original, sin perjuicio de

su ulterior copia, siempre bajo fe de Secretario, cuando razones técnicas lo hagan preciso. Igualmente la transcripción mecanográfica ha de hacerse con compulsa y fe de Secretario. Y por último, es al juez y no a la Policía a quien compete determinar y seleccionar los pasajes que se entiendan útiles para la instrucción de la causa, excluyendo los que carezcan de relevancia para la investigación y, sobre todo, aquellos que, por afectar a la intimidad de terceros ajenos al proceso y cuyas conversaciones no sean de interés para la causa, deben con mayor razón ser excluidos de la publicidad.

7.º La limitación temporal de la utilización de la medida interceptadora de las comunicaciones telefónicas. La LECrim. autoriza (art. 579.3) períodos trimestrales individuales, pero no podrá prorrogarse la intervención de manera indefinida o excesiva porque ello la convertiría en desproporcionada e ilegal (S 9 de mayo de 1994).

8.º La existencia previa de un procedimiento de investigación penal, aunque cabe sea la intervención de las telecomunicaciones, la que ponga en marcha un verdadero procedimiento criminal, pero sin que puedan autorizarse intervenciones telefónicas de carácter previo a la iniciación de éste (SS 25 de junio de 1993 y 25 de marzo de 1994).

3. Las comunicaciones electrónicas como medio de prueba

Cuando nos referimos a los medios de prueba quiere decirse que nos encontramos ya en la fase final de plenario en el proceso penal, en el que se va a llevar a cabo el enjuiciamiento y fallo de los hechos objeto de acusación. Desbordada ya la fase de investigación e instrucción del proceso, cabe preguntarse entonces por el modo en el que lo averiguado durante la investigación en relación a los medios electrónicos de comunicación y sus manifestaciones o plasmaciones (documento electrónico) tienen cabida en el acto del juicio oral.[297] Se trata de determinar la efectividad procesal de esa

297 Estos aspectos respecto al documento en el proceso, aunque sin una clara distinción entre prueba civil y prueba penal en CARRASCOSA ÁLVAREZ, V., "El documento electrónico como medio de prueba", en *Dogmática penal, política criminal y criminología en evolución*, ROMEO CASABONA (Ed.), Universidad de La Laguna, 1997, pp. 187 y ss.

serie de actuaciones previas en referencia a los datos electrónicos de valor relevante para la decisión del proceso.

a) La irrupción de estos modernos medios de telecomunicación y otros avances técnicos han supuesto la necesidad de reflexionar sobre su posible utilización en la investigación criminal y también su validez como medio de prueba con el que el Tribunal pueda formar su convicción en el fallo. Este último aspecto es el que nos interesa en este momento.

Para afrontar este tema puede resultar válida la distinción entre fuente de prueba y medio de prueba que se remonta a CARNELUTTI.[298] La fuente de prueba designa una realidad extrajurídica preexistente e independiente del proceso y el medio de prueba alude a la actividad necesaria para introducirla en el proceso. La regulación procesal no afecta por tanto a las fuentes de prueba, sino que la realidad social las manifiesta. Pero las leyes sí se encargan de establecer el modo por el cual tales fuentes de prueba se incorporan al proceso. Desde este punto de vista también cabe plantear coherentemente el problema de considerar la eficacia de todos aquellos avances científicos que no son recogidos expresamente como medios de prueba en la regulación legal.

También se avala su admisión en el proceso de los nuevos medios de prueba no previstos expresamente con la declaración constitucional del art. 24 por la que se afirma el derecho de los ciudadanos "a utilizar los medios de prueba pertinentes para su defensa". Igualmente los principios de tutela judicial efectiva y el de presunción de inocencia refuerzan la posibilidad de acudir a todos los medios de prueba idóneos, salvo que –de acuerdo a la interpretación del Tribunal Constitucional–[299] tal práctica implique un abuso, exista ánimo de dilatar el proceso o se prevean grandes dificultades en su práctica.

---

298 Véase al respecto NOYA FERREIRO, Mª.L., *La intervención de comunicaciones orales directas en el proceso penal*. Tirant lo blanch, 2000, pp. 303 y ss. A esta autora seguimos en la exposición de esta distinción. También mantiene y utiliza esta distinción la sentencia TS de 26 junio de 2000, BDE 810/2000, en un caso de escuchas telefónicas.

