INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS EN EL SISTEMA PENAL. APROXIMACIÓN AL DERECHO PENAL EN LA SOCIEDAD DE LA INFORMACIÓN

DR. ENRIQUE ANARTE BORRALLO
Profesor Asociado de Derecho Penal
Universidad de Huelva
anarte@uhu.es

PALABRAS CLAVE: Ciberdelincuencia • Delincuencia informática • Sociedad de la información
KEY WORDS: Cybercrime • Computer crime • Information Society

1. INTRODUCCIÓN

I). Las innovaciones tecnológicas apoyadas en la informática y en las redes de comunicación mundial, así como su expansión en las últimas décadas, han derivado en un nuevo paradigma sociológico nominado Sociedad de la Información[1] y/o del Conocimiento. En este sentido, el conocido *Informe Bangemann*[2] habla de una «*nueva revolución industrial*, basada en la información, que se puede procesar, almacenar, recuperar y comunicar de forma ilimitada e independiente de …, tiempo y distancia». Se trataría, según esto, de nuevos sistemas sociales[3] basados en los servicios, cuyos principios axiales dejarían de ser el capital y el trabajo para centrarse en el "conocimiento teórico"[4].

[1] Así la Exposición de Motivos del *Anteproyecto de Ley de Servicios de la Sociedad de la Información y de Comercio electrónico*, afirma que «lo que la Directiva 2000/31/CE [DO L178 de 17 de julio de 2000]denomina "sociedad de la información" viene determinado por la extraordinaria expansión de las redes de telecomunicaciones y en especial de Internet como vehículo de transmisión e intercambio de todo tipo de información». También ha sido objeto de recepción por parte de la Directiva 2001/29/CE, de 22 de mayo [DO L 167/11, de 22 de junio de 2001].
[2] Disponible en http://www.rewi.hu-berlin.de/datenschutz/report.html.
[3] Se pretende pues la superación de la "era industrial" y el intento de definición del llamado postindustrialismo. Sobre esta transformación, cf. David Lyon, "From postindustrialism to Information Society: A New Social Transformation?", Sociology, 20 (1986), p. 577-588; el mismo, *The Information Society: Issues and Illusions*, 1988, Cambridge: Basil Blackwell; el mismo, "The Information Society Concept in Public Policy", en Frank Gregory/Raymond Plant (eds), *Information Technology: The Public Issues*, 1989, Manchester: Manchester University Press; el mismo "Cyberspace Sociality: Controversies

II). De este entorno, la Exposición de Motivos del Convenio sobre ciberdelincuencia[5] subraya la digitalización y la convergencia y globalización de redes informáticas, aspectos que pueden ser completados en algunos detalles, aunque sin ánimo de exhaustividad[6]:

(a) El sistema depende directa e intensamente de tecnologías avanzadas de la información, basadas primordialmente en la automatización y en la digitalización[7]. Con todo, su aplicación no sólo tiene lugar en entornos socioeconómicos "sofisticados", sino en el ámbito cotidiano e incluso doméstico, lo que permite augurar que los impactos también repercutirán, aunque lógicamente con grados y modos diversos, en casi todas las formas delictivas[8] y en casi todas las instancias y mecanismos del control del delito.

(b) Estas tecnologías proporcionan una capacidad "ilimitada" de almacenaje, sistematización y accesibilidad de la información[9], que se ve acrecentada gracias a conexiones en red, principalmente Internet (*interconected set of networks*), que permite el acceso a todos los contenidos disponibles en cualquier punto de la red.

(c) Esto mismo además posibilita ilimitadas comunicaciones e intercambios de información, que se llevan a cabo de forma relativamente sencilla y descentralizada, por sujetos que actúan con bastante autonomía. En realidad, los intercambios pueden ser de muy diverso tipo: personales, comerciales, académicos, de ocio, ..., en tanto que la naturaleza virtual del sistema los posibilite.

(d) Se subraya también que cada sujeto interviniente puede ser, a la vez emisor y receptor de información[10]. Y, asimismo, que en ese sistema de comunicación e intercambio virtual los usuarios actúan, de forma más clara que para el resto de

over Computer-mediated Communication", en Brian Loader (ed.), *The Governance of Cyberspace*, 1997, Londres-Nueva York: Routlege. Pero, como pone de relieve el propio Lyon, *Postmodernidad* (trad. Belén Urrutia, de la segunda edición inglesa, *Postmodernity*, publicada en 1999), 2000, Madrid: Alianza, p. 17, «en cuanto intentamos hablar de la postmodernidad tropezamos con la modernidad», esto es, de alguna manera -igual que los teóricos de la Sociedad del Riesgo (en especial Ulricht Beck), la conciben como una segunda modernidad-, algunos de los trazos de la Sociedad de la Información estarían ya dibujados en la modernidad. En el terreno jurídico, esto probablemente se corresponde con una lectura de las nuevas regulaciones como producto del *evolucionismo jurídico*. Sobre ello, cf., por todos, el trabajo de Porras Nadales, en este volumen.

[4] Así David Lyon, *Postmodernidad*, como en la nota 3, p. 17

[5] Suscrito en Budapest el 23 de noviembre de 2001 y auspiciado por el Consejo de Europa (ETS núm. 185, firmado por España en esa misma fecha, pero aún no ratificado). Disponible tanto en la versión francesa como en la inglesa en http://conventions.coe.int.

[6] Para la mayor parte de las indicaciones que siguen, cf. Morón, *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red*, 1999, Pamplona: Aranzadi, *passim*, que, por otra parte, aunque emplea también con profusión el término sociedad de la información, destaca el de sociedad digital aludiendo principalmente a la superación del mundo analógico (p. 19 s).

[7] Para ser más precisos habría que diferenciar tres etapas postindustriales: la *era electrónica*, en la que aparecen y empiezan a propagarse los ordenadores personales; la *era de la información propiamente dicha*, en la que el uso de aquéllos se masifica, son introducidos en el ámbito doméstico y comienza su interconexión mediante redes; y la *era digital*, caracterizada por la normalización de todo tipo de redes informáticas, detectándose la identidad de una cultura diferenciada para la nueva sociedad "digital": la cibercultura, que «encarna la forma horizontal, simultánea, puramente espacial, de la transmisión», como ha destacado Primo Levy, *Sobre la cibercultura*, Revista de Occidente, 206 (1998), p. 31 (advirtiendo, no obstante, de la pluralidad del ciberculturas, Piscitelli, *Ciberculturas. En la era de las máquinas inteligentes*, 1995, Buenos Aires: Paidós).

[8] De modo que prácticamente todos los delitos podrán ser cometidos con medios informático-cibernéticos (cf., sólo Gutiérrez Francés, "Delincuencia económica e informática en el nuevo Código penal", en *Cuadernos de Derecho Judicial* [CDJ], 1996/XI [monográfico "Ámbito jurídico de las tecnologías de la información". Dir. M. A. Gallardo Ortiz], p. 250). Sobre esto, véase *infra* nota 28.

[9] Destaca el valor criminógeno de este aspecto, Corcoy Bidasolo, "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", en S. Mir Puig (comp.), *Delincuencia informática*, 1992, Barcelona: PPU, p. 145 y 176.

contactos sociales modernos, como sujetos anónimos. Con ello, en la Sociedad de la Información se realiza de forma paradigmática[11], uno de los aspectos de la sociedad del riesgo que la dogmática penal funcionalista más ha destacado, su anonimato[12], una característica que ya la Escuela de Chicago[13] identificó como el rasgo más patético de la existencia metropolitana. De este dato interesa tanto su dimensión individual, en el sentido de que el "ciudadano electrónico" puede aspirar a múltiples contactos sin ser identificado más que por su perfil informático o internauta, como la relativa al control social[14], en tanto que replantea las posibilidades y medios a través de los cuales la sociedad y las agencias correspondientes aspiran a ejercerlo.

Junto a ello, cabe indicar que también en otros rasgos comunes del patrón de conducta tecnológica -a saber, su virtualidad y su ambigüedad o ambivalencia o la crisis de la teoría de la acción humana, considerada como comportamiento racionalmente conducible- se advierten aspectos que pueden alcanzar especial interés jurídico-penal. En efecto, en la medida en que lo distancian del arquetipo de conducta penalmente relevante, esto es, la conducta comisiva intencional y directamente dañina del bien jurídico protegido individual, parece que se facilita la expansión de modelos de imputación "extraordinaria", que se basan fundamentalmente en la no evitabilidad y están más cerca de las directrices que rigen las reglas de la autoría mediata, la omisión, la *actio libera in causa* o de la estructura de los delitos de peligro contra bienes jurídicos colectivos, etcétera.

(e) Se produce asimismo una estrecha convergencia de las tecnologías informáticas con las telecomunicaciones, que se impulsan mutuamente generando sistemas telemáticos integrados e híbridos[15]. Todo ello en un contexto de renovación muy acelerado.

(f) En las caracterizaciones precedentes está ya implícito otro aspecto sustancial de la Sociedad de la Información: su carácter transnacional o, si se prefiere, global, que relativiza no sólo la significación conductual de las magnitudes espacio-tiempo, sino también el valor de las fronteras estatales, jurídicas e incluso culturales. Más aún, como dice Rodotà, la globalidad de la red no se refiere solamente al hecho de que se extiende por el planeta entero, realmente hoy es la forma extrema de globalización[16].

(g) Se comprende por todo ello que se destaque la fascinación que rodea a las transformaciones indicadas[17], que se han convertido en objetivo prioritario del interés socio-económico[18], político, científico o mediático, etcétera. En ello se realiza la Sociedad de la Información como Sociedad del espectáculo, donde éste también es un producto de consumo. Probablemente, la fascinación[19] se extiende también a la percepción macrocriminológica respecto de la delincuencia informática, que si no se presenta todavía como demoniaca, como en el caso de la organizada, sí se la tiñe de rasgos hasta cierto punto

[10] Hilgendorf, "Neuen Medien und das Strafrecht", *ZStW*, 113 (2001), p. 650; al respecto, asimismo, Morón, como en la nota 6, destacando el consiguiente fortalecimiento de las libertades garantizadas constitucionalmente que ello comporta. Con todo, como advierte S. Rodotà ("Libertà, opportunità, democrazia informazione", *Congreso Internet e privacy. Quali reggole?*, Roma, mayo-1998, disponible en http://www.privacy.it/garanterelrod.html.), no se produce una ruptura con el sistema jerárquico previamente conocido pues «non tutti possono nello stesso tempo assumere il ruolo di produttori e consumatori delle informazioni».

[11] Cf. Morón, como en la nota 6, p. 27 y nota 11 al píe.

[12] Así, Jakobs, "La ciencia del Derecho penal ante las exigencias del presente", *EDJ*, 20 (2000), p. 123.

[13] Vid. Matza, *El proceso de desviación* (trad. Julio Carabaña), 1981, Madrid: Taurus, p. 123.

[14] Subraya que Internet facilita el anonimato y las dificultades de persecución que ello comporta, Marchena, "Algunos aspectos procesales de Internet", *CDJ*, 2000/IV (monográfico «Problemática jurídica en torno al fenómeno de Internet», Dir. J. M. Martín-Casallo López), p. 70. Parecido, Zöller, "Verdachtlose Recherchen und Ermittlungen im Internet", *GA*, 2000, p. 563 s.

[15] Lo subraya Hilgendorf, como en la nota 10, p. 650.

[16] Como en la nota 10.

[17] Lo menciona también Morón, como en la nota 6, indicando además que «las opciones ante el futuro propuesto por las nuevas tecnologías discurren entre la utopía y la paranoia».

[18] Así el *Informe Bangemann*, como en la nota 2.

[19] Sobre la fascinación que siempre han ejercido el delito y el delincuente cf., por todos, García-Pablos de Molina, *Manual de Criminología. Introducción y teorías de la criminalidad*, 1988, Madrid: Espasa-Calpe.

mágicos, una visión que, como diría Bonger, no deja de ser precriminológica[20]. A mi juicio, con esta consideración se viene a corresponder, de un lado, una no menos efectista y ciega confianza[21] en el sistema de control penal para abordar los retos planteados. Pero también, de otro, la pretensión, fruto de la "soberbia tecnológica" que -como expresión particular de la derrota definitiva de la Historia, de la Política y del Derecho- niega al sistema jurídico toda virtualidad[22], ignorando, como subraya Rodotá[23], los rendimientos alcanzados, por ejemplo, con las reglas jurídicas sobre la *privacy*. Para afrontar esta tentación, insiste este ilustre jurista, resulta preciso escapar, entre otras cosas, de la retórica y del reduccionismo, así como del vértigo del jurista ante la complejidad de estos contextos[24], invocando -cabe añadir por nuestra parte-, en lo que sea razonable, lo que Hilgendorf[25] ha denominado el principio de la "Technikdistanz", esto es, que al fin y al cabo no pasará mucho tiempo para que adoptemos la misma aptitud ante estos avances tecnológicos que la que tenemos hoy respecto del teléfono.

(h) Por lo demás, esta fascinación se corresponde con el reconocimiento de la extraordinaria capacidad lesiva de la tecnología informática[26], que puesta al servicio del crimen entrañaría un potencial agresivo notablemente mayor que el de formas delictivas previas y que crece en tanto, para su funcionamiento, cada vez más sectores sociales dependen -y de forma más intensa- de las tecnologías de la información y del conocimiento y de las conexiones en red[27], por lo que se puede imaginar que cualquier bien jurídico puede verse afectado por esas vías[28]. Inicialmente, la preocupación se centró en los peligros que el uso de los sistemas tecnológicos avanzados conllevaba para la intimidad. Hoy, aparte de que ésta preocupa menos en su acepción epistolar y domiciliaria, que como "privacidad" -es decir, en razón de lo que ésta comporta de reconocimiento de una dimensión positiva que permite desplegar hacia fuera un significativo poder de control respecto de los datos a disposición de terceros-, se presta especial atención a otros daños y peligros, especialmente de carácter económico -individuales o colectivos-, social o político.

(i) Aunque, en palabras de Morón Lerma, «el ingreso en la era digital es ya un hecho», no se trata de un modelo social cerrado, sino completamente abierto y además regido por una alta aceleración de las condiciones de vida[29], que viene a suge-

[20] *Introducción a la Criminología* (trad. Antonio Peña, pról. y notas L. Garrido), 1943, México: Fondo de Cultura Económica, p. 72 s.

[21] O, si se prefiere, la fascinación hacia el Derecho penal. Cf. García-Pablos, *Derecho penal. Introducción*, ²2000, Madrid: Servicio de Publicaciones de la Facultad de Derecho, Universidad Complutense de Madrid, p. 49.

[22] Esta orientación se aproxima a la que por otras razones pretende la autoregulación. Sobre ella, véase *infra* nota 43 y texto.

[23] Como en la nota 10.

[24] Sobre esto también Marchena, como en la nota 14, p. 48.

[25] Como en la nota 10, p. 653.

[26] Jareño/Doval, "Revelación de daños personales, intimidad e informática (Comentario a la STS 234/1999, de 18 de febrero, sobre el artículo 197.2)", *La Ley*, 1999, p. 1.672, resaltando especialmente los peligros para la intimidad; Orts Berenguer/Roig Torres, *Delitos informáticos y delitos comunes cometidos a través de la informática*, 2001, Valencia; Tirant lo Blanch, p. 13 y 17, atribuyendo al Tribunal Constitucional la misma percepción. De la misma forma, la consideración 38 de la Directiva 2001/29/CE antes citada [nota 1] señala que la copia privada digital puede propagarse mucho más y tener un mayor impacto económico que la analógica.

[27] Falleti/Debove, *Planète criminelle. Le crime, phénomène social du siecle?*, 1998, Paris: Presses Universitaires de France, p. 22: el 40 % de las empresas no pueden funcionar sin ordenador más de cuatro horas; el 10 % más de un día; el 20 % más de tres días y el 30% más de una semana.

[28] Y que, salvo excepciones muy contadas, es imaginable que en la comisión de cualquier figura delictiva puedan desempeñar un papel significativo el empleo de medios informáticos, el uso de tecnologías y redes de comunicación (en este sentido, cf. Hilgendorf, como en la nota 10, p. 653; Jofer, *Strafverfolgung im Internet. Phänomenologie und Bekämpfung kriminellen Verhaltens in internationalen Computernetzen*, 1999, Francfort del Meno: Peter Lang, p. 97 s. Respecto de la informática, Orts/Roig, como en la nota 26, p. 158). Véase, asimismo, *supra* nota 8 e *infra* nota 63.

[29] Parecido Marchena, como en la nota 14.

rir la caracterización de la Sociedad de la Información como un sistema social efímero. En términos de política jurídica esto plantea en especial el dilema legislativo de optar por normas jurídicas de carácter *stringente* o elásticas[30].

III). Todavía podría seguirse una consideración más amplia de la Sociedad de la Información, subrayando no tanto su dimensión comunicativa, sino, a partir del recurso a *altas tecnologías*, extender su alcance a otros fenómenos que aún no siendo dependientes directamente de tecnologías informáticas o de la comunicación (TIC) se insertan en un sistema social paralelo. Se trata sobre todo de las tecnológicas genéticas[31] y de la nanotecnología, la robotización de la asistencia sanitaria o la expansión de los alimentos transgénicos. Pero estos aspectos no serán aquí objeto de consideración.

IV). Parece claro que algunas de las características indicadas se asemejan a ciertos aspectos de la llamada Sociedad del Riesgo. Este vínculo no ha pasado desapercibido a la doctrina penal y en este sentido Silva Sánchez[32] señala que «la criminalidad asociada a los medios informáticos y a Internet (la llamada "ciberdelincuencia") es, seguramente, el mejor ejemplo» de la evolución de la criminalidad en la Sociedad del riesgo, lo que probablemente lleve a calificar el contexto sociológico de los delitos cibernéticos como "Sociedad global del riesgo"[33] o "Sociedad del riesgo informatizada"[34]. Partiendo, pues de esta percepción, en principio, se advierte una fuerte demanda de seguridad que haga frente a estos riesgos -que hasta cierto punto no dejan de ser, como los propios de la Sociedad del riesgo, reflexivos, universales y difícilmente imputables-.

Por otra parte, en los párrafos precedentes se han puesto de manifiesto algunas ideas que evidencian la validez del intento de aplicar las claves epistemológicas -no exentas de contradicciones y todavía insatisfactorias- del llamado Derecho penal del riesgo[35], para analizar la respuesta jurídico-penal a la delincuencia propia de la Sociedad de la Información y, en particular, que los postulados metodológicos, político-criminales, y dogmáticos invocados por los críticos del Derecho penal del riesgo pueden ser de algún interés para evaluar lo que podríamos denominar el Derecho penal de la Sociedad de la Información.

Por lo demás, a la demanda general de seguridad referida acompaña, aunque no de modo tan visible y con un significado diverso, una creciente preocupación por la seguridad jurídica[36], tanto en lo que concierne a la pretensión de reducir la incertidumbre en los intercambios referidos, como en lo que respecta a controlar y minimizar los riesgos de que las intervenciones, preventivas o reactivas, fundamentadas en la demanda de general seguridad resulten arbitrarias. Pero, aún con esta

[30] Llama la atención sobre este dilema Rodotà, como en la nota 10.

[31] Donde por cierto también se dan algunos aspectos típicos de la respuesta penal a los dilemas de la Sociedad del Riesgo, como el simbolismo. A este respecto, cf. Higuera Guimerá, *El Derecho penal y la genética*, 1995, Madrid: Trivium, p. 58 ss. Recientemente también Luzón Peña, "Función simbólica del Derecho Penal y delitos relativos a la manipulación genética", Cerezo Mir (ed.), *Modernas tendencias en las Ciencias del Derecho Penal y en la Criminología*, 2001, Madrid: UNED, p. 131-138.

[32] *La expansión del Derecho penal*, ²2001, Madrid, Civitas, p. 28.

[33] Hilgendorf, como en la nota 10, p. 651, nota 7, refiriéndose a casos de ataques informáticos como los llevados a cabo con el virus "I love you", que afectó a tres millones de ordenadores, o los que también en 2001 bloquearon grandes servidores como "Amazon.com".

[34] Así Sieber en su intervención en el encuentro celebrado en la Universidad de Passau en mayo de 2001, según el informe de Jeßberger/Krauß, "Diskussionbeiträge der Strafrechtslehererertagung 2001 in Passau", *ZStW*, 113 (2001), p. 828.

[35] Al respecto, cf. recientemente Blanca Mendoza, *El Derecho Penal en la Sociedad del Riesgo*, 2001, Madrid, Civitas. Asimismo, el trabajo antes citado (nota 32) de Silva Sánchez.

[36] Morón, como en la nota 6, p. 20.

salvedad, lo cierto es que, en especial, predomina un discurso político-criminal que propugna el establecimiento de un sistema de protección que responda los citados peligros y proporcione las condiciones de seguridad necesarias para que la Sociedad de la Información pueda desarrollarse. Se plantea con ello, en particular, la necesidad de crear nuevos tipos o subtipos penales (con una relación más o menos estrecha con otros ya existentes) que respondan a transformaciones en formas de criminalidad clásicas impulsadas en las nuevas tecnologías, o a necesidades de protección frente a nuevas modalidades de ataque o derivadas de la aparición, *ex novo* o por radical transformación, de bienes jurídicos relacionados con las nuevas tecnologías y el contexto sociológico vinculado con ellas, y que, en cualquier caso, obedezcan a las exigencias de un Derecho penal de la seguridad. De todos modos, de esta tendencia lo más cuestionable sería que se impusiera una opción jurídica y jurídico-política decantada en este ámbito por una especie de Justicia penal *Nasdaq* que, a la vista de las insuficiencias actuales y bajo la presión de la demanda de efectividad, renunciara, en favor de un sistema de imputación diferenciado, a las reglas, lenguaje y principios propios de un Estado de Derecho[37].

Conforme a ello, en su conjunto, el Derecho penal que se pretende para la Sociedad de la Información estaría regido por premisas similares a las que han inspirado el Derecho penal de la Sociedad del riesgo y en la misma medida supone un modelo de intervención punitivo que, como éste, se aleja de los principios y formas clásicas de imputación, en tanto responde también a la expansión y a la flexibilización, con los riesgos "colaterales" que a su vez ello comporta para los principios del Estado de Derecho. Estas orientaciones de Derecho sustantivo, valen también para otras esferas del sistema penal. Y, en efecto, se acompañan con un amplio catálogo de medidas procesales y de transformación de las instancias de control penal, que al mismo tiempo se invocan para realizar aquellos objetivos, y en particular para neutralizar las dificultades de persecución. En especial, se plantea la necesidad de aprovechar en la lucha contra el crimen, y sobre todo sus formas más gravosas -entre ellas la delincuencia informática y la cibercriminalidad- esas tecnologías, de manera que éstas proporcionarían al sistema penal nuevos mecanismos de control. En este sentido, las tecnologías de la Sociedad de la Información proporcionan instrumentos de control especialmente incisivos, que acentúan esos efectos "colaterales" respecto de bienes jurídicos como la libertad o la intimidad. A este respecto, la fragilidad de estos frente a las nuevas tecnologías ha dado lugar a que se hable, por un lado, del fin de Internet como espacio de libertad y de la reinstauración de la censura[38] y, de otro, de la segunda muerte de la *privacy*, en la medida en que se acentúan y extienden los rasgos de estas formas de control que apuntan hacia un "totalitarismo virtual": su carácter permanente, certero e invisible[39], que aunque se ponga el acento en su origen institucional público, debe referirse también a los que provienen de intervenciones de personas o entidades privadas.

[37] Parecido a lo que aquí se plantea, Hilgendorf, como en la nota 10, p. 653.

[38] Cf. solamente, Bremer, *Strafbare Internet-Inhalte in internationales Hinsicht. Ist der Nationalstaat wirklicht überholt?*, 2001, Francfort del Meno: Peter Lang, p. 19 (accesible en http://ub-dok.uni-trier.de/diss/diss60/20000927/200009 27.pdf).

[39] Por todos, Morales Prats, "Privacy y reforma penal: la propuesta de anteproyecto de nuevo Código penal", *Documentación jurídica*, Volumen I, 1983, Madrid, p. 577 s.

En todo caso, las transformaciones antes sintetizadas suponen un reto no sólo para el Derecho penal, y en este sentido se señala que la gestación del nuevo sistema social conlleva notables incertidumbres para el sistema jurídico en general[40] o incluso se indica que habría supuesto para el mismo una auténtica conmoción[41]. Además, para el conjunto del ordenamiento jurídico, se puede decir, simplificando radicalmente, que la transformación gira también en torno a dos polos relacionados por una fuerte tensión que, como se ha visto, también está presente en el Derecho penal: las nuevas tecnologías abren la puerta a nuevos bienes jurídicos y amplían la virtualidad y significación de algunos de los clásicos; al mismo tiempo generan peligros evidentes para esos nuevos bienes jurídicos y para los clásicos.

En fin, resulta evidente que, consideradas en su conjunto, las indicaciones precedentes, por de pronto, muestran, para el ámbito referido, una tendencia inversa[42] a la que invoca un modelo autoregulativo, o, si se prefiere, la capacidad autoregulativa de las nuevas tecnologías[43]. Al contrario, asume una orientación expansiva y flexibilizadora que, por ello mismo, debe ser observada con cautela.

V) En algunos aspectos, las consideraciones precedentes son ya demostrativas de ciertas particularidades, pero hay que insistir en que, de todos modos, el análisis al que antes se hizo mención habría de tener en cuenta claves específicas como, por poner otro ejemplo[44], que en el ámbito propio de las nuevas tecnologías y su creciente círculo de influencia la imputación no depende, comparativamente, tanto del empleo de elementos normativos[45] muy porosos y, por lo mismo, poco seguros[46] -característicos de las intervenciones jurídicas en el Derecho de la Sociedad del Riesgo-, como del uso de criterios directamente dependientes de posibilidades e instrumentales tecnológicos muy avanzados, bastante complejos y no menos volátiles respecto nuevos hallazgos[47]. Como más adelante se verá, esto se advierte en el empleo de cláusulas o coletillas del tenor "u otro artificio semejante" o las que se emplean en la estafa informática. De todos modos, quizás esto no sea sino una evolución por hipertrofia de dos de los elementos característicos de la Sociedad del Riesgo, la dependencia tecnológica y la aceleración de las condiciones de vida.

[40] Sin duda, al respecto, los trabajos de Pérez Luño constituyen un punto de referencia imprescindible. Entre otros: *Nuevas tecnologías, sociedad y derecho*, 1987, Madrid: Fundesco; *Manual de informática y derecho*, 1996, Barcelona: Ariel.

[41] En la doctrina penal, en este sentido, por todos, Gutiérrez Francés, *Fraude informático y estafa*, 1991, Madrid: Ministerio de Justicia, p. 42.

[42] Esto no tiene necesariamente que suponer una derrota definitiva o "efectiva" de tal propuesta. En cuanto a lo segundo, ciertamente, la cifra negra (sobre esto, véase *infra*, apartado III del epígrafe 2) sería bastante ilustrativa.

[43] Contra esta orientación, Pérez Luño, "Internet: atentados criminales y respuestas jurídicas", *EJMF*, 1997/III, p. 342. Similar, Marchena, como en la nota 14, p. 53-56 (no obstante, cf. p. 64).

[44] También cabría mencionar el papel de la jurisprudencia (sobre esto véase *infra* notas 163 s y texto) o la base social que apoya el Derecho penal del riesgo y la que demanda el de la Sociedad de la Información (vease también *infra* nota 109 y texto).

[45] Que, en cualquier caso, no dejan de usarse. Basta con mencionar el Convenio sobre ciberdelincuencia (véase *supra*, como en la nota 5), que para todas las conductas punibles que contempla requiere que se realicen «without right» (arts. 2 a 10).

[46] Sobre la problemática en cuestión cf., por todos, Doval, *Posibilidades y límites para la formulación de las normas penales. El caso de las leyes en blanco*, 1999, Valencia: Tirant lo Blanch, *passim*.

[47] Si no me equivoco, vinculada con esta cuestión estaría la observación de Orts/Roig, como en la nota 26, p. 162, demandando una visión interdisciplinar (y además global), al menos en algunos de los aspectos planteados por la utilización fraudulenta de la tecnología informática y el análisis de los tipos penales concernidos (lo que a su juicio sólo entraña una visión sesgada de la amplia problemática), y en tanto ello sea compatible con las funciones del Derecho penal. Cf., asimismo, Morales Prats, "La intervención penal en la red. La represión penal del tráfico de pornografía infantil: estudio particular", en Zúñiga/Mendez/Diego (coords.), *Derecho penal, sociedad y nuevas tecnologías*, 2001, Madrid: Colex, p. 115.

VI). En las páginas que siguen se trata de ver con más detalle hasta qué punto se han realizado esos rasgos flexibilizadores y ampliatorios con relación al Derecho penal español. El análisis se lleva a cabo primordialmente en la esfera del Derecho penal sustantivo -con un alcance siempre sintético y selectivo, prestando atención sólo algunas de las instituciones y tipologías penales que se habrían visto más directamente afectadas por la implementación y expansión de las aquéllas-, aunque se hacen breves referencias a otros subsistemas penales. En todo caso, antes, se aborda la delimitación conceptual del objeto y las características básicas de la criminalidad de la Sociedad de la Información, apuntando que el proceso de evolución tanto de tal delincuencia como de su control es en parte interactivo.

2. CUESTIONES CONCEPTUALES Y SUSTRATO CRIMINOLÓGICO

I). Desde el punto de vista terminológico se plantean dudas, sobre todo, en torno a dos cuestiones. Por una parte que, a la vista de la imposibilidad de alcanzar un concepto jurídico-penal suficientemente preciso, en vez de hablar de delito informático (o incluso de delitos informáticos)[48] se prefiere usar la denominación "delincuencia informática", expresión considerada más adecuada para identificar un objeto relativamente impreciso[49].

La segunda cuestión se refiere a que no ha pasado mucho tiempo desde que dicha expresión alcanzara cierto arraigo, cuando ya se va imponiendo el término ciberdelincuencia (*cybercrime* o *cybercriminality* en la versión inglesa, o en Alemania *Internetkriminalität*, *Datennetzkriminalität*[50] o [Multi]*Mediendelinquez*), para hacer referencia más específica a los delitos cometidos en o a través de las redes informáticas. No obstante, es habitual hacer uso del término "delincuencia informática" para abarcar también estos supuestos, del mismo modo que son frecuentes usos de la expresión "ciberdelincuencia" (como se puede advertir en algunas de las previsiones del reciente Convenio sobre Ciberdelincuencia) de carácter generalizador y, por lo tanto, sustitutivos del anterior, una opción que se ve favorecida por la hipótesis de que a medida que el fenómeno de la conexión en redes se extienda se irá oscureciendo la identidad informática propiamente dicha.

II). Más problemático resulta delimitar el alcance que se deba atribuir a dichas expresiones. Sin entrar en el núcleo de la discusión[51], cabe destacar, ante todo, que ni existe una figura delictiva única específica de delito informático[52] o cibernético, ni hay un único concepto ni de delincuencia

[48] Opción muy en voga en España en los años ochenta.

[49] Cf., al respecto, Gutiérrez Francés, como en la nota 41; Romeo Casabona, *Poder informático y seguridad jurídica*, 1987, Madrid: Fundesco, p. 23 y 41.

[50] Cf. Hilgendorf, "Grundfälle zum Computerstrafrecht", *JuS*, 1997, p. 323 ss; el mismo, como en la nota 10, p. 650, 653 s, que quiere reservar la denominación a hechos que sólo son posibles a través de Internet o que por lo menos ésta facilita de forma considerable (precisando, p. 650, nota 3, que, no obstante, comprende no sólo Internet, sino también redes de datos internas: Intranets): espionaje o robo de datos, interceptación del tráfico de datos; hacking; sabotaje de software (p. ej. mediante virus) o de direcciones (incluido su bloqueo); distribución de materiales pornográficos; alteraciones o borrado de datos; simulación de identidad informática; uso de informaciones falsas.

[51] Al respecto, García-Pablos de Molina, "El impacto de las tecnologías y medios de información en el Derecho penal", *Boletín Citema*, 118 (1985), p. 13 ss; Gutiérrez Francés, como en la nota 41; Donn B. Parker; *Fightin Computer Crime*, 1983, Nueva York: Charles Schbner's Sons, p. 23; Romeo Casabona, como en la nota 49, p. 22 s y 40-43;

[52] Gutiérrez Francés, como en la nota 41, p. 8, 250 s.

informática (o de cibercriminalidad), de modo que en cada esfera se emplean con diversos sentidos. Por citar sólo un ejemplo, mientras a efectos jurídico-penales sustantivos el Convenio sobre ciberdelincuencia maneja un concepto centrado en determinadas tipologías delictivas, para ciertos efectos procesales amplía su ámbito comprendiendo, además de aquéllas, cualesquiera otras en que el instrumento o el objeto hayan sido sistemas informáticos[53], lo que ante el previsible incremento de la penetración de los mismos supondrá que cada vez más delitos, prácticamente sin limitación en cuanto a su tipología, queden sometidos a este particular del citado Convenio.

Los inconvenientes de semejantes conceptos, que en definitiva no ofrecen ninguna especificidad, habían sido ya advertidos por la doctrina, que se esforzó en proporcionar, respecto del de delincuencia informática, algún criterio restrictivo, como el hecho de que la conducta se llevara a cabo operando sobre la base de las funciones propias de los ordenadores, a saber, el procesamiento y transmisión automatizados de datos y la confección y/o utilización de programas para tales fines[54]. Por lo demás, parece claro que aquellas opciones conceptuales homogeneizadoras son igualmente disfuncionales desde una perspectiva político-criminal regida por el principio de proporcionalidad. En efecto, si, por una parte, la respuesta penal debe acomodarse a la gravedad de los hechos y si, por otra, aunque haya casos de delincuencia informática (o más específicamente la cibernética) que comparados con otros hechos delictivos similares comportan una lesividad mayor y es más difícil combatirlos, resulta igualmente evidente que esto no se puede predicar de toda la delincuencia informática, entonces, es erróneo destinar indiscriminadamente en el ámbito de la delincuencia informática recursos político-criminales cualificados con fundamento y finalidades específicos.

> En última instancia, da la impresión de que ni siquiera desde el punto de vista criminológico resulta significativo un concepto tan amplio, pese a que la Criminología, en tanto que, por su propósito globalizador no podría quedar prisionera de ningún Derecho positivo concreto[55], llega a considerar como objeto de interés *"círculos sociales" próximos al crimen*[56] o fenómenos concomitantes que, aunque no aparezcan abarcados por la prohibición jurídico-penal, se les atribuye cierta virtualidad criminógena o neutralizadora de la que puedan tener otros factores[57]. Esta perspectiva se puede advertir en el interés mostrado por ciertas conductas que no están criminalizadas, como sería el caso del *spamming*, esto es, del envío inconsentido de mensajes publicitarios por correo electrónico a una multitud de desconocidos, que incluso podría no ser ni siquiera ilícito. Aunque el caso más destacado, pero al mismo tiempo el más problemático para ilustrar la inclinación observada, es probablemente el del llamado *hacking*. De estos comportamientos, aunque, en principio, se indica que quien los practica se entromete en el sistema informático sin autorización y se impulsa no en las intenciones criminales o vandálicas que conlleva el *craking*, sino en razones educativas o de diversión (eso es, sin ánimos delictivos adicionales a la infiltración, como da-

[53] Para más detalles véase *infra* epígrafe 4. Se trata de una definición muy habitual en la literatura alemana (cf., por ejemplo, Eisenberg, *Kriminologie*, [4]1995, Colonia y otras: Carl Heymanns, § 47, marg. 65, p. 930), pero también, aunque con un alcance todavía más amplio, en la norteamericana: así, se incluye entre los delitos informáticos y los ciberdelitos, no sólo aquellos en que el ordenador es el instrumento o el blanco, sino también aquellos en que constituye un aspecto incidental (no es necesario, pero lo facilita) de otro delito, y los "crimes associated with the prevalence of computers", que están relacionados con el ordenador y sus elementos periféricos: piratería de software, violaciones del copyright y falsificación de software y hardware (David L. Carter, *Computer crime categories: How Techno-criminals Operate*, http://nsi.org/Library/Compsec/crimecom.html).

[54] En este sentido, cf. Romeo Casabona, como en la nota 49, p. 42 s.

[55] Así, por todos, Göppinger, *Criminología*, 1975, Madrid: Reus, p. 6.

[56] García-Pablos, como en la nota 19, p. 75.

[57] Cf., por todos, Garrido/Stangeland/Redondo, *Principios de Criminología*, [2]2001, Valencia: Tirant lo Blanch, p. 48-50.

ñar, espiar, defraudar o manipular)[58], se llega a afirmar que son la antesala de infracciones informáticas mucho más graves. Y, así, se aventura que quien empieza siendo un *hacker* acaba convirtiéndose en un *cracker*, o se señala que éste no es un sino «*dark side hacker*»[59], lo que quizás explique que a veces se le califique como de "vándalo informático" o incluso que se le llegue a identificar con el delincuente informático en general. En todo caso, aparte de estas discrepancias conceptuales se advierten diferencias de tratamiento punitivo: hay países donde la conducta de "hacking" en su sentido más estricto (y menos específicamente delictivo) resulta impune; otras legislaciones que siguen vías intermedias requieren, al menos, la violación de medidas de seguridad o propósitos delictivos o ilícitos; pero, en fin, no faltan países en los que, partiendo de las premisas antes indicadas, se identifica la conducta punible con la de cualquier intruso informático[60], es decir, cualquiera que accede de forma subrepticia, sin autorización o más allá de lo autorizado, a un sistema informático o red de comunicación electrónica de datos[61]. En mi opinión, este último proceder, que puede tener una justificación criminológica, no resulta adecuado ni desde el punto de vista político-criminal ni atendiendo a consideraciones jurídico-penales, en particular porque abarca conductas cuyo contenido criminal material es demasiado tenue y lejano, reafirmando de nuevo una orientación presente en el Derecho penal del riesgo[62].