299 Así NOYA FERREIRO, Mª.L., *La intervención de comunicaciones orales directas en el proceso penal*. Tirant lo blanch, 2000, p. 305.

Naturalmente la legislación procesal penal, originaria del siglo pasado, no pudo prever las consecuencias que para la prueba iban a tener los modernos avances en la telemática y otros campos. No existiendo, por tanto, una regulación expresa respecto al cauce procesal para insertar estos avances tecnológicos en el mismo juicio oral, es preciso acogerse a alguno de los ya previstos. Hay que tener en cuenta que de acuerdo a la concepción del proceso penal en la legislación española, en principio, únicamente constituye prueba valorable por el tribunal la practicada durante el juicio oral (art. 741 LECrim.).

En el sentido señalado la sentencia TS de 2 de junio de 2000,[300] para un caso de interceptación de las comunicaciones telefónicas, señala que las mismas "pueden ser incorporadas al proceso como medio autónomo de prueba, bien por sí misma con audición directamente por el Tribunal de las cintas, bien a través de su transcripción mecanográfica, como documentación de un acto sumarial previo, o a través de las declaraciones testificales de los funcionarios policiales que escucharon las conversaciones intervenidas". Lo relevante en este momento procesal es que tal incorporación al plenario se realice bajo el respeto a los principios de inmediación, contradicción y publicidad para que puedan ser tomados como piezas de convicción en la finalización del proceso.

Es decir, que respecto a la efectividad probatoria de los resultados obtenidos mediante este tipo de intervenciones de comunicaciones ya no se plantea el cómo de la práctica material de una medida limitativa del derecho constitucional al secreto de las comunicaciones y sus requisitos, sino el derecho a un proceso con todas las garantías.[301]

La práctica material durante el período de investigación sin los requisitos que le son propios, que ya hemos visto, convertiría la misma en prueba ilícita, de imposible apreciación por el Tribunal para formar su convicción sobre los hechos y la responsabilidad de los imputados. A este respecto es necesario distinguir, por el diver-

300 BDE 766/2000.

301 Como señala la sentencia TS de 19 de mayo de 2000 –BDE 74/2000– FJ sexto y decimoséptimo.

so régimen legal de garantías de que deben rodearse, las distintas clases de datos relativos a las telecomunicaciones. Por una parte los datos relativos al contenido de las comunicaciones. Además los datos de tráfico generados por las comunicaciones establecidas durante la prestación del servicio. Y finalmente los datos de los abonados necesarios para la prestación del servicio pero no generados en los procesos de comunicación. Únicamente los primeros se consideran que afectan al Derecho constitucional al secreto de las comunicaciones, obteniendo el máximo grado de protección.

En este sentido la Sentencia del TS de 22 de marzo de 1999[302] entiende que la solicitud por el Juzgado de Instrucción de un listado de llamadas telefónicas mediante Providencia (sin motivación) no vulnera el Derecho Fundamental al secreto de las comunicaciones, pues no integra el objeto de protección constitucional, no afectando al contenido de tal Derecho. El Tribunal de instancia había mantenido la tesis contraria considerando tal extremo prueba nula por violación del Derecho Fundamental. La sala segunda del Supremo recuerda sin embargo que no se produce vulneración de las garantías pues se trata de datos de carácter personal custodiados según las previsiones de la LO 5/1992 que únicamente exige intervención de autoridad Judicial pero sin ulteriores requisitos.

Ahora, en el momento del plenario, practicada legítimamente la intervención, se trata de insertar la misma en el juicio oral de manera que pueda ser considerada por el Tribunal bajo el principio de libre valoración de la prueba con posible incidencia en la inicial presunción de inocencia de los acusados.

La práctica en el juicio oral se llevará a cabo mediante alguna de las fórmulas previstas y ya mencionadas, garantizándose el respeto a los principios de contradicción, publicidad e inmediación. Si es preciso efectuar una autenticación previa al propio juicio oral de los contenidos y datos de las comunicaciones, se realiza bajo la fe pública judicial y con asistencia de los letrados defensores. Así la sentencia 26 de junio 2000[303] señala que en este tipo de interven-

302 *Actualidad Penal* 1999-2, 424, pp. 1101 y ss.