Por otra parte, ante estos inconvenientes conceptuales, han acabado imponiéndose -sobre todo en el ámbito jurídico-penal-, en lugar de definiciones o descripciones de la delincuencia informática, listados más o menos completos y sistematizados (por ejemplo, según el bien jurídico protegido[63], el medio de ataque o combinando ambos aspectos) de delitos informáticos o cibernéticos[64]. Esta

[58] Morón, como en la nota 6, p. 43; Sieber, "Documentación para una aproximación al delito informático", en Mir Puig (comp.) como en la nota 9, p. 77; Gutiérrez Francés, como en la nota 41, p. 300.

[59] Cf. el Glosario de Daniel Ferrandis Ciprián, en Orts/Roig, como en la nota 26, p. 173-183 (en especial, 175, 177s), remitiéndose a http://watson-net.com/jargon.

[60] El Convenio sobre ciberdelincuencia contempla entre las infracciones contra la confidencialidad el *acceso ilegal*, que describe como el acceso intencional no autorizado a un sistema inforático o a cualquiera de sus partes, dejando en manos de los firmantes del Convenio el establecimiento de exigencias adicionales, como que se cometa violando medidas de seguridad, con la intención de obtener datos del ordenador u otra intención deshonesta, o respecto de un sistema informático que esté conectado a otro (art. 2).

[61] Cf., al respecto, aparte de la nota precedente, Morón, como en la nota 6, p. 42; Gutiérrez Francés, "Delincuencia económica e informática en el nuevo Código penal", en *Cuadernos de Derecho Judicial* (CDJ), 1996/XI (monográfico "Ámbito jurídico de las tecnologías de la información". Dir. M. A. Gallardo Ortiz), p. 299 s.

[62] Sobre el perfil de la criminalidad de la Sociedad del Riesgo, cf., por todos, Prittwitz, *Strafrecht und Risiko. Untersuchung zur Krise von Strafrecht und Kriminalpolitik in der Risikogesellschaft*, 1993, Francfort del Meno: Vittorio Klostermann, p. 172-198.

[63] Por ejemplo, Sieber, "Computerkriminalität uns Informationsstrafrecht in der internationalen Informations- und Risikogesellschaft", Kühne/Miyazawa (ed.), *Neue Strafrechtsentwicklungen im deutsch-japanischen Vergeich*, 1995, Colonia: Heymann, p. 34-47, agrupa las infracciones según que afecten prioritariamente a derechos relativos a la personalidad o a intereses patrimoniales o económicos -como las manipulaciones informáticas (de cuentas y balances, de tarjetas bancarias, abusos telefónicos), el sabotaje informático y el chantaje informático, el hacking, que a veces comporta daños de ese tipo, el espionaje informático y el robo de software y otras formas de piratería-, contemplando, no obstante, un grupo de "otros delitos" que afectan a otros bienes jurídicos, en el que incluye ataques de diverso tipo: con propósitos de tipo político o similares, de carácter pornográfico y ataques a bienes jurídicos tradicionales como la vida o la integridad física, por ejemplo, por manipulación de equipos informáticos usados en hospitales, en centrales nucleares, etcétera. Sieber resalta que la variedad de los ataques se irá ampliando conforme más parcelas de la vida incrementen su dependencia de la informática y de las telecomunicaciones, subrayando asimismo la cada vez más estrecha relación entre éstas y aquélla, lo que no deja de ser una manifestación más de que las nuevas tecnologías no sólo se caracterizan por la digitalización, la conexión en redes, sino también por lo podría denominarse su carácter híbrido, aquí en el sentido de que se aparecen combinadas técnicas, espacios, lenguajes, culturas, etcétera (cf. Hilgendorf, como en la nota 10, p. 650).

[64] Respecto de la cibercriminalidad se dice que «son aquellas actividades en las que se emplean ordenadores, teléfonos, equipos celulares y otros dispositivos tecnológicos con propósitos ilícitos como fraudes, robos, vandalismo electrónico,

opción no obstante no deja de ser insatisfactoria porque, en especial desde el punto de vista del principio de proporcionalidad, no permite identificar las razones que fundamentan una ampliación del ámbito de lo punible o de la agravación punitiva o simplemente de la especificidad punitiva o procesal. En general, como ocurre también en el caso de la criminalidad organizada, estos inconvenientes conceptuales no hacen más que subrayar la dificultad de acotar estos fenómenos delictivos, así como la respuesta a los mismos, facilitando por lo tanto que bajo dicha respuesta queden abarcados hechos que -aun guardando cierta conexión criminológica, en tanto que "fenómenos concomitantes"- no reúnen los rasgos y la lesividad que antes se indicaron, o que la "selección" acabe limitándose o concentrándose en los supuestos de menor entidad, y, en definitiva, acentuando el carácter asmático de la respuesta penal.

Las definiciones son, pues, numerosas y dispares, lo que requeriría una atención que aquí no se puede prestar. No obstante, sólo a título orientativo, conviene mencionar el catálogo de infracciones punibles del Convenio sobre ciberdelincuencia. En primer término, refiere *las infracciones contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos*, incluyendo en este grupo el acceso ilegal, la interceptación ilegal, los atentados a la integridad de los datos y de los sistemas y el abuso de dispositivos (art. 2 al 6). En segundo término, las *infracciones informáticas*, que abarcan la falsificación y el fraude informáticos (arts. 7 y 8). En tercer término, las *infracciones relativas a los contenidos*, que abarcan exclusivamente las relacionadas con la pornografía infantil (art. 9). Y, por último, las *infracciones relativas a los atentados a la propiedad intelectual* y a los derechos anexos (art. 10). No obstante, como se ha anunciado, para algunas particularidades procesales, el Convenio amplia su alcance a otras infracciones penales cometidas por medio de un sistema informático, e incluso con relación a la recogida de pruebas electrónicas su alcance se extiende a cualquier infracción penal.

III). Una aproximación criminológica debe partir de un lugar común de la literatura especializada: la altísima cifra negra que se daría tanto en la delincuencia informática propiamente dicha, como -quizás incluso en mayor medida- en la cibercriminalidad, y que no es propiamente un fenómeno de los llamados "paraísos informáticos", esto es "ayunos de regulación en la materia"[65], sino que afecta también los países con legislaciones prohibicionistas. Incluso se afirma que tales manifestaciones delictivas constituirían precisamente un ejemplo paradigmático de escasa persecución penal, si bien en este caso ello tendría menos que ver con la praxis de la selección que con problemas específicos de descubrimiento de tales delitos[66].

De todos modos, por lo que se refiere a España, esta peculiaridad no se apoya en una validación sistemática, sino que fundamentalmente es el resultado de traspolar las conclusiones obtenidas en Estados Unidos en base a las cifras oficiales y, en menor medida, de encuestas de victimación y autodenuncia.

A partir de los datos disponibles, que no es seguro que reúnan los estándar de fiabilidad exigibles, se hacen estimaciones que en lo que respecta a la cifra negra están relativamente estabilizadas: de los ilícitos informáticos cometidos, sólo se descubre el uno por ciento[67]. Asimismo, que de este porcentaje sólo el catorce por ciento llega a los tribunales y sólo el tres por ciento de los ilícitos juzgados da lugar a sentencias condenatorias con privación de libertad. Obviamente, estos desequilibrios contables refuerzan la hipótesis de partida, pero también advierten acerca de elementales cautelas metodológicas,

infracciones de la propiedad intelectual y daños y acceso en sistemas y redes informáticas»: David L. Speer, "Redefining borders: The challenges of cybercrime", *Crime, Law & Social Change*, 34 (2000), p. 259-273 (260). Por su parte, Jofer, como en la nota 28, p. 34 ss, menciona los delitos de difusión específicos de la red, el uso abusivo de Internet como medio de comunicación del hecho y aquellos en que Internet constituye el instrumento virtual del hecho. Véase también *supra*, nota 50.

[65] Así Orts/Roig, como en la nota 26, p. 163.

[66] Así, Schwind, *Kriminologie. Eine praxisorientierte Einführung mit Beispielen*, [8]1997, Heidelberg: Kriminalistik, § 8, marg. 11, p. 137.

[67] I. Peterson, "Computer crime: Insecurity in numbers", en *Science News*, 125 (1984), p. 12 (referido por Gutiérrez Francés, como en la nota 41, p. 72).

entre las que cabe citar ciertas peculiaridades de la Justicia penal norteamericana muy propicia a soluciones procesales que acaban con la contienda penal en un momento previo a la sentencia condenatoria o con sentencias absolutorias pactadas.

No obstante, el déficit del control es compartido prácticamente por toda la doctrina[68], incidiendo en que se trata de un tipo de criminalidad que, por su propia configuración, por ejemplo[69] su itinerancia y nomadismo virtual[70] o la escasez de rastros que deja[71], resulta difícil de descubrir e investigar[72], de manera que aunque se perfeccionaran los mecanismos e instrumentos de control (reduciendo tanto los defectos en su configuración como las anomalías), siempre se presentaría una cifra negra inusual[73]. Aún así, no faltan discrepancias en torno a los costes y posibilidades reales de una política criminal que persiguiera, con más dedicación y medios (entre ellos los jurídicos), franquear la porción *estructural* de esa dificultad.

Esta alta cifra negra tiene también una variante cualitativa, en el sentido de que se conoce poco y mal la criminalidad informática y la cibercriminalidad. De ello se impondría, por lo menos, una moderada prudencia con relación a la validez científica del expediente analítico, en la medida en que se estaría construyendo sobre porcentajes muy poco representativos del conjunto de la criminalidad informática y de la ciberdelincuencia. En tal sentido, en términos de verificabilidad o testabilidad[74], los esbozos descriptivos rozarían la conjetura y se moverían más bien en el terreno de la mera especulación, por muy razonables y ajustadas al sentido común que se nos presenten las conclusiones.

IV). Junto con este aspecto, la aproximación criminológica se ve dificultada por el hecho de que aún siendo una criminalidad que, según apuntan los datos disponibles, ha crecido incesantemente, tiene escaso arraigo[75] y parece que ha ido evolucionando a una velocidad desconocida en la Historia de la Criminalidad.

V). A estas advertencias que ponen en cuarentena cualquier esbozo fenomenológico sobre la criminalidad informática y en particular sobre la cibercriminalidad, hay que añadir su heterogeneidad, que hace ya prácticamente imposible una síntesis global. De todos modos, se mencionarán a continuación algunos rasgos sobre los que cada vez se insiste más y sobre los que se construye la propuesta político-criminal expansiva y agravatoria.

En principio, se trataría de una criminalidad transfronteriza[76] (que en ocasiones está implantada en los llamados "paraísos informáticos"[77]), aunque no es infrecuente que tenga un alcance local (o que los hechos se lleven a cabo en países que dis-

[68] Al respecto, entre otros, González Rus, "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", *Revista de la Facultad de Derecho de la Universidad Complutense de Madrid*, 12 (1986, Monográfico Derecho e Informática), p. 126 ss; Gutiérrez Francés, como en la nota 41, p. 72; Morales Prats, *Tutela penal de la intimidad: privacy e informática*, 1984, Barcelona, p. 325; Morón Lerma, como en la nota 6, p. 36; Romeo Casabona, como en la nota 49, p. 36, 72; Schwarzenegger, "Der raümliche Geltungsbereich des Strafrechts im Internet. Die Verfolgung von grenzüberschreintender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Österreich", *Schweizerisches Zeitschrift für Strafrecht*, 2000, p. 113; Sieber, "Criminalidad informática: peligro y prevención", en Mir Puig (comp.), como en la nota 9, p. 31 s; Tiedemann, *Poder económico y delito*, 1985, Barcelona: Ariel, p. 123.

[69] Para más detalles cf. Mata y Martín, *Delincuencia informática y Derecho Penal*, 2001, Madrid: Edisofer S.L., p. 153.

[70] Vid. Morón, como en la nota 6, p. 122. Mata y Martín, como en la nota 69, p. 154.

[71] Cf. Consentino y otros, "Tras los pasos de la seguridad perdida", en *Informática y Derecho*, 23-24 (1988), p. 1.198.

[72] Sieber, como en el nota 58, p. 94; Mata y Martín, como en la nota 69, p. 152-154.

[73] Quizás pueda aquí corroborarse la percepción interactiva referida, en virtud de la cual una mejora de los mecanismos de control, en alguna medida significativa, se compensa con una modernización de la criminalidad.

[74] Cf. al respecto Akers, *Criminological Theories. Introduction and Evaluation*, ²1999, Chicago-Londres: Fitzroy Dearborn Publishers, p. 7-10.

[75] Como punto de partida de esta criminalidad se menciona (Rosoff/Pontell/Tillmann, *Profit without honor: white-collar crime and the looting of America*, Nueva Yersey: Prentice-Hall, 1998, p. 366) el hecho ocurrido en la década de los sesenta en Estados Unidos, cuando jóvenes, motivados por una mezcla de picardía y codicia, accedieron ilegalmente a la red "Ma Bell", reproduciendo la multifrecuencia empleada por la compañía AT&T, lo que les permitió realizar llamadas telefónicas al extranjero sin cargo. Un dato significativo es que la compañía había descrito la nueva tecnología en sus publicaciones técnicas restringidas, confiando en que, fuera de ese entorno, nadie las leería o que, aunque lo hiciera, no las entendería.

[76] Orts/Roig, como en la nota 26, p. 162; Schwarzenegger, como en la nota 68, p. 109.

[77] Sobre esto, Mata y Martín, como en la nota 69, p. 151; Orts/Roig, como en la nota 26, p. 162

ponen de sistemas de control más perfeccionados). Con ello, se quiere destacar no sólo su carácter internacional, sino también su carácter de delitos "a distancia", en el sentido de que hay una clara separación, que precisamente en esos casos traspasa fronteras, entre la acción y el resultado, entre el autor y la víctima o, si se quiere, entre el autor y la escena del crimen. Esa separación precisamente es superada -prácticamente sin diferencia de tiempo- gracias a los sistemas y redes informáticas y digitales y se convierte en una ventaja para el autor y un inconveniente para su persecución.

Quizás sea algo más sesgada su caracterización como criminalidad organizada[78], aun en el caso de que se le dé al término una significación muy relajada, como se habría reflejado en casos relativamente conocidos en los que los implicados actuaron aislada e individualmente. Desde luego, no puede servir de base para argumentar en el sentido indicado el hecho de que entre algunos infractores informáticos, especialmente jóvenes, se haya detectado cierta intercomunicación plasmada en los llamados *electronic bulletin boards systems*. De todos modos, convendría separar lo que es la calificación de la delincuencia informática como organizada, de la consideración de que organizaciones criminales cometen también delitos informáticos y, sobre todo, que hacen uso con cada vez más frecuencia de medios informáticos y redes sofisticadas de telecomunicación, a lo que por lo demás sería preciso responder igualmente con medios tecnológicos avanzados[79].

También resultaría insuficiente la pretensión de establecer un estrecho vínculo de la criminalidad informática con la delincuencia económica. Aunque los perfiles de la delincuencia económica no están suficientemente definidos y desde luego no responden exclusivamente al concepto del *white collar crime*, útil más bien al objeto de identificar peculiaridades del autor, como por ejemplo su "carrera criminal"[80], da la impresión de que hoy esta vinculación es sólo parcialmente significativa, como lo demostraría, por ejemplo, la existencia de intromisiones que persiguen objetivos lúdicos o políticos[81].

En todo caso, se trata de una delincuencia compleja, lo que resulta del uso de alta tecnología[82]. Más aún, cada vez son más frecuentes hechos que muestran una clara tendencia a la sofisticación y profesionalización[83].

VI). En cuanto al *perfil del delincuente informático*, ha experimentado una significativa transformación[84], en la que se advierte un desplazamiento desde una silueta preferente[85], primero, de jóvenes obsesionados por el medio o, más tarde, de empleados resabiados que actúan con ánimo de venganza y sin fines lucrativos inmediatos –aunque se considerara que provocaban los daños más cuantiosos[86]-, a rasgos más interesados, ya sea con propósitos lucrativos -tanto de carácter económico empresarial, como simplemente patrimonialista-, ya sea con propósitos más agresivos indiscriminados o respecto de instituciones básicas para el funcionamiento del Estado, que no obstante no han eliminado los perfiles antes indicados. De todos modos estas indicaciones no pueden ocultar la heterogeneidad que presenta el perfil conjunto, y la necesidad de tomar en cuenta perfiles específicos como el del "pedófilo internauta".

VII). La consideración de los *efectos* se enfrenta a inconvenientes parecidos, a la vista, entre otras cosas, de la heterogeneidad de las modalidades delictivas. Ciertamente, no son equiparables los daños de los ataques a bienes jurídicos personales, como la privacidad o la libertad sexual o, si se prefiere, la indemnidad de los menores, en el caso de la ciberpornografía, con las variantes de los daños de carácter patrimonial o empresarial. De todos modos, suele convenirse que, generalmente, y en comparación con otras formas delictivas, los daños son mayores.

En todo caso, en cuanto a delitos informáticos patrimoniales y socioeconómicos, la cuantificación de los daños plantea dudas sobre su fiabilidad[87], entre otras cosas porque no aparecen con autonomía en las estadísticas o sencillamente porque

[78] Cf. Orts/Roig, como en la nota 26, p. 162.

[79] Al respecto, cf. Militelo, "Iniciativas supranacionales en la lucha contra la criminalidad organizada y el blanqueo en el ámbito de las nuevas tecnologías", en Zúñiga/Mendez/Diego (coords.), como en la nota 47, p. 183-185.

[80] A este respecto, Weisburg/Waring/Chayet, *White-Collar Crime and Criminal Careers*, Cambridge y otras: Cambridge University Press, *passim.*

[81] Orts/Roig, como en la nota 26, p. 13.

[82] Ibídem, p. 162.

[83] Ibídem, p. 13.

[84] En este sentido, Gutiérrez Francés, como en la nota 41, p. 75.

[85] Normalmente, caracterizables como delincuentes primarios u ocasionales (Romeo Casabona, como en la nota 49, p. 36), varones, que según los más recientes estudios rondan una edad promedio entre los treinta y los treinta y cinco años.

[86] Romeo Casabona, como en la nota 49, p. 36.

[87] Cf. Kaiser, *Kriminologie. Ein Lehrbuch*, [3]1997, Heidelberg: C.F. Müller, § 74, marg. 59 s.

son difíciles de calcular. Se podrían dar infinitas cifras, pero la mayoría constata dígitos espectaculares, que en su conjunto se consideran superiores a los que provoca la delincuencia patrimonial tradicional: los costes anuales se mueven entre los 550 millones (que plantea el *National Center for Computer Crime Data*) y los 15 billones de dólares (manejada por la *Inter-Pact computer security organization*), e incluso más. De todos modos, convendría precisar que junto con hechos que provocan daños incontables, también se producen supuestos, la mayoría, de escasa cuantía.

Al margen de estos daños más inmediatos y, aunque imprecisos, relativamente cuantificables, se le atribuyen[88] un haz de efectos dañinos parecidos a los imputables a la criminalidad económica[89]. Por ejemplo, en ese terreno habrían de situarse las indicaciones manejadas por la Asamblea plenaria de entidades aseguradoras sobre efectos derivados siniestros informáticos, incluidos los provenientes de ataques intencionales: el sesenta por ciento de las empresas pequeñas y medianas que los sufren terminan desapareciendo en el plazo de cinco años. Pero, además, cada vez se presta mayor atención a daños más difusos de carácter colectivo o institucional, cuya evaluación resulta más compleja o sencillamente es inviable en el marco de un proceso penal.

VIII). En rigor, las carencias analíticas cortarían en seco una argumentación plausible sobre la explicación de la delincuencia informática, más aún tratándose de un objeto tan heterogéneo y cambiante. Por lo tanto, sólo a título exclusivamente especulativo pueden hacerse algunas aproximaciones breves, selectivas y necesariamente simplificadoras, con las que sólo se pretende apuntar, a título ejemplificativo, algunas conexiones posiblemente fructíferas.

Desde luego, parece claro que si la Sociedad de la Información *padece* de una clara *anomia*, y en especial de una anomia "jurídica"[90], al tiempo que «nadie duda ya que la revolución informática está cambiando la estructura interna de la sociedad»[91], la teoría de la anomia, incluso en la versión de su más conocido promotor Emile Durkheim, podría ser útil e incluso permitir avanzar que, si el cambio y la aceleración de las condiciones constituyen un factor estructural de este modelo social, quizás haya que hablar, al menos conceptualmente, de una anomia y de una criminalidad estructurales.

A ello habría que añadir algo que destacaron las teorías de la desorganización social, que el anonimato -un aspecto igualmente característico de la red- incrementaría las posibilidades de actividades delictivas.

En todo caso, en este marco teórico, parece clara cierta coherencia respecto de esta forma de criminalidad no sólo de la tesis normalidad del crimen, sino de la de su *fuerza innovadora*, que ya había sido advertida por el propio Durkheim[92] y que fue desarrollada con posterioridad por Merton[93] y sus discípulos Cloward y Ohlin[94]. Algunos datos episódicos, como el hecho de que algunos autores de delitos informáticos hayan sido acogidos como técnicos por las empresas que sufrieron ataques informáticos, ilustrarían parcialmente sobre el particular.

Con relación a otro aspecto de la innovación, cabe acudir remontándose algo más atrás a las leyes de la "imitación" de Gabriel Tarde, consideraciones a las que los comportamientos criminales no serían ajenos, en particular, a la moda y a los procesos de innovación, de forma que podría establecerse cómo modas criminales nuevas se superponen a otras más viejas mediante el aprendizaje imitativo y la innovación tecnológica: del mismo modo que el bandolero europeo prepararía la aparición del salteador de diligencias americano del siglo diecinueve, el falsificador es reemplazado por la adulteración de

[88] Kaiser, como en la nota 87, § 74, marg. 60.

[89] Sobre tales efectos, cf., por todos, Bajo/Bacigalupo (Silvina), *Derecho penal económico*, 2001, Madrid: Ceura, p. 31-33.

[90] Morales Prats, como en la nota 47, p. 116.

[91] Y, como señala Morón, como en la nota 69, p. 25,

[92] *Las reglas del método sociológico* (trad. A. Ferrer y Robert), 1978, Madrid: Akal, p. 86-93, en especial p. 86.

[93] "Estructura social y anomia: revisión y ampliación", en Fromm y otros, *La familia*, 1972, Barcelona, p. 67-107; Merton, *Teoría y estructura sociales* (trad. F.M. Torner y R. Borques, de la tercera edición en inglés de 1968), México: FCE, *passim*, en especial, p. 142, 209-213, 249.

[94] Quienes prestaron especial atención a la virtualidad criminógena adicional de la existencia de "oportunidades ilícitas efectivas", también en el sentido de un aprendizaje diferencial de los medios ilícitos (cf. Cloward/Ohlin, *Delinquency and opportunity. A theory of delinquent gangs*, 1960, Nueva York-Free Press, p. 150 s).

programas de software, o el ladrón de bancos es reemplazado por aquellos que mediante manipulaciones informáticas sofisticadas consiguen transferencias de fondos bancarios[95].

Volviendo a las tesis mertonianas, conviene matizar que su propuesta sobre la anomia presta atención más bien al potencial explicativo del desequilibrio entre medios y fines y de la desigualdad de oportunidades, junto con el universalismo en la definición de aquéllos. Pues bien, a la vista de que podrían haberse acentuado tales desequilibrios en la Sociedad global de la Información, correspondería a ésta un potencial criminógeno adicional.

No menos interés puede tener la contemplación del fenómeno partiendo de los postulados actualizados de la Escuela clásica. Esto lleva a considerar el comportamiento delictivo como resultado de una decisión racional, aunque puedan existir singulares discrepancias en orden a identificar las bases y el proceso de esa decisión (ya sea de un hecho en particular, ya de una trayectoria criminal, y desde luego de su abandono), que, además de complejo, es variado (por ejemplo, según el tipo de delito). Parece claro que cuanto más se estrechen las conexiones entre la cibercriminalidad y la delincuencia económica o incluso la organizada, estas propuestas teóricas serían más apropiadas.

Más recientemente, se ha procedido a conectar[96] tales propuestas con consideraciones más específicas (acudiendo a la teoría de las actividades rutinarias, a la teoría de las oportunidades, o a la teoría de la prevención situacional[97]), tratando sobre todo de explicar el aumento de criminalidad en las sociedades desarrolladas, llegando a vincularse dicho incremento con la ampliación de los objetivos delictivos y la ausencia o disminución de la vigilancia (tanto en sentido formal como informal).

En términos político-criminales esto se ha traducido con frecuencia en una confianza manifiesta hacia modelos de prevención situacional, que, de alguna manera, pueden encontrar algún parentesco con el enorme interés mostrado en la lucha contra la delincuencia informática y la cibercriminalidad por el empleo de sistemas disuasorios de profilaxis técnica, esto es, por medidas de seguridad técnicas[98].

Incluso, no han faltado propuestas que inciden en la exclusividad de estas medidas y la inutilidad del control penal, ni otras más moderadas que se limitan a establecer su prioridad.

En cualquier caso, la implementación de tales medidas provoca riesgos, que no son desconocidos. Por poner algunos ejemplos: los que se derivan de la utilización de medidas de protección "contraofensivas"; o los relacionados con mecanismos de encriptación, que pueden dificultar a las instancias públicas la efectividad del ejercicio legítimo de sus funciones de control, que frente a ello pretenden disponer de instrumentos de desencriptación, que por su parte pueden dar pie a excesos en dichas funciones.

De las teorías del etiquetamiento interesa retener más que su reflexión sobre el proceso de desviación mismo, su interés por enfocar el estudio de la delincuencia atendiendo a la configuración y funcionamiento del sistema de control. A este respecto, hay que reiterar las dificultades de control[99], que, como se vio, presentan variadas manifestaciones, como diversas son sus razones (por ejemplo el vértigo y el desfase provocado por los avances tecnológicos), y que en gran parte explican que la respuesta a la criminalidad informática sea -aparte de poco efectiva- hasta cierto punto asustadiza, y se asiente en una significativa ampliación de la esfera de lo punible, de la que forma parte una no menos elocuente tendencia flexibilizadora de las reglas de imputación.

De esta orientación, también característica del modelo político-criminal de la Sociedad del Riesgo, son particulares muestras la especialización de la Justicia penal en sus diversas fases, la orientación de la persecución en especial respecto de las ganancias[100], la cooperación internacional[101] y una ampliación del papel de los aspectos procesales a costa de los específi-

[95] Refieren estos reemplazos Rosoff/Pontell/Tillmann, como en la nota 75, p. 366. Para otros relacionados con los fraudes informáticos, cf. Herrera Moreno, "El fraude informático en el Derecho penal español" *AP*, 2001 (consultada la versión electrónica, epígrafe VI, D).

[96] Cf., por ejemplo, aunque con relación a una problemática ajena al contexto considerado en este trabajo, Clarke/Felson, "Routine Activity and Rational Choice", *Advances in Criminological Theory*, 5 (1993), p. 9.

[97] Desde donde se postula como medio de prevención el uso de tecnologías avanzadas como la videovigilancia.

[98] Cf. Romeo Casabona, como en la nota 49, p. 40, refiriendo entre esas medidas de seguridad el aseguramiento de los daños y los códigos éticos y deontológicos.

[99] Vid. Mata y Martín, como en la nota 69, p. 155 ss.

[100] Sieber, como en la nota 58, p. 94 ss.

[101] Por todos, cf. Tiedemann, "Computerkriminalität und Strafrecht", *Kaiser-FS*, 1998, Berlín, p. 1.379 s.

camente sustantivos, que se ve facilitada por la introducción o reforzamiento de las posibilidades de intervención tecnológicas de las instancias investigadoras, que en algunos casos se plasma en la legitimación de sistemas de vigilancia permanente o de sistemas de control generalizados, que por lo tanto inciden en sujetos que ni siquiera son sospechosos[102].

Las teorías del etiquetamiento han proporcionado a este respecto un sólido arsenal crítico que, partiendo de la tendencia de las agencias de control penal a realizar su función de selección de forma sesgada, permite poner en guardia frente modelos de control penal que faciliten todavía más ese sesgo. Esto lleva a observar con cautela las tendencias político-criminales mencionadas y en especial a establecer reservas adecuadas que eviten, ante el proceso de globalización de la política criminal, que a través del sistema penal se facilite la colonización jurídica[103].

De nuevo, y desde la perspectiva auspiciada por esta corriente criminológica, pueden advertirse otras coincidencias específicas entre el control penal de la delincuencia de la Sociedad del Riesgo y el de la criminalidad de la Sociedad de la Información. El *caso Compu-Serve* sirve a tales efectos en la medida en que, por una parte, da la impresión de que la persecución penal se dirige más bien hacia un chivo expiatorio y, de otra parte, que la persecución penal no suele acabar con condenas, pero ya las actuaciones procesales comportan un alto gravamen para el imputado, que luego no se ve compensado con la absolución: en especial, mientras las actividades de cargo suscitaron un enorme y continuado interés en la opinión pública alemana, la sentencia absolutoria en segunda instancia sólo mereció una insignificante nota periodística en el *Frankfurter Allgemeiner Zeitung*[104].

IX). En cuanto a la perspectiva victimológica, hay que recordar que ya el interaccionismo, resaltó que la conducta de la víctima no es un elemento neutro si se busca una explicación al delito. A este respecto, suele señalarse que las víctimas de delitos informáticos o de cibercrímenes en muchos casos no habían adoptado precauciones técnicas mínimas para evitar tales agresiones. De otra parte, se aduce que la impunidad de estas manifestaciones delictivas, y por ello también la alta cifra negra que en ellas se da, se debe a que las víctimas no presentan denuncias, no continúan hasta el final sus pretensiones procesales[105] o ni siquiera reconocen su condición de víctimas[106], por temor a que con ello se amplifiquen los efectos negativos[107], y en particular, sobre todo en el caso de empresas o instituciones, se perjudique su imagen pública, en tanto la victimación ponga de manifiesto precisamente la fragilidad del sistema seguridad del afectado[108].

Al margen de esto, se debe destacar que aunque víctimas de estos delitos suelen ser empresas e instituciones, también pueden verse afectados sujetos individuales. Por otra parte, como se demostró con el virus "I love You" aparecido en 2000, el número de víctimas de delitos informáticos y cibercrímenes puede ser millonario. Se estima que en el caso citado resultaron afectados dos millones y medios de ordenadores en EE. UU., un cuarto de millón en Europa y cien mil en Asia. Esto pone de relieve algunos rasgos que también se dan en la delincuencia de la Sociedad del Riesgo, en particular, que los daños pueden ser globales, y que cualquiera al margen de su posición social puede verse afectado directa o indirectamente, con lo que para estos delitos, de alguna manera, potencialmente, víctimas somos todos. Esto explica que los demandantes

[102] Wolter en el Encuentro de Passau ya citado subrayó esto críticamente (cf. Jeßberger/Krauß, como en la nota 34).

[103] La necesidad de esta cautela ya la he apuntado en otras ocasiones: "Crónicas Iberoamericanas. Principales reformas penales. España", *RP*, 1 (1998), p. 100 s; "Crónicas Iberoamericanas. Criminalidad organizada. España", *RP*, 2 (1998), p. 103 y "Conjeturas sobre la criminalidad organizada", en Ferré/Anarte, *Delincuencia organizada. Aspectos penales, procesales y criminológicos*, 1999, Huelva: Universidad de Huelva, p. 56.

[104] Cf., por todos, Bremer, como en la nota, p. 19 s.

[105] Como se acaba de indicar, en algunos casos incluso la empresa afectada llega a acuerdos con el autor integrándolo en la misma.

[106] Cf. Tiedemann, como en la nota 101, p. 1.374; lo comparte, Mata y Martín, como en la nota 69, p. 154, subrayando la sensación de impunidad que con ello se proporciona a los autores de este tipo de delitos. De todos modos, en encuestas de victimación realizadas en Estados Unidos se advierte que el reconocimiento victimario ha aumentado: en 1986, sólo el 7% de empresas encuestadas lo admitió, en 1993, el 70% (el 24% incluso reconoció daños superiores a los 100.000 $), en 1995, de 150, 148 y, de éstas, el 43% reconoció haber sido victimizada 25 veces o más.

[107] Morales Prats (en Quintero [Dir.], *Comentarios al Nuevo Código penal*, ²2001, Pamplona: Aranzadi, p. 1.006), señala que una razón político-criminal de la privatización del *ius persequiendi* en los delitos contra la intimidad está en que, ante la amplificación de los daños que el proceso pudiera conllevar, el titular del bien jurídico en algunos casos preferirá no instarlo.

[108] Cf. Tiedemann, como en la nota 68, p. 126.

de un endurecimiento de la respuesta penal no sean sólo los habituales gestores morales, sino que a la lista se añadan las grandes corporaciones[109], si bien esta actitud se compatibiliza con la de una clara desconfianza a poner en manos a las agencias de control penal instrumentos de control de carácter tecnológico.

3. IMPACTOS BÁSICOS EN EL DERECHO PENAL

Para describir -en cualquier caso, como ya se anunció, de forma sucinta y fragmentaria- los impactos más significativos de las tecnologías de la información y del conocimiento en el Derecho Penal se distinguirán tres planos. En el primero, se tratarán algunas cuestiones generales que afectan a los presupuestos y límites de la intervención penal y algunas cuestiones de la imputación penal. En el segundo se considerarán, de forma también selectiva, algunas las tipologías delictivas más significativas en las que ha fraguado la tendencia considerada. Y, en tercer lugar, se añadirán unos breves apuntes penológicos y procesales.

1.1. Cuestiones generales

I). Aunque seriamente pueda dudarse de su naturaleza sustantiva, se traen aquí a colación, en primer lugar, las transformaciones que afectan al *ámbito espacial de la ley penal* que, en este terreno, en general, apuntan hacia la neutralización de algunos de los rasgos propios del sistema jacobino. Con ello se trata de dar respuesta al carácter global de la Sociedad de la Información y de la criminalidad más enraizada en ella, que relativiza o incluso neutraliza las fronteras y que, como se indicó, suele manifestarse a través de "delitos a distancia"[110].

Es conveniente no confundir conceptualmente el Derecho aplicable y la jurisdicción competente, si bien, en la actualidad, la trascendencia práctica de esta diferenciación es mínima, por lo que, al menos en nuestro país, no se establecen diferencias, extrayéndose de las reglas jurisdiccionales el régimen del Derecho aplicable[111]. Esto, no obstante, la diferencia se puede advertir aun hoy cuando se plantea que mientras respecto de la primera cuestión rige el principio de legalidad, respecto de la segunda suele reconocerse alguna virtualidad al principio de oportunidad. Quizás en el futuro, en la medida en que el sistema jacobino se vaya relajando, la diferenciación cobrará importancia, sobre todo, si se llegara a admitir que en determinados supuestos los tribunales de un país apliquen el Derecho de otro Estado. Lo que sí debe quedar claro es que, aunque en diverso grado, la tensión garantista está presente en los dos casos, pero también -si bien suavizada- cuando de lo que se trata es de decidir sobre la colisión de Derechos aplicables o de jurisdicciones competentes, que asimismo conceptualmente son asuntos distintos entre sí y de los anteriormente indicados[112].

Desde el punto de vista del control penal las transformaciones en curso se dirigen a facilitar que los derechos nacionales se puedan aplicar a hechos vinculados con Internet. Básicamente[113], esto se

[109] Cf. Speer, como en la nota 64, p. 264.

[110] Hilgendorf, como en la nota 10, p. 659

[111] Así, la doctrina dominante, al extrapolar las reglas jurisdiccionales de la Ley Orgánica del Poder Judicial: cf. Bustos Ramírez, *Manual de Derecho Penal. Parte General*, 41994 (aumentada, corregida y puesta al día por Hormazabal Malarée), Barcelona: PPU, 168-171; Bustos Ramírez/Hormazabal Malarée, *Lecciones de Derecho Penal*, *volumen I, Fundamentos del sistema penal, esquema de la teoría del delito y del sujeto responsable y de la teoría de la determinación de la pena*, 1997, Madrid: Trotta, p. 111-114; Cerezo Mir, *Curso de Derecho penal español. Parte General. I. Introducción*, 51996, Madrid: Tecnos, 193-208; Mir Puig, *Derecho Penal. Parte General*, 41996, p. 21-23; Morillas Cuevas, *Curso de Derecho Penal Español* (Dir. Manuel Cobo del Rosal), 1996, Madrid: Marcial Pons, p. 119-126; Quintero Olivares (dir., con la colaboración de Fermín Morales Prats y J. Miquel Prats Canut), *Manual de Derecho Penal. Parte General*, 1999, Pamplona Aranzadi, p. 183-187.

[112] Cf., con referencia al ámbito delincuencial analizado, Schwarzenegger, como en la nota 68, p. 111-115.

[113] Otra vía posible sería una ampliación del concepto de territorio, que abarcaría, además de los buques y naves del pabellón en cuestión, el "territorio virtual".

pretende afrontar por tres vías, que no obstante no son incompatibles entre sí, de modo que con frecuencia se trata de opciones y particularidades de las mismas que son combinables. La primera, consiste en la ampliación del sistema de excepciones a la territorialidad de la ley penal, particularmente a través del llamado principio de jurisdicción universal[114]. Da la impresión de que en estos contextos, incluso, la lucha contra el crimen reclama una inversión del sistema de regla-excepción (donde, aquí, la primera se habría venido cumplimentando con el principio de territorialidad y las excepciones con los principios de personalidad activa, real y justicia universal). Con todo, la doctrina es consciente de los riesgos que conllevaría la implantación de un sistema incondicionado de persecución *a tout court* de la delincuencia informática, aunque se asiente en la asunción explícita del principio de justicia universal[115]. De todos modos, esto no deja de ser una orientación de la que incluso se separa el Convenio sobre ciberdelincuencia, y que, por el momento, tampoco ha llegado a plasmarse en el Derecho español. En efecto, en el listado de delitos respecto de los que rige el principio de justicia universal establecido en la Ley Orgánica del Poder Judicial (que en cualquier caso lo somete a la prohibición de doble sanción[116]), no hay ningún supuesto de específica configuración informática o en red, aunque en el mismo se incluyen delitos cuya vinculación con la ciberdelincuencia es clara, como son los relativos a la prostitución y a la corrupción de menores e incapaces[117].