303 BDE 810/2000.

ciones de las comunicaciones "su validez dependerá de la concurrencia de las condiciones de certeza y credibilidad, disponibilidad para las partes y sometimiento a contradicción en el plenario". En definitiva estas modalidades limitativas de derechos constitucionales, resultando legítimas, son hábiles para desvirtuar la presunción de inocencia constitucional, de acuerdo al principio de libre valoración de la prueba por el Tribunal.

b) A continuación nos vamos a referir al instrumento electrónico por excelencia y a algunas de sus peculiaridades como elemento de prueba en el proceso penal. En conexión con el documento digital dedicaremos algún espacio también a la firma electrónica.

El concepto clásico de documento apegado ineludiblemente a las técnicas disponibles hasta hace pocos años para formalizar las declaraciones de voluntad, se ha visto sacudido por la irrupción del documento electrónico que introduce cambios significativos aunque a lo mejor no tantos como pudiera parecer. El documento electrónico presenta diferencias externas importantes con el concepto tradicional, por lo que se pueden plantear al intérprete dudas sobre su posible incorporación al proceso.[304]

Así en cuanto al soporte material del contenido del documento, electrónicamente estamos ante soportes magnéticos, frente al papel como representación usual del documento. El lenguaje del que se vale el documento electrónico para manifestar su contenido, consiste en un lenguaje codificado diverso del escrito convencional. La firma como signo de autenticidad e identidad del declarante también sufre alteraciones. En el documento clásico consiste en la firma autógrafa mediante un trazado gráfico y en el documento electrónico se trata de firmas digitales basadas en técnicas criptográficas. Además el documento electrónico no es perceptible directamente, pues requiere un ordenador como intermediario necesario para acceder a su contenido.

---

304 Sobre ello HERNÁNDEZ GUERRERO, F.J./ÁLVAREZ DE LOS RÍOS, J.L., "Medios informáticos y proceso penal", *en Estudios Jurídicos, Ministerio Fiscal IV*, 1999, pp. 575 y ss. Véase también SUÑÉ LLINAS, E. "Documento digital y firma electrónica", *Revista General de Legislación y Jurisprudencia* 2/2000, pp. 209 y ss.

No existe en la legislación procesal penal una regulación específica del documento electrónico como medio de prueba. Por ello se plantea su asimilación a otros medios ya reconocidos y regulados. Así cabe entender que su mayor proximidad se da con el documento a efectos probatorios, con el cual no le separan distancias insalvables si –despojado el concepto tradicional de los detalles más aferrados a situaciones históricas concretas– se concibe el mismo como "representación destinada e idónea para reproducir una manifestación de voluntad".[305] En el ámbito del derecho penal material se entiende que el Código Penal de 1995 ha reconocido ya la inclusión del documento electrónico al señalar el art. 26: "A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica".[306] Incluso la propia jurisprudencia va abriendo camino a su incorporación al proceso.[307]

La mayor o menor facilidad para su incorporación puede depender de los mecanismos de autenticación que se consigan establecer en el tráfico documental electrónico. De modo que aquellos documentos que no presenten las máximas garantías (firma electrónica en sus distintas posibilidades) o se hagan dudosos pueden ser incorporados mediante previo reconocimiento judicial o bien mediante prueba pericial.

c) La firma digital se establece para evitar los problemas de autenticidad del documento electrónico. Frente a los problemas de vulnerabilidad de los documentos contenidos y transmitidos en redes informáticas, la firma electrónica aparece como un medio que permite conseguir una mayor seguridad en el tráfico de este tipo

305 Definición recogida en HERNÁNDEZ GUERRERO, F.J./ÁLVAREZ DE LOS RÍOS, J.L., "Medios informáticos y proceso penal", en *Estudios Jurídicos, Ministerio Fiscal IV*, 1999, p. 578.

306 Véase GARCÍA CANTIZANO, Mª. C., *Falsedades Documentales*, Tirant lo blanch, 1997, especialmente pp. 45 y ss.

307 Así la sentencia TS de 3 de noviembre de 1997 (A. 8251), citada en HERNÁNDEZ GUERRERO, F.J./ÁLVAREZ DE LOS RÍOS, J.L., "Medios informáticos y proceso penal", en *Estudios Jurídicos, Ministerio Fiscal IV*, 1999, p. 580.

de documentación. En realidad hay que tener en cuenta que únicamente el sistema denominado de firma digital avanzada posee la misma eficacia jurídica que la firma manuscrita conforme a lo señalado en el art. 3.1 del RD Ley 14/1999 sobre firma electrónica.[308] Ello no obstante no quiere decir que otras firmas digitales distintas de la avanzada carezcan de eficacia jurídica.