II). La segunda vía para evitar lagunas de punibilidad se refiere específicamente a la cuestión del "*lugar del delito*"[118]. Esta opción, en cierta medida, presupone la insuficiencia o la falta de previsión de la primera. De hecho, la doctrina pretende hacer uso de esta vía, por ejemplo, para sortear que los delitos contra la propiedad intelectual no estén en el listado abarcado por el principio de justicia universal[119]. Concretamente, se plantea considerar que rige la teoría de la ubicuidad, en virtud de la

[114] Este recurso prioritario al principio de justicia universal no impide la viabilidad de otros principios (cf. Schwarzenegger, como en la nota 68, p. 116). De hecho, si el autor es español, y se dan las condiciones del art. 23.2 de la LOPJ, la extraterritorialidad vendrá de la mano del principio de personalidad (activa); o, aunque raramente (Mata y Martín, como en la nota 69, p. 148), del principio real (cf. art. 23.3 LOPJ). Por su parte, en el Convenio sobre ciberdelincuencia las excepciones a la territorialidad no llevan al principio de justicia universal, sino -aparte del principio del pabellón- al de personalidad activa que adquiere un alcance mayor que el que en general le atribuye la legislación española, abarcando también los delitos cometidos por españoles o nacionalizados cuando ningún Estado tiene respecto de ellos competencia territorial (art. 22. Al margen de ello, el art. 24.1 del Convenio contempla la jurisdicción del Estado en que se encuentre el presunto autor, cuando no pueda ser extraditado por razón de su nacionalidad). Esto de alguna manera se corresponde con que en la actualidad la doctrina reconozca algunos rendimientos a este denostado principio, bien en general (cf., por todos, aunque no sin matices, Cerezo, como en la nota 111, p. 201 y 203 s) o, en especial, para resolver algunos de los delitos relacionados con Internet (cf. Bremer, como en la nota 38, p. 232 ss).

[115] Así Marchena, como en la nota 14, p. 80 s; Mata y Martín, como en la nota 69, p. 149 s; Seminara, "La pirateria su Internet e il diritto penale", *Rivista Trimestrale di Diritto penale dell'economia*, 1997/1-2, p. 111.

[116] Art. 23.5. LOPJ. Para otras particularidades del citado principio, cf., por todos, Cerezo, como en la nota 111, p. 206.

[117] Por cierto que la ampliación a los delitos de corrupción impuesta en la reforma de 1999 no sólo viene a cubrir una eventual laguna y a coordinar la LOPJ con el CP, sino que explicita un claro propósito de dotar de cierta estabilidad a la criminalización de estos hechos.

[118] Marchena Gómez, como en la nota 14, p. 74-79; Mata y Martín, como en la nota 69, p. 145-150; Schwarzenegger, como en la nota 68, p. 110; Seminara, como en la nota 115, p. 111.

[119] Cf. Orts/Roig, como en la nota 26, p. 163, no sin advertir las dificultades de la solución.

cual se puede entender cometido el delito en el lugar de la acción o en el del resultado, indistintamente, de forma que la jurisdicción nacional entraría en juego tanto si la acción se llevó a cabo en su territorio y el resultado tuvo lugar fuera, como si el hecho se realizó fuera produciéndose el resultado en su territorio. Es claro que, en la medida en que las conductas consideradas sean más globales, y por lo tanto tengan más contactos con puntos geográficos distintos, será posible acudiendo al principio de ubicuidad alcanzar efectos parecidos a los que conlleva el principio de justicia universal[120].

Sin embargo, la teoría de la ubicuidad no está consagrada en nuestro ordenamiento jurídico, aunque éste tampoco recoge una opción alternativa, no pudiendo invocarse en contra una eventual aplicación analógica del artículo 7 del Código Penal que recurre al criterio de la acción para determinar la legislación aplicable en el tiempo[121]. Con todo, se indica a veces que la opción de la ubicuidad cuenta con la favorable acogida de la doctrina y de la jurisprudencia. No obstante, esto debe matizarse, porque si bien la doctrina defiende tal solución como propuesta político-criminal[122], esto no aparece tan claro cuando se plantea el asunto *de lege lata*, más aún si lo que se discute no es la distribución competencial entre juzgados o tribunales españoles, sino la cuestión jurisdiccional y en última instancia la de la ley aplicable. Por otra parte, no son infrecuentes los pronunciamientos jurisprudenciales a favor de la teoría del resultado[123].

Ciertamente, los propósitos que animan a la solución de la ubicuidad son plausibles, particularmente desde la perspectiva de la evitación de lagunas -y en especial de que el autor organice el

[120] Cabría quizás plantearse que la ampliación del ámbito espacial podría ser incluso mayor, pues en principio no consta que para la aplicación del principio de territorialidad haya que tener en cuenta el *non bis in idem*, que en cambio afecta por imperativo del número 5 del artículo 23 de la LOPJ a la determinación de la jurisdicción nacional según el principio de justicia universal. No obstante, creo que la prohibición de doble sanción tiene rango constitucional y rige aunque no esté contemplada específicamente.

[121] Tampoco cabrá ya invocar en contra el art. 335 de la hoy derogada Ley Orgánica del Poder Judicial («el conocimiento de los delitos comenzados a cometer en España y consumados o frustrados en países extranjers, corresponderá a los Tribunales y jueces españoles, en el caso de que los actos perpetrados en España constituyan por sí delito, *y sólo respecto a éstos*». El subrayado es nuestro), que dio pie a la doctrina mayoritaria para afirmar que en los casos de delitos a distancia regía la teoría del resultado. Para referencias, cf. Gimbernat Ordeig/González de Amezúa, "Algunos problemas de extradición en el Derecho español", en Gimbernat, *Estudios de Derecho Penal*, ^{3}1990, p. 130 s, quienes, en cambio, tras argumentar contra ese criterio, concluyeron que «la legislación española acepta, en referencia al lugar de comisión de delito, la teoría de la ubicuidad» (ibídem, p. 131 ss).

[122] Así, si no me equivoco, Zugaldía, *Fundamentos de Derecho Penal. Las teorías de la pena y de la ley penal (Introducción tórico-práctica a sus problemas básicos)*, ^{3}1993, Valencia: Tirant lo Blanch, p. 335. Defiende la ubicuidad como criterio *de lege lata*: Bustos, como en la nota 111, p. 172 s (pero sin abarcar los delitos en tránsito, o sea, cuando ni la actividad ni el resultado se producen en el país, sino que transcurre en el interior parte del proceso. En tales casos, ni la teoría de la ubicuidad ofrece una respuesta satisfactoria. No obstante, podría considerarse que se está utilizando como medio el territorio español, quedando por tanto comprendido dentro de la actividad delictiva. El hecho -por ejemplo, un paquete bomba enviado desde Argel a Francia interceptado en España- debería considerarse una tentativa acabada llevada a cabo en territorio español,aplicando el prinicpio de ubicuidad desde el punto de vista de la actividad). Ahora, no tan claro: Bustos/Hormazabal, como en la nota 111, p. 115.

[123] V. gr. los Autos del TS 27-10-1998 y 21-1-1998.

hecho discrecionalmente buscando el país que mejor le garantice la impunidad[124]-, que es la razón normalmente invocada en su defensa. Sin embargo, tal opción, como se acaba de indicar, carece de apoyo legal, más allá del supuesto del artículo 301 del Código Penal (blanqueo de capitales), y no puede ser adoptada sin más, sobre la base de la generalización de la solución prevista en dicho precepto, sin infringir la prohibición de analogía *in malam partem*[125]. Aparte de ello –y a falta de pronunciamiento legal-, tratándose de un problema valorativo[126], para resolverlo, habrá que ponderar los intereses en conflicto, de manera que la adopción de la solución más apropiada difícilmente puede regirse sólo por la necesidad de carácter preventivo-general de eliminación de lagunas de punibilidad que, aunque de primer rango, no necesariamente excluye la consideración de otros factores o tiene absoluta prioridad sobre ellos. En este sentido -aparte de que además de la razón invocada hay otros argumentos de prevención general que pueden apuntar en la dirección contraria-, las particularidades de la materia obligan a advertir que no se trata de un asunto jurídico-penal más. Aquí están en juego intereses políticos y principios de Derecho internacional, como la prohibición de inmiscuirse en asuntos de otro Estado, que si no puede ser anulada por la invocación a exigencias formalistas y garantistas del Derecho, tampoco (o menos) podrá serlo por la demanda político-criminal de evitar las lagunas de punibilidad. Resulta difícil aceptar que, mediante una solución hermenéutica, que además conlleva el establecimiento de una específica facultad de castigar no prevista expresamente en la ley, pueda anularse o postergarse la toma en consideración de intereses internacionales como los mencionados, cuya evaluación depende de sutiles y contingentes particularidades, a las que no son ajenos aspectos materiales como el rango como potencia internacional del Estado de que se trate. Al mismo tiempo, debe reconocerse que resulta chocante que mediante este expediente técnico-jurídico relativo al lugar del delito, ajeno a las previsiones del legislador, se pudieran alcanzar en un numero significativo de casos resultados similares a los que conllevaría la opción abierta y expresa de la ley a favor del principio de justicia universal. Además, conviene advertir, que esta solución aparece como problemática si no existen reglas complementarias o fueros secundarios que determinen la competencia preferente o exclusiva[127], y aquí efectivamente estas reglas o fueros faltan. En fin, por lo menos, parece prudente plantearse que quien quiera evitar que otros Estados impongan su ley en Internet, quizás deba predicar con el ejemplo y abstenerse de imponer unilateralmente la propia[128].

Además conviene tener en cuenta que incluso en países cuyo Derecho positivo contempla, como el § 9, ap. 1 del Código penal alemán[129], el criterio de la ubicuidad, éste no se concibe normalmente como un principio incondicionado que, en el caso de publicaciones en Internet, llevara a la globalización del Derecho penal alemán[130], sino que está sometido a excep-

[124] Especialmente preocupado por ello, Schwarzenegger, como en la nota 68.

[125] Cf. Cerezo, *Curso de Derecho penal español. Parte General. II. Teoría jurídica del delito*, [6]1998, Madrid: Tecnos, p. 78-80, mostrándose, no obstante, partidario *de lege ferenda* para la determinación del lugar del criterio de la ubicuidad.

[126] Ibídem.

[127] Cerezo, como en la nota 125, p. 77.

[128] Parecido, aunque respecto de otra opción hermenéutica, Hilgendorf, como en la nota 10, p. 661.

[129] Al respecto, cf. *S/S*-Eser ([26]2001), § 9, marg. 6.

[130] Defienden la aplicabilidad del Derecho alemán en virtud del principio de terriorialidad y la regla de la ubicuidad impuesta en el § 9 del StGB: Conradi/Schlömer, "Strafbarkeit des Internet-Provider", *NStZ*, 1996, p. 366, 368 s; Graf, "Internet: Straftaten und Strafverfolgung", *Deutschte Richterzeitung*, 1999, p. 281 s; Kuner, "Internationale Zuständi-

ciones o límites[131]. Por ejemplo, se plantea la viabilidad de requerimientos o conexiones adicionales[132] en función del tipo de delito[133], de carácter subjetivo[134] u otros de orden objetivo normativo[135], que, en síntesis, aspiran a restringir la preocupante aplicabilidad global del Derecho penal alemán que podría resultar de la simple consideración de que se hayan bajado o podido bajar los contenidos ilícitos por parte de internautas situados en territorio alemán[136].

III). Todavía queda otra vía técnica a través de la cual se plantea ampliar el alcance de la jurisdicción nacional: ensanchando los conceptos de acción y resultado. Lógicamente, la magnitud de la ampliación dependerá de que para el problema considerado en el apartado anterior se siga la teoría de la acción, la del resultado o la de la ubicuidad. En cuanto al concepto de acción[137], se sugiere, por el momento de forma minoritaria, considerarla no en el sentido de acción típica completa, sino de modo que bastaría la realización parcial de la misma[138], e incluso abarcando tramos específicos de la serie causal[139]. En este último caso, si se sigue la teoría de la acción o la de la ubicuidad, se podría llegar a invocar la jurisdicción nacional aunque respecto de ella se trate sólo de un "delito en tránsito". De forma parecida, actualizando la "teoría de la mano larga", se plantea tomar como acción también el lugar en que esté ubicado el servidor y al cual el autor dirige los datos y en el que bajo su control los almacena[140]. Es generalizada la opinión de que difícilmente puede admitirse que

gkeitskonflikte im Internet", *Computer und Recht*, 8/1996, p. 453, 456; Sieber, "Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen", *JZ*, 1996, p. 429 s, apoyándose sólo en que los contenidos sean accesibles en Alemania.

131 Hay que tener en cuenta además que para hechos cometidos en el extranjero cuyo resultado tiene lugar en territorio alemán rige, de conformidad con el § 153 c II StPO, el principio de oportunidad procesal (cf. *S/S*-Eser, § 9, marg. 16).

132 A este respecto, cf. la exposición de Hilgendorf, como en la nota 10, p. 661-673.

133 Aquí podría plantearse la exclusión de los delitos de mera actividad y los de peligro abstracto realizados en el extranjero por carecer de resultado (véase a continuación el apartado III de este mismo subepígrafe).

134 Collardin, "Straftaten im Internet", *Computer und Recht*, 1995, p. 618 ss, exige que el autor se haya propuesto la accesibilidad desde Alemania (críticamente, Hilgendorf, "Überlegungen zur strafrechtliche Interpretation des Übiquitätsprinzips im Zeitalter des Internet", *NJW*, 1997, p. 1.873 s; el mismo, como en la nota 10, p. 661; más matizadamente, Cornils, "Der Begehungsort von Äusserungsdelikten im Internet", JZ, 1999, p. 394 s).

135 Por ejemplo, la propuesta (Breurer, "Anwendbarkeit des deutschen Strafrechts auf exterritorial handelnde Internet-Benutzer", *Multimedia Recht* [MMR], 1998, p. 141, 144. Críticamente, Hilgendorf, como en la nota 10, p. 664, invocando sobre todo la violación del principio de igualdad) de aplicación de los requisitos del § 7 que establece la aplicación del Derecho penal alemán a hechos cometidos en el extranjero fundamentada -aunque con salvedades, como la concurrencia de identidad de la norma- en el principio de personalidad activa (num. 1) o en el principio de personalidad pasiva (num. 2); o la que exige que concurra el principio de identidad de la norma (Kienle, *Internationales Strafrecht und Strafrecht im Internet. Zum Erfordernis der Einschränkung des Übiquitätsprinzip des § 9 Abs. 1 Var. 3 StGB*, 1998, Constanza: Hartung-Gorre, p. 173 y, para matices, p. 176. También críticamente, Hilgendorf, como en la nota 10, p. 665).

136 Eser, como en la nota 129, inclinándose por una línea intermedia, de modo que junto con el lugar material de la acción se tenga también en cuenta el emplazamiento virtual del servidor.

137 Cf. Schwarzenegger, como en la nota 68, p. 117 ss.

138 Así, en un delito de varios actos, la fundamentación de la aplicación del Derecho de un país se fundamentaría con que uno de ellos se hubiera practicado en dicho país (cf. Jescheck, *Tratado de Derecho Penal*, tomo I [trad. y adic. S. Mir Puig y F. Muñoz Conde], 1983, Barcelona: Bosch, p. 239). O, respecto de una tentativa (cf. *S/S*-Eser, § 9, marg. 4).

139 A favor, en general, Jescheck, como en la nota 138, p. 240, invocando razones de prevención general. En contra, la doctrina dominante, cf. Schwarzenegger, como en la nota 68, p. 117 s.

140 Cornils, como en la nota 134, p. 396; S/S-Eser, § 9, marg. 4 (cf., asimismo, Lehle, *Der Erfolgsbegriff und die deutsche Strafrechtszustandigkeit im Internet*, 1999, Constanza: Hartung-Gorre, p. 50 s). Críticamente, Hilgendorf, como en la nota 10, p. 666.

se entienda cometido el delito en el lugar donde se ubiquen los nodos conectores[141], si bien a veces se hace la salvedad de levantar la exclusión en el caso de que la ruta cibernética haya sido controlada por el sujeto.

Con relación al resultado, la discusión[142] es quizás más ardua[143], porque como es sabido se trata de un concepto que en general es hoy particularmente problemático[144]. Al objeto de conseguir una ampliación del ámbito del Derecho penal aplicable se propone alejarse del concepto estricto de resultado que lo identifica con la modificación del mundo exterior separada espacial y temporalmente de la acción, pues, de acoger esta acepción y seguir respecto del lugar del delito la teoría de la ubicuidad o la del resultado (se habla en tal caso de *teoría restrictiva del resultado*), entonces, no podría extenderse la jurisdicción nacional cuando la acción típica del delito de mera actividad o de peligro abstracto se hubiera llevado a cabo fuera, ya que tales delitos carecen de un resultado en el sentido indicado y su alcance típico se agota con aquella acción[145]. Para obviar tal inconveniente, se plantea atenerse al resultado en sentido jurídico-material, esto es, como afectación del bien jurídico protegido, que se pretende que no podría faltar en los delitos referidos, de manera que si para un delito de mera actividad o de peligro abstracto dicha afectación tuvo lugar en territorio nacional, entonces ya podría fundamentarse la jurisdicción. O, simplemente, apreciando que el "peligro abstracto" -lo que se suele identificar con que existiera la posibilidad de acceso- es ya un resultado[146] al menos a estos efectos, con lo que prácticamente cualquier país podría invocar su jurisdicción respecto de tales hechos. Incluso se maneja la propuesta de considerar que a estos efectos resultado no es sino la manifestación externa de la voluntad, de modo que en tanto dicha exteriorización haya tenido lugar en un determinado país habría un resultado que fundamentaría, partiendo de la teoría del resultado (o, si así se pretende, de la teoría de la ubicuidad), la aplicabilidad del Derecho penal allí vigente. Otras veces, la propuesta se limita a reseñar que el resultado comprende no sólo el resultado típico, sino también los llamados "resultados intermedios". Partiendo de una ampliación del concepto de resultado, normalmente, se llevaría a considerar que desde el momento en que los

[141] Fundamentalmente, por la ausencia en estos lugares de tránsito del bien jurídico protegido: así, Marchena, como en la nota 14, p. 75, mencionando en apoyo de la exclusión la solución adoptada respecto a su respectivo ámbito de aplicación por el art. 4.1.c) de la Directiva 95/46/CE y el art. 2.1.c) de la LOPDCP. Conforme, Mata y Martín, como en la nota 69, p. 146. Cf., por otra parte, Schwarzenegger, como en la nota 68, p. 118.