La firma digital se basa en la criptografía de claves asimétricas generadas informáticamente.[309] Una de las claves, conocida como clave privada, sólo es conocida por su titular. La clave pública se da a conocer a las Entidades de Certificación que van a garantizar la autenticidad de la firma digital. Con la clave pública el receptor del mensaje desencripta su contenido y constata que ha sido encriptado por quien poseía la clave privada. El receptor puede comprobar así la identidad del emisor y la autenticidad del mensaje. El sistema de firma electrónica se logra mediante la participación de las Entidades de Certificación, que mediante el registro de las claves públicas permiten identificar al titular de cada clave pública. Para activar la firma electrónica se dispone de un soporte o tarjeta de identificación electrónica, accesible mediante la introducción del correspondiente número de identificación personal.[310]

DÍAZ FRAILE señala las distintas funciones que cumple la firma electrónica, especialmente en consideración a la contratación electrónica por ser este ámbito en el que la firma digital posee mayor relevancia, pero con trascendencia para todos los campos. Por una parte permite establecer que con quien se contrata es quien dice ser (autenticación). Además, respecto al contenido, avala que el mensaje no ha sido alterado o modificado (respeto a la integridad). También impide que se acceda al mensaje o documento de forma inconsentida (confidencialidad). Por último hace que una vez aceptado no pueda ser rechazado sin que exista pacto de retracción o desistimiento (función de no repudiación).

---

308 Véase SUÑÉ LLINAS, E., "Documento digital y firma electrónica", *Revista General de Legislación y Jurisprudencia* 2/2000, p. 213.

309 Véase HERNÁNDEZ GUERRERO, F.J./ÁLVAREZ DE LOS RÍOS, J.L., "Medios informáticos y proceso penal", en *Estudios Jurídicos, Ministerio Fiscal IV*, 1999, p. 582.

310 DE MIGUEL ASENSIO, P.A., *Derecho Privado de Internet*, Civitas, 2000, p. 338.

Por su parte HERNÁNDEZ GUERRERO/ÁLVAREZ DE LOS RÍOS[311] señalan algunos problemas que pueden aparecer respecto al empleo de la firma digital.[312] Un primer problema hace relación a la identidad del firmante y otro a la validez temporal de la firma digital. Afirma este autor que en realidad la firma digital sólo prueba que se utilizó la clave privada del sujeto y no, sin embargo, el acto personal de la firma. Esto sucede a diferencia de la firma autógrafa que consiste en una biometría y, por tanto, siendo auténtica, confirma el acto personal de la firma. De manera que no existiría una necesaria coincidencia entre presencia de la correcta firma digital y la voluntad real de firma del titular de la clave privada. Se presenta un problema entonces de autoría real de la firma electrónica con una posible falsedad en la misma.

Lo cierto es que en la firma autógrafa no dejan de presentarse situaciones en algún sentido semejantes. Puede suceder, como también en la autógrafa, que se haya inutilizado su clave sin su consentimiento (imitación de la autógrafa –falsedad– o, incluso, que se haya coaccionado para conseguir que la persona suscriba el documento –posible extorsión, falsedad...) En definitiva que en ambas modalidades de firma no dejarán de presentarse supuestos en los que la presencia de la firma no se vea respaldada por una inequívoca voluntad de asumir las obligaciones y derechos reflejados en el documento.

Además las claves empleadas en la firma digital tienen asignadas de forma anticipada un período temporal de validez, durante el que su empleo resulta legítimo y produce todos los efectos legalmente previstos. Puede darse la firma electrónica una vez acabado el plazo de vigencia de la clave, situación con efectos todavía por determinar. Incluso hay que tener en cuenta que el período de validez puede revocarse por anticipado o puede igualmente revocarse por la pérdida de la clave, introduciendo supuestos problemáticos.

311 "Medios informáticos y proceso penal", en *Estudios Jurídicos, Ministerio Fiscal IV*, 1999, pp. 583-4.