[142] Cf. Heinrich, "Der Erfolgsort beim abstrakten Gefährdungsdelikt", *GA*, 1999, p. 72 ss; Hilgendrof, como en la nota 10, p. 666-675; Kienle, como en la nota 135; Lehle, Der *Erfolgsbegriff und die deutsche Strafrechtszustandigkeit im Internet*, 1999; Schwarzenegger, como en la nota 68, p. 119-127; Sieber, "Internationales Strafrecht im Internet. Das Territorialitätsprinzip der §§ 3, 9 StGB in globalen Cyberspace", *NJW*, 1999/52, p. 2.065 ss.

[143] Aparte de los aspectos citados hay otros no menos problemáticos: por ejemplo, si deben ser considerados resultados a estos efectos los llamados "resultados típicos intermedios" o ciertas condiciones objetivas de punibilidad (cf., al respecto, Hilgendorf, "Überlegungen zur strafrechtliche Interpretation des Übiquitätsprinzips im Zeitalter des Internet", *NJW*, 1997, p. 1.873, 1.876, 1.878; el mismo, como en la nota 10, p. 662 s). No es problemático, en cambio, que el resultado de peligro concreto tenga aquella consideración (cf., no obstante, Koriath, "Zum Streit um die Gefährdungsdelikte", *GA*, 2001, p. 51, 58 s).

[144] Cf., por todos, Laurenzo Copello, *El resultado en Derecho penal*, 1998, Valencia: Tirant lo Blanch, *passim*.

[145] Cf. Hilgendorf, como en la nota 10, p. 669.

[146] Críticamente, Hilgendorf, como en la nota 10, p. 662 s.

contenidos fueran colocados en Internet podrían ser reclamados desde cualquier lugar, con lo cual se fundamentaría la jurisdicción de cualquier Estado. Para evitar esto, que cuenta con el rechazo mayoritario[147], se ha planteado una restricción que tiene un alcance técnico. Concretamente, Ulricht Sieber[148] propone entender que el resultado en virtud del cual se fundamenta la jurisdicción nacional se produce en Alemania cuando los datos son enviados desde el extranjero ("Pusch Technologie"), pero no cuando están en el extranjero y deben ser reclamados desde el territorio en cuestión (Pull-Technologie)[149].

> De todos modos, como es sabido, la determinación de si un delito es de actividad, de peligro abstracto o de resultado (de lesión o de peligro concreto) resulta con frecuencia problemática (aunque cada vez se tiende a interpretar más figuras como delitos de peligro), con lo que se presentarían de nuevo otras alternativas que vuelven a dejar relativamente abierta la posibilidad de ampliar el ámbito de la ley aplicable, si se sigue el planteamiento antes calificado de minoritario.
>
> Por otra parte, da la impresión de que la mayoría de las propuestas ampliatorias del ámbito espacial de la ley penal no responden sino a otro modo de considerar la ubicuidad que, apoyándose en que las leyes no siempre hablan de la acción o del resultado, sino de la comisión, realización o ejecución de la infracción[150], vendría a plantear que un determinado Derecho sería aplicable en tanto que pudiera determinarse una conexión "geográfica" con cualquier elemento del delito, no sólo la acción o el resultado.

En realidad, estos planteamientos expansivos suponen, en resumidas cuentas, un intento de funcionalizar los conceptos indicados en razón de un único propósito de eliminar lagunas de punibilidad, que no obstante también puede resultar cuestionable porque desconoce otros parámetros político-criminales o incluso de naturaleza constitucional que igualmente deberían ser objeto de consideración, como, por ejemplo, por un lado, que realmente existan serias posibilidades para hacer viable la efectividad de la ampliación jurisdiccional o, por otro, la prohibición de doble sanción.

Las propuestas referidas han sido planteadas en su mayoría con vistas al Derecho alemán en el que como antes se dijo rige el principio de ubicuidad. Que este principio deba regir en Derecho español es algo que, como también se indicó, no resulta evidente. En todo caso, quien pretenda invocar tal principio no puede perder de vista que el mismo carece de apoyo legal en nuestro Derecho y que, por lo tanto, hasta las mismas correcciones ven alterado su sentido porque están planteadas respecto de un sistema jurídico-positivo en el que dicho principio rige. Si acaso, esto habría de implicar que las correcciones restrictivas deben ver reforzada su capacidad limitadora. Más aún, si hay que agarrarse a la vigencia en nuestro Derecho del principio de ubicuidad, por lo menos, junto con el nexo territorial de la acción o del resultado, que deben ser interpretados sin ampliaciones injustificadas, debe requerirse un punto de conexión cualificado y razonable, que Hilgendorf ha cifrado en una "territoriale Spezifizierung"[151], pero que en mi opinión debería representar una directriz que respetara los límites legales, el carácter valorativo del problema, la naturaleza secunda-

[147] Cf. Hilgendorf, como en la nota 10, p. 667.

[148] En Hoeren/Sieber (ed.), *Handbuch Multimedia-Recht - Rechtsfragen des elektronischen Geschäftsverkehrs*, 1999, Munich: C.H. Beck, § 19, marg. 410.

[149] Críticamente, Hilgendorf, como en la nota 10, p. 668.

[150] Sobre esta ambigüedad, cf. Quintano, *Compendio de Derecho Penal. Vol. I. Parte General*, 1958, Madrid: Editorial Revista de Derecho Privado, p. 138.

[151] Como en la nota 10, p. 668-670, consciente de que no es un criterio cerrado.

ria y fragmentaria del Derecho penal, que no puede verse desplazada por el hecho de que se plantee su aplicación a hechos sólo parcialmente territoriales, las posibilidades de hacer efectiva la pretensión penal, el carácter jurídico-internacional y político-internacional del dilema. Esto se debe combinar con la amplia aplicación procesal del principio de oportunidad y una orientación pragmática que impida la innecesaria acumulación de concurrencias jurisdiccionales. En todo caso, debe plasmarse un rotundo rechazo a cualquier pretensión de abrazar a toda costa cualquier conexión meramente criminológica, sin atender al rango y valor conjunto de las diversas cuestiones implicadas.

IV). De cualquier forma, parece claro que la viabilidad de un sistema de persecución universalizado por una u otra vía es irrealizable si los desarrollos legislativos no responden a una clara tendencia armonizadora, cosa que en efecto se puede apreciar, no sin disfunciones, en la evolución del Derecho penal informático y cibernético de los últimos años, que se lleva a cabo partiendo de directrices expansivas, como claramente se advierte en el citado Convenio sobre ciberdelincuencia, por ejemplo, al plantear en el art. 6 num 1 b la criminalización no sólo de la fabricación o tráfico, sino la posesión de los llamados "hacking tools" u otro software peligroso[152].

Esta armonización se enfrenta con numerosos escollos difícilmente salvables, algunos de los cuales, dada la naturaleza global de la Sociedad de la Información, adquieren una significación destacada. Me refiero en particular a la necesidad de considerar las diferencias culturales. A este respecto, sólo quiero subrayar que, a diferencia de lo que ocurre cuando un extranjero comete un delito en España, para los casos aquí relevantes puede seguir estando en su propio país y que esos valores culturales "desviados" estén plenamente vigentes. Se puede compartir que la autodeterminación de los pueblos y la autonomía ética de los individuos no puede servir de cobertura a violaciones masivas de la dignidad humana. Sobre esto, más allá de dificultades para ponerlo en práctica no puede caber hoy ninguna duda, pero, por lo mismo, y en tanto que esa autodeterminación y autonomía forman parte del contenido de la dignidad humana no pueden ignorarse las diferencias culturales. Sin atender a consideraciones como éstas, que invitan por lo menos a considerar que la evolución del Derecho penal ha permitido reconocer efectos significativos en orden a determinar la

[152] Subraya la ampliación resultante Sieber en su intervención en el encuentro celebrado en mayo de 2001 en la Universidad de Passau (según recogen Jeßberger/Kreuß, como en la nota 34, p. 828). El precepto dice exactamente así: *1*.- Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: *(a)* the production, sale, procurement for use, import, distribution or otherwise making available of: *(i)* a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; *(ii)* a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and *(b)* the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. *2*.- This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. *3*.- Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

relevancia jurídico-penal de diferencias culturales en el Derecho penal nacional, la reflexión sobre las perspectivas de un Derecho penal *intercultural* está, a mi juicio, condenada al más absoluto fracaso[153].

V). Como ya se apuntó, en los tipos que representan más directamente a la delincuencia que nos ocupa se detecta la concurrencia de elementos que no son objeto de una simple constatación cognitiva por parte del juez, sino que necesitan operaciones más complejas. Se trata en particular de lo que han sido denominados "elementos científicamente conformados" o "elementos científicos del tipo", que escapan a la dualidad elementos descriptivos/elementos normativos[154]. Cabe intuir que la generalización de tipos con contenidos de estas características acarreará numerosas y variadas incógnitas en torno a la adecuación de la actual configuración de la Justicia y de la dogmática penales. En este sentido, Torío, siempre tan atento a estos grandes retos del Derecho penal, destaca que estos conceptos estarían libres del emotivismo o de la valoración intrínseca o constitutiva, así como la dependencia del jurista respecto del dictamen científico, y que ello hace necesaria una estrecha colaboración entre científicos y juristas[155]. No obstante, esto debe ser dejado aquí de lado, para subrayar simplemente un aspecto colateral relativo al empleo, vinculado precisamente con los avances científicos, de cláusulas que podrían denominarse "intemporales" y que tratan de salvaguardar la vigencia del principio de no retroactividad de las leyes penales y evitar lagunas de punibilidad causadas por saltos tecnológicos vinculados con la aparición de nuevos descubrimientos, técnicas, instrumentos etcétera, sin modificar el texto legal, como es el caso de la expresión "cualquier otra señal de comunicación" (art.197 CP)[156].

VI). Uno de los rasgos característicos del Derecho penal del riesgo es, como ya se indicó, un cambio significativo de las técnicas de tipificación y de las reglas de imputación. En cuanto a lo primero, la transformación se centra[157] en la opción prioritaria por formas típicas de peligro (particularmente de peligro abstracto), circunstancia que también se advierte en algunos de los tipos más significativos del Derecho penal de la Sociedad de la Información[158] y la postergación de los elementos descriptivos, en beneficio de otros de carácter predominantemente normativo o, como se acaba de ver, de elementos científicamente conformados y cláusulas intemporales. Y, respecto de

[153] Sobre ambas cuestiones, con referencias, cf., Hilgendorf, como en la nota 10, p. 675-679. Asimismo, genéricamente, Silva Sánchez, como en la nota 32, p. 103-111, también con referencias.

[154] Sobre esto, cf. Torío, "Elementos teleológicos y científicos en el tipo del injusto", Quintero/Morales (eds.), *El nuevo Derecho Penal epañol. Estudios penales en memoria del Profesor José Manuel Valle Muñiz*, 2001, Pamplona, Aranzadi, p. 817-826, que menciona también como elementos que rompen esa dualidad los "referibles a una regla de experiencia".

[155] Ibídem. Por otra parte, véase *supra* nota 47.

[156] Agustín Jorge Barreiro, en Rodríguez Mourullo (Dir.)/Jorge Barreiro (Coord.), *Comentarios al Código Penal*, 1997, Madrid: Civitas, p. 568.

[157] De todos modos, no puede desconocerse un amplio uso en las descripciones típicas de elementos de tendencia subjetiva, que de alguna manera ejercen de contrapeso ante la evidente anticipación de la barrera de lo punible. De todos modos, en el Convenio sobre Ciberdelincuencia tales elementos suelen aparecer como cláusulas disponibles para las Partes signatarias.

[158] Contrastando esta hipótesis con el reciente Convenio sobre ciberdelincuencia, sin duda, se advierte esa estructura típica, por ejemplo, en el acceso ilegal (art. 2. Véase *supra* nota 60) y en las varientes del "misuse of devices" (art. 6. Véase *supra* nota 152)

las reglas de imputación, el reforzamiento de las formas de imputación que podríamos denominar "extraordinarias", así como la flexibilización de las categorías dogmáticas tradicionales. Da la impresión de que algunos aspectos característicos de la Sociedad de la Información (carácter prolijo y promiscuo, estandarización y multiplicación de las interacciones, anonimato, carácter anómico e inseguro de los espacios virtuales...), en conjunción con particularidades del Derecho penal y aspiraciones sociales traducidas en orientaciones político-criminales, favorecerán esta reorientación de las bases del sistema de imputación.

VII). Esto necesitaría ser considerado con más detenimiento. Sin embargo, aquí sólo se va a traer a colación una problemática, la de la responsabilidad penal de los llamados *providers*[159] por los contenidos alojados o circulantes en su servidor[160], en la que se advierte un claro paralelismo con el Derecho penal del riesgo, en tanto que respecto de ellos se confirmaría que hay algunas "profesiones peligrosas" y que «los que ejercen estas profesiones deben contar permanentemente con una responsabilidad penal»[161].

Efectivamente, se ha demandado la imposición de responsabilidades penales a tales proveedores de acceso o servicio, pese a no existir en la legislación deberes genéricos o específicos de evitación, control, supresión o colaboración con la autoridades frente a aquellos contenidos. Debe matizarse que, en principio[162], pueden darse por fracasados los intentos de establecer deberes genéricos a partir de los cuales deducir tal responsabilidad, y en definitiva de convertir la mera aportación técnica o inactividad del proveedor en fuente de responsabilidad penal cuando no existe una obligación específica. En este sentido, la jurisprudencia internacional habría jugado un papel inverso[163] al desempeñado por la jurisprudencia europea en el desarrollo de los rasgos más incisivos del Derecho penal del riesgo, oponiéndose a una fundamentación de esa responsabilidad asentada prioritamente en deberes de carácter genérico[164]. De igual forma, la Directiva 2000/31/CE del Parlamento y del Consejo europeos contempla que no se impondrá a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen o de realizar búsquedas activas de hechos o circuntancias reveladores de actividades ilícitas. Naturalmente, esta orientación no res-

[159] Cf. Sieber, como en la nota 148, § 19, margs. 106 ss. En el Convenio sobre ciberdelincuencia, a los efectos del propio Convenio, se entiende por "proveedor de servicio" (art. 1, c) «cualquier entidad pública o privada que proporciona a los usuarios de su servicio la posibilidad de comunicar por medio de un sistema informático» y «cualquier otra entidad que procesa o *stores* datos informáticos en nombre de tal servicio de comunicación o usuarios de tal servicio».

[160] Orts/Roig, como en la nota 26, p. 136 s.

[161] Hassemer/Muñoz Conde, *La responsabilidad por el producto en Derecho penal*, 1995, Valencia: Tirant lo Blanch, p. 168.

[162] Un mínimo de prudencia aconseja no descartar una vuelta atrás por más que las declaraciones restrictivas provengan de la jurisprudencia constitucional, lo que les da cierta estabilidad, teniendo en cuenta que la tensión entre libertad y seguridad que subyace se acentúa en temas especialmente sensibles, como los del terrorismo y la protección de la infancia (a este respecto, cf. Picotti, como en la nota 169, p. 212, subrayando el papel de la normativa internacional y la absoluta necesidad de una protección especial de esta naturaleza, incluso respecto a meras "comunicaciones" o manifestaciones caprichosas para garantizar a los menores un desarrollo equilibrado y libre de su personalidad -«condición especial, a su vez, para el correspondiente desarrollo y progreso de la sociedad futura»).

[163] No obstante, cf. Hilgendorf, como en la nota 10, p. 674, respecto de la sentencia del Tribunal Supremo alemán en el *caso Töben*.

[164] En especial, el Tribunal Supremo norteamericano respecto que la *Communications Decency Act* de 1996.

ponde sólo a criterios jurídicos, sino que se asienta también en razones económicas[165], políticas y sociales de peso. En especial, una opción consecuente con la pretensión indicada sería técnicamente inviable, congestionaría los sistemas de telecomunicación y acabaría con uno de los mayores atractivos de la red, su la naturaleza abierta.

A mi juicio, la discusión sólo ha alcanzado un mínimo de racionalidad político-criminal en el momento en que el Derecho cibernético[166] ha empezado a fijar las posiciones jurídicas de determinados sujetos intevinientes en las telecomunicaciones en red como las que establece la Ley de Servicios Telemáticos (TDG) alemana -cuyo § 5, en síntesis, excluye la responsabilidad jurídica (en general) del proveedor, respecto de contenidos ajenos, cuando no tiene conocimiento del carácter ilícito de la información difundida o carece de posibilidades técnicas para evitar o bloquear la difusión o suprimir los contenidos ilícitos-, pues sin apoyo en obligaciones específicas, a mi juicio, la discusión carece de toda singularidad y comporta, cuando se pretendan derivar imputaciones penales, una expansión inadmisible del Derecho penal. Esta tendencia, que es internacional, sin embargo, no ha llegado a cristalizar todavía en el Derecho español que, por el momento, debe afrontar la discusión en torno a la responsabilidad penal de los proveedores al margen de estas especificaciones.

En todo caso, en orden a centrar el interés principal del debate, hay que limitarse a considerar, como señalan Orts/Roig[167], los supuestos de contenidos circulantes por espacios abiertos de la red, no así en aquellos casos en que se transmiten de forma restringida a través del correo electrónico[168]. De otra parte, tampoco puede resultar particularmente problemático, si bien en este caso en el sentido de afirmar la responsabilidad penal, cuando la intervención del proveedor se realiza como una aportación más de un plan criminal, prevaliéndose de aquella condición, o cuando es el mismo proveedor el que de forma exclusiva lleva a cabo el hecho, colocando en la red los contenidos penalmente relevantes.

Para ilustrar la problemática planteada, que ocupa a la doctrina española y extranjera[169], cabe traer a colación, dejando al margen los detalles, el conocido caso "CompuServe" juzgado en Alemania en el que se ventilaba la responsabilidad del director de esta empresa alemana que hacía de proveedora e intermediaria para Alemania de su matriz "CompuServe-USA", respecto de la pornografía infantil a la que podían acceder los suscriptores alemanes. La empresa alemana fue inicialmente

[165] Cf. *S/S*-Lenckner/Perron, § 181, marg. 66 b.

[166] Del mismo modo que en el Derecho informático propiamente dicho, la LOPDP impone a responsables o encargados de los ficheros automatizados obligaciones de control y colaboración bajo el principio de corresponsabilidad.

[167] Como en la nota 26, p. 164. Si no me equivoco, en la misma línea, Picotti, como en la nota en la 169, p. 213; Seminara, como en la nota 115, p. 99.

[168] De todos modos, pueden resultar problemáticos determinados casos como las llamadas "listas" que son espacios relativamente circunscritos pero, al mismo tiempo, relativamente abiertos, y en las que puede haber sujetos, como administradores o moderadores, que asumen roles que implican cierto control.