312 Otros problemas mencionados en DE MIGUEL ASENSIO, P.A., *Derecho Privado de Internet*, Civitas, 2000, pp. 341 y ss.

BIBLIOGRAFÍA

ACHENBACH "*Das* Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität". *Neue Juristisches Wocheschrift* 30 (1986).

ASSOCIATION INTERNATIONALE DE DROIT PENAL. Resolutions sections II, "Computer crimes and other crimes against information technology". *International Review of Penal Law* 66/1995.

BAON RAMÍREZ, R., "Visión general de la informática en el nuevo Código Penal". *Ámbito Jurídico de las Tecnologías de la información*. *Cuadernos de Derecho Judicial, CGPJ,* 1996.

CARSTEN, U., "Computerbetrug (&263ª StGB*)", Internet-Zeitschrift für Rechtsinformatik,* en http://www.jurpc.de/aufsatz/.

CHOCLAN MONTALVO, J.A., "Estafa por computación y criminalidad económica vinculada a la informática", *Actualidad Penal 1997.*

CHOCLAN MONTALVO, J.A., *El delito de estafa*, Bosch 2000.

CARRASCOSA ÁLVAREZ, V., "El documento electrónico como medio de prueba", en *Dogmática penal, política criminal y criminología en evolución*, ROMEO CASABONA (Ed.), Universidad de La Laguna, 1997.

CONDE-PUMPIDO FERREIRO. *Estafas*, Tirant lo blanch, 1997.

CONSENTINO, G., y otros. "Tras los pasos de la seguridad perdida. Delitos informáticos". *Informática y Derecho* 23, 26 (1998).

CONVENIO DEL CONSEJO DE EUROPA SOBRE CYBER-CRIMINALIDAD.

CORCOY, M./JOSHI, U., "Delitos contra el patrimonio cometidos por medio informáticos". *Revista Jurídica de Cataluña* 3 (1988).

CORCOY BIDASOLO, M., "Protección penal del sabotaje informático. Especial consideración de los delitos de daños". *La Ley,* vol. 1, nº 2400 (1990).

CORRIAS LUCENTE, G., *Il diritto penale dei mezzi di comunicazione di massa*. CEDAM, 2000.

CUESTA ARZAMENDI, J.L., DE LA. "Las nuevas corrientes internacionales en materia de persecución de delitos sexuales a la luz de los documentos de organismos internacionales y europeos". *Delitos contra la libertad sexual 21. Estudios de Derecho Judicial*, CGPJ, 1999.

DE MIGUEL ASENSIO, P.A., *Derecho Privado de Internet*, Civitas, 2000.

DEL PESO NAVARRO, E., "El pago mediante medios electrónicos". *Actualidad Informática Aranzadi* 5 (1992).

FERNÁNDEZ LÓPEZ, J.M., "La nueva regulación de la protección de datos personales en España a partir de la Ley Orgánica 15/1999 de 13 de diciembre". *Ius & Law* 1 y 2 (2001).

GARCÍA CANTIZANO, Mª.C., *Falsedades Documentales*, Tirant lo blanch, 1997.

GONZÁLEZ GÓMEZ. *El tipo básico de los delitos contra la propiedad intelectual*. Tecnos, Madrid, 1998.

GONZÁLEZ RUS, J.J., "Protección penal de sistemas, elementos, datos y programas informáticos". *Revista Electrónica de Ciencia Penal y Criminología* 1 (1999), en http://www.criminet.ugr.es/recpc/.

GUTIÉRREZ FRANCÉS, Mª.L., "*Fraude informático y estafa*", Ministerio de Justicia, 1991.

GUTIÉRREZ FRANCÉS, M.L., "En torno a los fraudes informáticos en el Derecho español"*, Actualidad Informática Aranzadi* 11 (1994).

GUTIÉRREZ FRANCÉS, Mª.L., "Delincuencia económica e informática en el nuevo Código Penal". *Ambito Jurídico de las Tecnologías de la información*. *Cuadernos de Derecho Judicial, CGPJ,* 1996.

HERNÁNDEZ, C. Hackers. *Los piratas del Chip y de Internet*. Libro electrónico en http://perso.wanadoo.es/snickers/.