[169] Boese, *Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet*, Francfort del Meno, 2000; Conradi/Schlömer, "Strafbarkeit des Internet-Provider!, NStZ, 1996, 366 ss (Parte I) y 472 ss (Parte II); Derksen, "Strafrechtliche Verantwortung für in internationalen Computernetzen verbreitete Daten mit strafbarem Inhalt", *Neue Juristische Wochenschrift* (NJW), 1997, p. 1.878 ss; Picotti, "Fundamento y límite de la responsabilidad penal de los proveedores de acceso y servicio en Internet", *RdPP*, 3, 1999, p. 211-222; Magni/Spolidoro, "La responsabilità degli operatori in Internet: profili interni ed internazionali", *Diritto informatico*, 1997, p. 61 ss; Ritz, *Inhaltverantwortlichkeit von Online-Diensten. Strafbarkeit von Online-Diensten in ihrer Funktion als Inhalteanbieter, Online-Service-Provider und Internet-Access-Provider für die Verbreitung von Pornographie im elektronischen Datennetz (Ein Rechtsvergleich)*, 1998 ,Francfort del Meno: Peter Lang; Seminara, como en la nota 115, p. 71 ss; Sieber, "Responsabilità penali per la circulazione di dati nelle reti internazionali di computer. Le nuove sfide di Internet" (trad. M. Sforza), *RTDPE*, 1997, p. 743-785 y 1.193-1232.

advertida por la fiscalía de Baviera, lo que le llevó a instalar un software que hacía de filtro, pero que al poco tiempo se vio que no podía evitar por completo el acceso de los usuarios alemanes. Pese a que los técnicos informáticos declararon que técnicamente no era posible impedirlo al cien por cien, la Audiencia de Munich condenó al director de CompuServe, si bien el Tribunal del Land le absolvió por entender entre otras cosas que, pese a la estrecha relación empresarial, el recurrente no había actuado dolosamente, si no que más bien había intentado seriamente el bloqueo de los contenidos ilícitos[170].

Generalmente, el título invocado para plantearse la responsabilidad de proveedores de acceso o servicios es la comisión por omisión, pese a que respecto de ciertos delitos la viabilidad de este título habría de ser directamente excluida si se toma en cuenta la opinión de algunos autores que, a la vista del artículo 11 del Código penal español, que se refiere a los "delitos que consistan en la producción de un resultado", entienden que habría que dejar fuera los delitos de mera actividad y los de peligro abstracto, a salvo de que en ellos se contemple específicamente una conducta omisiva.

Pero, dejando esto de lado, y sobre todo a la vista de que como se ha indicado en el Derecho español no se impone a los proveedores ninguna obligación específica, habrá que plantear la discusión en orden a si cabría fundamentar por otra vía la eventual responsabilidad en comisión por omisión. A falta de un deber legal genérico o específico del que pueda extraerse una posición de garante, se plantea si sería entonces título suficiente la previa injerencia, naturalmente, en los casos en que el proveedor haya contribuido positivamente a la creación de un peligro. A este respecto se suele indicar mayoritariamente que la apertura de espacios o la oferta de soportes en red son conductas socialmente adecuadas, abarcadas por el riesgo permitido y además lejanas respecto al peligro de realización del resultado que no sería inherente al actuar precedente, sino que más bien se realizaría autónomamente sólo por la acción voluntaria del autor de la comunicación ilícita[171]. Otras alternativas de exclusión de tal responsabilidad residen[172] en la ausencia de bases de imputación objetiva[173] o de imputación subjetiva de la comisión por omisión, que en no pocos casos, quizás algunos de los más significativos -esto es, del Derecho penal sexual de menores-, vendrá dada por la dificultad de que el proveedor comparta el ánimo lúbrico invocable en estos delitos aún cuando se trate de omisiones.

Sin embargo, hay una serie de datos prelegislativos que permiten advertir que en el Derecho español se consagran en breve algunos de los deberes específicos que vienen imponiéndose en el Derecho extranjero. La *Directiva 2001/31/CE del Parlamento Europeo*, como se ha dicho, no contempla la imposición de deberes genéricos, salvo una obligación de retirada con celeridad respecto de contenidos de carácter ilícito que le sean conocidos y *sensu contrario* su responsabilidad (no específicamente penal) sólo si ha originado la información o han intervenido en la utilización ilícita de la tecnología o, por no actuar con celeridad para retirar tales contenidos, si conocieron su carácter ilícito (particularmente, artículos 12 al 15). En este momento, se tramita la adaptación de esas directrices a través del *Anteproyecto de ley de Servicios de la Sociedad de la Información y de comercio electrónico*. En síntesis, el Anteproyecto parte del principio de que los prestadores de servicios de la Sociedad de la Información sólo son responsables (civil, penal o administrativamente) de los contenidos que ellos mismos elaboren

[170] Una síntesis del caso en Hilgendorf, como en la nota 10, p. 657 ss.

[171] Sieber, como en la nota 169, p. 1.206-1.208. Aparentemente conforme, Picotti, como en la nota 169,

[172] Sobre todo ello, cf., Derksen, como en la nota 169, p. 1.883-1.885; Picotti, como en la 169, p. 212 s; Sieber, asimismo como en la nota 169, p. 1.213-1.220.

[173] Así, respecto de los resultados eventualmente no impedidos, pero sin precisar más el principio de no imputación, Sieber, como en la nota 169, p. 1.219.

o que se hayan elaborado por su cuenta (artículos 12 y 13.1), excluyendo su responsabilidad por contenidos ajenos, en el ejercicio de actividades de intermediación, transmisión, copiado, almacenamiento o localización cuando respeten las normas relativas a la responsabilidad por transmisión o provisión de acceso (art. 14), por almacenamiento o reproducción provisional o temporal (art. 15), por almacenamiento a petición de usuario (art. 16) o por provisión de enlaces a contenidos o instrumentos de búsqueda (art. 17).

A título meramente elucubrativo, se puede plantear si en tales condiciones procedería declarar la responsabilidad en comisión por omisión del proveedor, en base a los deberes que impone el Anteproyecto de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico. La respuesta necesitaría de un análisis pormenorizado que aquí no se puede llevar a cabo. Pero sí pueden establecerse algunas pautas orientativas: estas particularidades consagran sólo títulos posibles de responsabilidad diversa, sin prejuzgar, a salvo del principio de proporcionalidad, si a cada violación de estas obligaciones se le deben reconocer consecuencias jurídico-penales o simplemente civiles o administrativas. Más bien, el modo en que quedan configurados en el Anteproyecto permite poner de manifiesto que sólo en casos particularmente graves entraría en juego la responsabilidad penal. Una segunda cuestión concierne a la naturaleza de estas previsiones y su entronque en el sistema de presupuestos del delito. A este respecto, creo que aquellas previsiones actúan a modo de filtro de la responsabilidad penal, de manera que para poder plantearse ésta, los hechos, como mínimo, habrán de suponer una infracción de los deberes indicados, debiendo rechazarse "automáticamente" aquella responsabilidad si los hechos que se realizaron están bajo la cobertura de limitación de responsabilidad que establece el *Anteproyecto*. No obstante, la efectividad de esta función de filtro debe coordinarse con el sistema de presupuestos de la responsabilidad penal que rige en nuestro Derecho, lo que entre otras cosas, determinará que, salvaguardando dicha función, se habrán de sincronizar estas previsiones con las diversas fases de imputación que integran aquel sistema. No creo que sea posible una solución homogénea, como se ha planteado en la doctrina alemana, entre otras cosas porque es preciso atender a las previsiones específicas de cada tipo penal y a las peculiaridades del requisito a que se condiciona la limitación de responsabilidad: no tiene que tratarse del mismo modo el respeto a «las normas generalmente aceptadas y empleadas por el sector para la actualización de la información» (art. 15, c, del Anteproyecto) que el «conocimiento efectivo de que la actividad o la información a la que se remiten o recomienda es ilícita» (art. 17, 1, a del Anteproyecto). Es decir, que habrá que evaluar específicamente si estos requerimientos son elementos del tipo (objetivo o subjetivo), se contemplan como causas de justificación o afectan a la culpabilidad. De todos modos, el hecho de que la responsabilidad que se pueda invocar sea, en la mayoría de los casos, en comisión por omisión y dada la carga adicional que el tipo, sobre todo el tipo objetivo, tiene en ella, arrastrará a éste muchas de las cuestiones planteadas. En principio, esta sincronización hará, al menos en términos de argumentación, más factible la concreción de las especificidades penales de estas bases de responsabilidad, que, como se ha indicado, y debe ser acentuado, se plantean sin prejuzgar el tipo de responsabilidad jurídica que corresponde. En fin, el hecho de que se llegaran a consagrar como Derecho positivo no excluiría que respecto de aspectos no regulados por el todavía Anteproyecto hubiera de plantearse la reflexión que antes se hizo respecto del Derecho vigente. Del mismo modo que, ni en ese momento ni ahora, cabe excluir otros títulos de imputación que no pasen por el artículo 11.

VIII) Para acabar con este subepígrafe, otra de las cuestiones generales a las que se ha prestado cierto interés es a la posibilidad de invocar para delitos cometidos por Internet la aplicación del artículo 30 del Código penal, cuyo primer número establece que en los delitos o faltas cometidos utilizando medios o soportes de difusión mecánicos no responderán criminalmente ni los cómplices ni quienes los hubieren favorecido personal o realmente, y en el 2 un conocido sistema de responsabilidad escalonada que empieza en el redactor y termina en el director de la empresa grabadora, reproductora o impresora. Antes que nada conviene poner de manifiesto que tal posibilidad sólo se plantea respecto de delitos con las particularidades que justifican el artículo 30, lo que hoy se entiende que afecta no sólo a delitos como las injurias o contra la intimidad, sino que pueden contemplarse otros siempre que, como los antes citados, su injusto solamente se capte en virtud de la extensión del conocimiento generalizado de lo que alguien dice o escribe[174]. Pero, dicho esto, la

[174] Así, Quintero, en Quintero (Dir.), como en la nota 107, p. 320. Conforme, Aránguez Sánchez, en Cobo del Rosal (Dir.), *Comentarios al Código penal. Tomo III. Artículos 24 a 94*, 2000, Madrid: Edersa, p. 329.

doctrina parece no tener inconvenientes para ampliar su ámbito de aplicación a medios de comunicación diversos del trío tradicional (prensa, radio y televisión) y por lo tanto a aquellos que han aparecido gracias a las tecnologías digitales, como Internet[175], para lo cual, se podría optar por el sentido propio de ingenio reproductor que el ser humano utiliza[176]. Esta extensión no puede ser impedida con la pretensión de que el artículo 30 constituye un mecanismo que amplía los títulos de imputación, pues, al contrario, los reduce, con lo que la eventual limitación por prohibición de analogía contra reo no tendría aquí valor[177]. Por otra parte, las previsiones del número 2 del artículo 30 no derogan o neutralizan las exigencias generales de imputación objetiva y subjetiva, y en especial el requerimiento de dolo en los delitos dolosos, ni las propias del artículo 28 (al que el 30 se remite expresamente), de manera que el director de la empresa difusora no responderá en ningún caso, aunque hubieran muerto el redactor del texto y el director de la publicación, si no hubiera actuado respecto del delito cometido de forma dolosa, y en su caso concurriendo los elementos subjetivos del tipo de que se trate. Con estas precisiones, la posibilidad de extender al ámbito indicado el régimen del artículo 30 depende tan sólo de que efectivamente exista una razón de identidad o semejanza entre los medios de difusión ubicados en Internet y los clásicos. Pero esto sólo parece posible parcialmente, en lo que respecta al número 1, no así para las más específicas previsiones del número 2, porque las posiciones de dirección a que se refiere dicho número no suelen darse en Internet[178].

No obstante, Orts/Roig[179] parecen considerar la posibilidad de que servidores y proveedores respondan en cascada, por las injurias o calumnias remitidas por correo electrónico cuando tuvieran conocimiento de ellas y control sobre el correo, aunque destacan que esto será inusual. Del mismo modo, siguen, responderían en cascada autores del texto, directores, ... cuando aquéllas se incluyen en periódicos electrónicos. En cambio, cuando la calumnia o injuria aparecen en la página web, la responsabilidad del proveedor y del suministrador estará condicionada por el conocimiento que tengan de que aquéllas se han producido. En cuanto a los delitos contra la propiedad intelectual[180], admiten el recurso al artículo 30 cuando se trate de información propia o seleccionada por quien ofrece el servicio, de manera que conforme al número 2 respondería el director de la publicación si no puede ser identificado el autor, por ejemplo, del plagio. En cambio, si el proveedor únicamente proporciona al usuario un servicio de acceso, transmisión o almacenamiento de los datos, no procederá declararlo penalmente responsable, salvo que conozca el carácter delictivo del hecho, pero incluso esto será difícil tanto por razones legales sustantivas como procesales si el autor cometió el hecho en el extranjero.

1.2. Formas típicas informáticas

I). Para casi todas las modalidades delictivas las tecnologías informáticas y de la información y comunicación pueden llegar a jugar no sólo un papel episódico, sino principal[181]. En este sentido, lo que va ser objeto de atención aquí no será, normalmente, que «should someone cause death or injury not with a blunt instrument but by interfering with a traffic control system, he would be

[175] Cf. Aránguez, como en la nota 174, p. 332.
[176] Así Quintero, como en la nota 174, p. 320.
[177] En esta línea cf. Quintero, como en la nota 174, p. 319 s.
[178] Cf. Aránguez, como en la nota 174, p. 346.
[179] Como en la nota 26, p. 144 s.
[180] Orts/Roig, como en la nota 26, p. 87.
[181] Véase *supra*.

equally liable to conviction of an offence against the person»[182]. Y es que no es menos responsable de las lesiones o muertes que cause quien manipula el sistema informático regulador del tráfico viario provocando graves accidentes, que quien con un arma blanca infiere aquéllas, aunque ni el delito de homicidio ni las lesiones contemplen específicamente que el medio lesivo o mortal sea informático o de alta tecnología. La selección de los delitos estudiados a continuación, fragmentaria y heterogénea en sus resultados, tiene como principal clave aglutinadora que esos componentes tecnológicos hayan sido incorporados al tipo de forma más o menos explícita. En especial, se estudian aquellos tipos que han sido introducidos últimamente en nuestra legislación penal para cubrir las lagunas detectadas y cuyo tratamiento jurídico-penal es, en cualquier caso, igualmente heterogéneo. Por otra parte, más que un estudio exhaustivo, que desborda las posibilidades de este trabajo, lo que interesa es reflejar cómo se ha ensanchado el Derecho penal con motivo de los delitos analizados, y cómo esta expansión, pese a no articularse, en general, en torno a la técnica de los delitos de peligro abstracto, resulta también desformalizadora y, además, responde a un propósito claramente agravatorio de la responsabilidad penal, sin que, no obstante, estén siempre claros y justificados los fundamentos agravatorios.

II). Así pues, dada la versatilidad de las tecnologías de la información y de la comunicación, prácticamente cualquier delito puede cometerse interviniendo éstas. Por ejemplo, cabe mencionar las defraudaciones al consumo del art. 283, la falsificación de cuentas de una sociedad prevista en art. 290, el blanqueo de capitales, contemplado en los arts. 298 a 304, los estragos regulados en el art. 346, los desórdenes públicos, previstos en el art. 560.1, u otras de más compleja cualificación típica como los fraudes en transacciones comerciales[183] En todo caso, tal posibilidad está condicionada a que la concurrencia instrumental o como objeto de lo informático no quede descartada por la textura típica de cada figura[184].

Hay también un delito cibernético que parece haber adquirido cierta actualidad y de alcance similar a los de pornografía infantil en red, por cuanto como ésta la punición se fundamenta en la difusión de contenidos ilícitos. Me refiero a la difusión de propaganda e ideas que inciten al racismo y a la xenofobia, cuya punición habría de reconducirse a las previsiones del art. 510 del Código penal.

III). En todo caso, a continuación sólo se prestará atención a algunos delitos con la relevancia indicada. Concretamente, se va a prestar atención a un delito contra las personas, un contra el patrimonio y otro contra el orden socioeconómico.

1.3. Derecho penal sexual

A). En materia sexual se experimentó en las últimas décadas[185] una progresiva despenalización[186], lo que permitió la reconstrucción de la fundamentación material de los delitos sexuales en

[182] Smith & Hogan, *Criminal Law*, [9]1999 (a cargo de John Smith), Londres y otras: Butterworths, p. 706.
[183] Para estas figuras cf. Orts/Roig, como en la nota 26, p. 158-162.
[184] Cf. Gutiérrez Francés, como en la nota 8, p. 252.
[185] Esta tendencia, en gran medida, ha sido supranacional y, respecto del proceso evolutivo del Derecho Penal y de la Política Criminal en Alemania tras la Segunda Guerra Mundial analizado por Roxin, *La evolución de la Política criminal, el*

torno a la libertad sexual[187], en definitiva, al derecho de la persona a no verse involucrada sin su consentimiento por otra persona en un contexto sexual[188]. Sin embargo, creo que los datos disponibles resultado de las reformas recientes, a saber la promovida por la LO 11/99[189], junto con las anunciadas a corto plazo, en general, dejarían traslucir más que un reacondicionamiento de las placas del *nuevo* Derecho penal sexual[190], el decidido propósito de concluir ese ciclo legislativo, en ámbitos específicos, como la protección de menores. En cualquier caso, el sentido de la novedad sería el endurecimiento, plasmado sobre todo en la elevación de los marcos punitivos[191], que también se corresponde con una intención explícita del legislador de abarcar, junto a la libertad perso-

Derecho penal y el Proceso penal (trad., en lo que respecta a esta parte, de Carmen Gómez Rivero), 2000, Valencia: Tirant lo Blanch, p. 17-36, coincide con la fase caracterizada por la fundamentación material del delito en el principio de lesividad social y la reorientación de los fines de la pena a la prevención, sobre todo la resocializadora, conciliándola con las exigencias garantistas (p. 20-25). Esta fase se enmarcaría entre la que lo fundamentaba en la ley ética y asumía una concepción retribucionista de la pena y un perfil garantista (p. 18-20), y la tendencia, en curso, que desplaza la concepción material del delito a la prevención general asegurativa, y debilita las metas resocializadoras y los derechos del acusado (p. 25-31).

186 Díez Ripollés, "El objeto de protección del nuevo Derecho penal sexual", *Revista de Derecho Penal y Criminología*, 2ª época, 6 (2000), p. 89, habla de un periodo de más de veinte años en el que las iniciativas político-criminales han ido, sin excepción, en la dirección opuesta a la protección de la moral sexual colectiva.

187 En el sentido del texto, cf. Tamarit, *La protección penal del menor frente al abuso y explotación sexual. Análisis de las reformas penales de 1999 en materia de abusos sexuales, prostitución y pornografía de menores*, 2001, Pamplona: Aranzadi, p. 55. Vid. también la nota precedente y p. 71 s, donde el autor allí citado afirma que «la libertad sigue constituyendo, con más motivos que nunca tras la aprobación del nuevo código penal el punto de referencia valorativo más esclarecedor del contenido de los delitos sexuales, y el criterio sobresaliente para la interpretación teleológica».

188 Textualmente, Díez Ripollés, *La protección de la libertad sexual. Insuficiencias actuales y propuestas de reforma*, Barcelona: Bosch, 1985, p. 23; todavía, el mismo, como en la nota 186, p. 71 s.