HERNÁNDEZ GUERRERO, F.J./ÁLVAREZ DE LOS RÍOS, J.L., "Medios informáticos y proceso penal", *en Estudios Jurídicos, Ministerio Fiscal IV*, 1999.

JAREÑO LEAL, A. / DOVAL PAIS, A., "Revelación de datos personales, intimidad e informática". *El Nuevo Derecho Penal Español. Estudios Penales en Memoria del Profesor José Manuel Valle Muñiz*, Aranzadi, 2001.

KINDHÄUSER, U., "Der Computerbetrug (% 263ª StGB) –ein Betrug?", *Festschrift für Geral GrünWald*, Baden-Baden, 1999.

MARCHENA GÓMEZ, M., "Intimidad e informática: la protección jurisdiccional del *habeas data". Boletín de Información. Ministerio de Justicia e Interior, nº 1768 (1996)*.

MARCHENA GÓMEZ, M., "Prevención de la delincuencia tecnológica". *Derecho de Internet. Contratación electrónica y Firma digital*. Aranzadi, 2000.

MARCHENA GÓMEZ, M., "Algunos aspectos procesales de Internet".

MATELLANES RODRÍGUEZ, N., "Algunas notas sobre las formas de delincuencia informática en el Código Penal". *Hacia un Derecho Penal sin fronteras* (DIEGO DÍAZ-SANTOS, Mª R./SÁNCHEZ LÓPEZ, V., Coordinadoras), Colex, 2000.

MILITELLO, V., "Nuoeve esigenze de tutela penale e trattamento electtronico della informazione", *Verso un nuovo Codice penale*, Giuffrè, Milano, 1993.

MORANT RAMÓN, J.L., "El peritaje en los delitos informáticos: problemas, lenguajes y criterios". *Ámbito Jurídico de las Tecnologías de la información*. *Cuadernos de Derecho Judicial, CGPJ,* 1996.

MORON LERMA, E., *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red*, Aranzadi, 2000.

NOYA FERREIRO, Mª.L., *La intervención de comunicaciones orales directas en el proceso penal*. Tirant lo blanch, 2000.

ORTS BERENGUER, E./SUÁREZ-MIRA RODRÍGUEZ, C., Los delitos contra la libertad e indemnidad sexuales, Tirant lo blanch, 2001.

PANSIER, F.J./JEZ, E., *La criminalité sur l´Internet*, PUF, 2000.

PICA, G., *Diritto penale delle technologie informatiche*, Utet, Torino, 1999.

POMANTE, G., *Internet e Criminalità*, Torino, 1999.

RIBAS ALEJANDRO, J., *Aspectos jurídicos del comercio electrónico en Internet*. Aranzadi, 1998.

RODRÍGUEZ PADRÓN, C., "Los delitos de utilización de menores o incapaces con fines o espectáculos exhibicionistas o pornográficos o para la elaboración de material pornográfico". *Delitos contra la libertad sexual 21, Estudios de Derecho Judicial*, CGPJ, 1999.

RODRÍGUEZ RAMOS, L., "Descubrimiento y revelación de secretos en el nuevo Código Penal". *Derecho al honor, a la intimidad y a la propia imagen II. Cuadernos de Derecho Judicial*, CGPJ, 1998.

ROJO GARCÍA, J.C., "Pornografía infantil en Internet". *Boletín Criminológico* 52/2001.

ROMEO CASABONA, C.Mª., Poder informático y Seguridad Jurídica. Fundesco, 1987.

ROMEO CASABONA, C.M., "La protección penal del software en el Derecho español", *Actualidad Penal* 35/1988.

SCHMID, N., *Computer sowie Check- und Kreditkarten- Kriminalität*, Zürich 1994.

SCHREIBER, W., "La delincuencia asistida por ordenador", *Interpol* 464 (1997).

SCHWARZENEGGER, CH., "Der raümliche Geltungsbereich des Strafrechts im Internet". *Schweizerishes Zeitschrift für Strafrecht* 2/2000.

SEMINARA, S., "La pirateria su Internet e il diritto penale*", Rivista Trimestrale di diritto penale dell´economia* 1,2 (1997).

SIEBER, U., *Computerkriminalität und Strafrecht*, München, 1977.

SIEBER, U., "Documentación para una aproximación al delito informático". *Delincuencia informática*. MIR PUIG (Comp.), PPU, Barcelona, 1992.

SIEBER, U., "Criminalidad informática: peligro y prevención". *Delincuencia informática*. (MIR PUIG Comp.). PPU, Barcelona, 1992.

SUÑÉ LLINAS, E., "Documento digital y firma electrónica", *Revista General de Legislación y Jurisprudencia* 2/2000.

TAMARIT SUMALLA, J.M., *La protección penal del menor frente al abuso y la explotación sexual*. Aranzadi, 2000.

TÉLLEZ AGUILERA, A., *Nuevas Tecnologías. Intimnidad y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*. Edisofern, 2001.

TORRES-DULCE LINFANTE, E., "Jurisprudencia del Tribunal Europeo de Derechos Humanos en materia de honor, intimidad y propia imagen". *Derecho al honor, a la intimidad y a la propia imagen II. Cuadernos de Derecho Judicial*, CGPJ, 1998.

TIEDEMANN, K., "Computerkriminalität und Strafrecht". *Internationale Perspektiven in kriminologie und Strafrecht. Festschrift für Günther Kaiser zum 70. Geburtstag II*. Berlín, 1998.

USTARAN, E., "Pornografía en Internet: la respuesta legal". *La Ley,* vol. I, (1997).

VASSILAKI, I.E., "Strafverfolgung der grenzüberschreitenden Internet-Kriminalität, *Computer und Recht* 9/1999.

ZENO-ZENCOVICH, V., "Il corpo del reato: pornografia minorile, libertad di pensiero e cultura giuridica". *Politica del diritto 4 (1998).*

El profesor Ricardo Mata y Martín es doctor por la Universidad de Valladolid, España y Profesor Titular de Derecho Penal en la Universidad de Valladolid. Ha realizado estancias de Investigación para su preparación en Friburgo de Brisgovia (Alemania) en el Max-Planck-Institut für Auslandisches und Internationales Strafrecht. Es Premio Extraordinario de Licenciatura y está en posesión del Primer Sexenio de investigación reconocido por la Comisión Nacional de Evaluación de la Actividad Investigadora del Ministerio de Educación y Cultura de España. Entre sus publicaciones cuenta con tres monografías (una de ellas dedicada al mundo de las nuevas tecnologías: *Delincuencia informática y Derecho Penal*, Edisofer, Madrid 2001, otra *Bienes Jurídicos y Intermedios y delitos de peligro*, Granada 1997 y la primera sobre *El delito de robo con fuerza en las cosas*, Valencia 1995) y una veintena de artículos en revistas científicas nacionales e internacionales (entre ellos "Algunas consideraciones sobre informática y Derecho penal. El caso de la estafa informática" y "Algunos aspectos de la delincuencia patrimonial en el comercio electrónico"). Ha dirigido un Proyecto de Investigación sobre "El Derecho penal ante el reto de la criminalidad informática" con la Universidad Carlos III de Madrid y otro sobre la "La protección penal del consumidor en el comercio electrónico" con la Junta de Castilla y León. Ha sido invitado a impartir múltiples cursos como especialista sobre distintos ámbitos del Derecho penal en países como Argentina, Bolivia o Portugal. Participa en un Programa de la AECI sobre "Gobierno Electrónico" a desarrollar en Chile, Cuba y Uruguay. Igualmente toma parte en un Programa Alfa de la Unión Europea dedicado al "Gobierno Electrónico" con las Universidades de Münster, Belfast, Burgos, Zaragoza y Valladolid.

La obra constituye una referencia para el estudio de la delincuencia informática. Consta de tres partes. La primera parte dedicada a los aspectos generales y elementos comunes de los delitos vinculados a la informática (concepto de delito informático, bien jurídico, problemas criminológicos y políticos-criminales). La segunda parte, aborda distintos tipos penales de delincuencia informática (estafa informática, propiedad intelectual, daños, protección de la intimidad, pornografía y otros delitos contra la libertad e indemnidad sexual). Y la tercera parte, analiza algunos problemas procesales de la delincuencia informática (determinación de la ley aplicable, medios electrónicos y proceso penal).

ISBN 99924-57-27-9

9 789992 457276

Editorial Hispamer
Colección *Textos Jurídicos*

INSTITUTO CENTROAMERICANO DE ESTUDIOS PENALES
UNIVERSIDAD POLITÉCNICA DE NICARAGUA