189 Conviene recordar que, en general, la reforma de 1999 se quedó a medio camino de las pretensiones agravatorias del Proyecto gubernamental (a este respecto, Morales Prats/García Albero, en Quintero (Dir.), como en la nota 107, p. 877). Sobre esta reforma: Alonso Pérez, *Delitos contra la libertad e indemnidad sexuales (perspectiva jurídica y criminológica): legislación, comentarios y jurisprudencia*, 2001, Madrid: Dykinson; Boix Reig/Orts Berenguer, "Consideraciones sobre la reforma de los delitos contra la libertad sexual, por la Ley Orgánica 11/1999", en Quintero Olivares/Morales Prats, *El nuevo Derecho Penal Español. Esudios Penales en Memoria del Profesor José Manuel Valle Muñiz*, 2001, Pamplona: Aranzadi, p. 1.007-1.031; García Albero, "El nuevo delito de corrupción de menores (art. 189.3)", *CDJ*, 2000; Gimbernat, "Prólogo" a Gimbernat/Mestre (comp.), *Código penal*, 51999, Madrid: Tecnos; Matallín Evangelio, *El nuevo delito de acoso sexual*, 2000, Valencia: Ediciones Revista General de Derecho; Orts/Suárez-Mira, *Los delitos contra la libertad e indemnidad sexuales*, 2001, Valencia: Tirant lo Blanch; Orts Berenguer/Alonso Rimo, "La reforma de los delitos contra la libertad sexual", en *Derecho Penal, Sociedad y Nuevas Tecnologías*, 2001, en Zúñiga/Mendez/Diego (coords.), como en la nota 47, p. 29-66; Pérez Parente, "La nueva reforma de los delitos contra la libertad sexual: algunos aspectos polémicos", *LL*, num. 5.092, 7 de julio de 2000, p. 1-5; Tamarit, "Muerte y resurrección del delito de corrupción de menores", *Aranzadi Penal*, 6 (1999).

190 De alguna manera creo que esta percepción es la que subyace cuando Díez Ripollés, como en la nota 186, p. 73, afirma que «el derecho penal sexual ha venido registrando desde 1978 una evolución constante, sólo levemente alterada en 1999».

191 Al menos en este aspecto, aquella tendencia, en realidad, ya era apreciable en el Código de 1995 (cf. Cancio Meliá, en Rodríguez Mourullo [Dir.]/Jorge Barreiro [Coord.], como en la nota 156, p. 515 s). Por otra parte, no han faltado desajustes con resultados contrarios (cf. Morales/García Albero, como en la nota 189, p. 895 y 898 s) y excepciones.

nal, bienes jurídicos notablemente más difusos y despersonalizados[192] y con un clima decididamente defensista, favorable a postergar la resocialización de delincuentes sexuales y a blindar su responsabilidad penal frente a las consecuencias que se siguen ordinariamente de la inimputabilidad[193]. En general, esta reversión se ha fundamentado en una necesidad de mayor protección de menores (e incapaces)[194/195], pero ha tenido un efecto expansivo en relación con la protección de adultos[196].

B). Una muestra más de esta intensificación de la respuesta penal son las previsiones cualificadoras del artículo 187.3, respecto de las modalidades previstas en los números 1 y 2, y del artículo 189.2, respecto de las figuras recogidas en el número 1, para el caso de que el culpable de los delitos citados formara parte de una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades. Con ello se quiere afrontar la convicción de que este tipo de criminalidad es con frecuencia organizada[197]. Pero con ello se pone también de relieve que este repunte agravatorio del Derecho penal sexual, al tiempo que participa de una peculiaridad criminológica frecuente en el Derecho penal del riesgo[198], sigue su tendencia expansiva difusa y desconectada de la gravedad que se atribuye a esa peculiaridad. En efecto, como otras veces, el plus punitivo queda configurado en el tipo de un modo tan impreciso y abierto que abarca no sólo los casos en que haya una sólida estructura organizativa o asociativa, contra la que es difícil luchar y que puede hacer mucho daño (en especial porque da continuidad a la voluntad criminal), y que justifican la agravación, sino concurrencias de menor peligrosidad[199]. Además, la articulación técnica de la respuesta parece incluso que está desenfocada, porque, si se quieren respetar los límites que impone el texto, quedan fuera casos de no menos gravedad. Piénsese, por ejemplo, cuando la

[192] En este sentido es significativo el punto de vista de Picotti, como en la nota 169, p. 211-212. En general, con respecto a la responsabilidad penal de los proveedores de acceso y servicio (véase *supra*), a propósito de la tensión entre libertad de comunicación (y certeza de operadores y usuarios) y la eficaz tutela de otros bienes e intereses, hace referencia junto al honor, la reputación, la libertad personal, la *privacy*, a las «"buenas costumbres" y "moral pública", que dado que tienen una dimensión intrínseca de carácter colectivo, están expresamente indicadas como límite para todo tipo de "manifestación", tanto en el art. 21.5 CI, como del art. 9.2 del Convenio Europeo [se refiere al de Salvaguarda de los Derechos del Hombre], cuanto de los arts. 18.3 y 19.2, letra b) del Pacto Internacional [de los Derechos Civiles y Políticos]».

[193] En realidad, esta orientación restrictiva, que de alguna manera impide o dificulta la relevancia en términos de imputabilidad de trastornos sexuales y patologías psíquicas asociadas a dichos trastornos, parece que siempre ha regido en el Derecho penal sexual. En especial, sobre la imputabilidad del pedófilo, cf. Tamarit, como en la nota 187, p. 143-151, indicando que el problema tiene muchos puntos en común con el de las psicopatías.

[194] Cf. Orts/Alonso, como en la nota 189, p. 40.

[195] Incluida la ampliación del plazo de prescripción, conforme a lo previsto en el artículo 132.1 (sobre esto, cf., por todos, Orts/Alonso, como en la nota 189, p. 61-64).

[196] Cf. Tamarit, como en la nota 187, p. 35 s, destacando la perversión que supone la utilización de la protección de menores como coartada o caballo de Troya de una política criminal regresiva.

[197] Cf. Díez Ripollés, "Trata de seres humanos y explotación sexual de menores. Exigencias de la Unión y legislación española", *Revista Penal*, 2, 1998, p. 21, indicando que tales conductas constituyen una forma grave de la delincuencia organizada internacional. Igual, Muñoz Conde, *Derecho Penal. Parte Especial*, [13]2001, Valencia Tirant lo Blanch, p. 234. Respecto de los casos de prostitución y trata de mujeres, cf. Medina Ariza, "Una introducción al estudio criminológico del crimen organizado", en Ferré/Anarte (eds.), p. 116-118. Respecto de la explotación de menores, cf. Maqueda Abreu, "El tráfico de personas con fines de explotación sexual", JpD, 38 (2000), p. 25 ss; más ampliamente, la misma, *El tráfico sexual de personas*, 2001, Valencia: Tirant lo Blanch.

[198] Por estas razones se explica que se diga que el nuevo Derecho penal sexual también asume algunas propiedades del Derecho penal para la Sociedad del Riesgo. En este sentido la intervención de Herzog, "Risiko und Strafrecht", en el Seminario *Crítica y Justificación del Derecho penal en el cambio de siglo. El análisis crítico de la Escuela de Franckfort*, celebrado en Toledo los días 13-15 de abril de 2000 (he consultado la versión alemana dactilografiada).

[199] Sobre todo ello, véase mi "Conjeturas sobre la criminalidad organizada", en Ferré/Anarte, *Delincuencia organizada*, en cuanto los aspectos jurídico-penales sustantivos del concepto de criminalidad organizada, p. 25-30, por lo que se refiere a sus efectos (p. 44-48) y en cuanto al desfase planteado (p. 55 s).

organización no se dedica, más que de forma episódica, a las actividades sexual-criminales descritas o, sencillamente, esa dedicación no puede ser probada. Y, evidentemente, no se puede inferir sin más ni de la constancia de otras actividades criminales ni de la específica conducta sexual de que se trate.

C). El paralelismo con el *moderno* Derecho penal se advierte asimismo en la concurrencia de dos instancias que han influido en la ampliación del Derecho penal sexual, como son, de un lado, la aparición de casos muy sonados que los medios de comunicación han recogido ampliamente[200] y, de otro, las demandas o propuestas de organismos internacionales de todavía más dureza, que, por cierto, todavía estarían pendientes de satisfacer[201]. No obstante, la internacionalización de la delincuencia sexual sólo es afrontada en la legislación penal española de forma parcial y, además, la previsión de eficacia de la reincidencia internacional, contenida ahora en el art. 194, no es nueva. En el Código sólo el artículo 189.1 b) (y el inciso complementario *in fine* de este número) proporciona un instrumento de internacionalización, si bien no hay que olvidar la Ley Orgánica del Poder Judicial, cuyo artículo 23.4, tras la reforma de la LO 11/99, incluye entre los delitos respecto de los que rige el principio de protección universal la prostitución y la corrupción de menores.

D). Pero, como se ha indicado, la línea central del replanteamiento del Derecho penal sexual -que en España se ha traducido en la reforma promovida por la LO 11/99, de 30 de abril y se enmarca en las orientaciones predominantes en la Política criminal internacional que, en el ámbito europeo[202], se han plasmado, particularmente, en la Acción común del Consejo de la Unión de 24 de febrero de 1997[203]- se apoya en el reforzamiento de la protección de los menores e incapaces, en la que, precisamente, desempeña un papel destacado la invocación a ataques relacionados con el uso de nuevas tecnologías[204], sobre todo en lo concerniente a Internet, en tanto que la demanda de representaciones sexuales infantiles habría aumentado por esa vía, con el consiguiente incremento de los atentados sexuales en que se ven implicados menores.

El artículo 9 del *Convenio sobre ciberdelincuencia* contempla (num. 1) que cada Parte criminalice infracciones relativas a la pornografía infantil, en las que el autor de forma intencional y sin autorización y mediante un sistema informático (a) la produce, (b) la ofrece o facilita su disponibilidad, (c) la distribuye o transmite, (d) la procura para sí mismo o para un tercero (e), o la posee en un sistema informático o en un medio de almacenamiento de datos. El número 2 define, a tales efectos, la "pornografía infantil" como cualquier material pornográfico que representa de forma visual (a) a un menor llevando a cabo comportamientos sexuales explícitos, (b) cuando éstos los lleva a cabo alguien que aparece como un menor o (c) cuando unas imágenes realistas representan a un menor realizando tales comportamientos. No obstante, el número 4 habilita a las Partes a obviar en todo o en parte las letras d) y e) del número 1.

En particular, estos ataques provienen de la grabación de escenas sexuales en la que participan menores de edad, que después son colocadas en Internet. Como respuesta a tales conductas o

[200] Vid. Picotti, como en la nota 169, p. 212, donde además se expresa abiertamente con un lenguaje característico de la concepción político-criminal subyacente al llamado Derecho penal del riesgo: «no puede realmente negarse o esconderse la verdadera necesidad de contrarrestar eficazmente -aplicando o, si es necesario, creando normas penales adecuadas- el uso "desviado" de la red, por parte de concretas minorías o grupos, que perjudica la seguridad misma, y en definitiva, limita la posibilidad de mayor difusión y utilización por parte de toda la colectividad».

[201] Además de *infra* nota 203 y texto, cf. al respecto Orts/Roig, como en la nota 26, p. 126 s. Vid. igualmente Morales Prats, "Pornografía infantil e Internet: la respuesta en el Código penal español", *CDJ*, 2000, p. 199.

[202] Para una breve referencia a la acogida de esta orientación en la legislación penal de Inglaterra, Gales, Holanda, Austria, Francia, Estados Unidos, Canada, Australia y algunos países asiáticos, cf. Morales Prats, como en la nota 201, p. 180 s, nota 4.

[203] Al respecto, cf. Díez Ripollés, "Trata de seres humanos y explotación sexual de menores. Exigencias de la Unión y legislación española", *Revista Penal*, 2, 1998, p. 17-22. Vid. también De la Cuesta Arzamendi, "Las nuevas corrientes internacionales en materia de persecución de delitos sexuales a la luz de los documentos de organismos internacionales y europeos", en *Estudios de Derecho judicial*, 21, 1999 (monográfico, Delitos contra la libertad sexual), p. 323 ss.

[204] Parecido, Mata y Martín, como en la nota 69, p. 102 s.

similares, el artículo 189.1 ha criminalizado -con una redacción que resulta demasiado ambigua, tanto por los elementos empleados en la tipificación como por la ambivalencia del contexto criminalizado- por una parte la utilización de menores para tales hechos y por otra el tráfico con las grabaciones. Concretamente, en la letra a) se castiga la utilización de menores o incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, o la financiación de cualquiera de estas actividades[205]. En la letra b), la producción, venta, distribución, difusión o exhibición de material pornográfico[206] en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. El arco punible se extiende, en la misma letra b), a quien facilite estas conductas, y en especial la difusión o exhibición "por cualquier medio", lo que en especial permite incluir en el tipo la difusión o exhibición en la red[207]. Y, en el inciso final del número 1, a la posesión "para la realización de cualquiera de estas conductas" (si bien en este último caso con imposición de la pena -prisión de uno a tres años- en su mitad inferior)[208].

Estas dos variantes de la explotación sexual de menores e incapaces, estan específicamente relacionadas, dependiendo la de la letra b) de la de la letra a)[209]. Desde esta premisa, hay que entender que la modalidad de la letra a) incrimina la utilización misma de menores, siendo, a mi juicio, su libertad sexual lo que se protege. En cambio, en la letra b), aun sin variar el bien jurídico protegido pero sí la inmediatez del ataque, no es la utilización de menores o incapaces lo que directamente se castiga, sino, -como en el inciso final del número 1, que castiga la posesión indicada- actos posteriores a la misma, como la producción[210], venta, distribución o exhibición[211]. Con esta técnica de tipi-

[205] En cuanto al tratamiento de quienes abonan una contraprestación por el acceso al material o representación pornográficos, la doctrina deja fuera los casos de quienes asisten gratuitamente (Muñoz Conde, como en la nota 197, p. 231). A mi juicio, sólo si se tratara de una contraprestación especialmente relevante de manera que individualizadamente la misma adquiere un significado sustancial para la intervención del menor podría considerarse como financiación típica. En otro caso, la contraprestación de entre un grupo indiferenciado y anónimo debe considerarse atípica, acudiendo incluso al principio de insignificancia.

[206] La precisión del artículo 9 (num. 2) del Convenio sobre ciberdelincuencia vinculando la "child pornography" con "pornographic material that vissual depicts" viene a situarse en la línea de identificar material pornográfico con representaciones pornográficas (así ya Díez Ripollés, como en la nota 188, p. 151).

[207] Carmona, en Cobo del Rosal (Dir.), *Compendio de Derecho Penal Español*, 2000, Madrid-Barcelona: Marcial Pons, p. 249.

[208] Este afán punitivo (Muñoz Conde, como en la nota 197, p. 229) no tiene que ser acentuado por el aplicador del Derecho, que debe limitarse a las reglas de imputación de un Estado de Derecho y estas no creo que obliguen a interpretar el precepto como un delito de sospecha, por más que «siempre será difícil probar cuándo la posesión del material pornográfico está destinada a las conductas de producción, venta, difusión o exhibición» (Muñoz Conde, como en la nota 197, p. 230).

[209] Respecto del tratamiento de los casos contemplados en la letra b) antes de la reforma se entiende que se resolvían a las formas de intervención del artículo 28, en relación con las previsión de la actual letra a). Por todos, Muñoz Conde, como en la nota 197, p. 229. Partidario de que el Código de 1995 lo hubiera incorporado, Gimbernat, como en la nota 189.

[210] Tiene razón Mata y Martín, como en la nota 69, p. 115 en que la producción no es posterior a la elaboración del material, pero creo que sí lo es (a lo más, en algunos casos, y precisamente los más avanzados tecnológicamente, podrá ser coetáneo) a la utilización del menor que (con la finalidad descrita) es realmente lo que se castiga en la modalidad de la letra a), en la que por cierto, contra lo que cree el citado autor (ibídem, nota 210), no se castiga "elaborar", lo que, a mi juicio, sólo constituye uno de los elementos tendenciales típicos de la conducta punible.

ficación, cuyo empleo se ha agudizado en el "moderno" Derecho penal, se acentúa el propósito de cerrar toda laguna de punibilidad[212], desplazando la barrera de lo punible para cubrir toda la *cadena criminal*, aunque en este caso tiene específicamente por objeto cortar tanto las fuentes de aprovisionamiento como las de difusión y reciclaje y en algún caso a la demanda o consumo mismo del producto ilícito[213] -que, en cualquier caso, aquí es impune-, y al mismo tiempo respondiendo de forma indiferenciada a lo largo de la cadena, esto es, independiente de las formas de aparición del delito.

E). Las figuras contempladas en el primer número del artículo 189 son merecedoras de algunas consideraciones particulares enfocadas desde la perspectiva de la utilización de tecnologías de la información o de la comunicación[214], que de todos modos, en general afecta, y sobre todo por lo que respecta a Internet, al Título VIII en la medida en que se relativiza todavía más la significación de lo pornográfico[215] e incluso de lo sexual. Aparte de esto, cabe empezar indicando que en el supuesto de que se lleve a cabo una retransmisión del espectáculo en que se utiliza a menores o incapaces "en directo" por cualquier red, sin que se llegue a confeccionar material pornográfico, quedaría incluido directamente en la letra a). Quien, a partir de esa retransmisión, grabe la representación y a continuación difunda lo grabado (o, en base al inciso final, el que disponga de la grabación con el propósito de difundirla) será, en cambio, castigado en base a lo previsto en la letra b)[216].

En cuanto al tratamiento de los casos de "pornografía infantil *virtual*", a mi juicio, no puede ser otro que la irrelevancia con relación al art. 189.1.b. Primero -lo que ya de por sí sería suficiente-, por razones de legalidad penal, pues el precepto comentado presupone literalmente que los materiales (es decir, representaciones) pornográficos han sido elaborados utilizando menores o incapa-

[211] Se trata estructuralmente de un supuesto semejante al delito de receptación (Gimbernat, como en la nota 189, invocando que ataca el mismo bien jurídico que el delincuente originario, pues perpetúa y agudiza la situación creada por el ladrón, y razones de prevención general ya que el perista supone un estímulo para que se cometan delitos contra la propiedad: muchos robos de joyas no se cometerían si el autor no contara con que "a posteriori" iba a encontrar una persona que diera salida a las alhajas sutraídas. De la misma manera el adquirente que pasa en el video las imágenes reproducidas perpetúa el ataque a la libertad y a la dignidad de los niños previamente grabados y contribuye al mantenimiento y expansión de una degradante industria. Gimbernat destaca que la singularidad de este tipo frente a casos como la adquisición de droga para el consumo propio, en tanto que aquí el titular del bien jurídico no es el adquirente, sino el menor y que comparados con la receptación son hechos más graves).

[212] En particular este «afán» se advertiría en el artículo 189, 3. Así Muñoz Conde, como en la nota 197, p. 232.

[213] Sobre esto, cf. Orts/Roig, como en la nota 26, p. 134. Véase *supra* nota 211.

[214] En cuanto a las previsiones de los números 4 y 5 no suponen, en principio, problemas específicos, desde la perspectiva indicada. En cuanto a la controvertida "corrupción de menores" del número 3, a mi juicio, constituye sólo un tipo residual reconducible también en cuanto al bien jurídico protegido a la libertad sexual y pensado para hechos de menor entidad que los previstos en el resto de preceptos del Título VIII que supongan una implicación personal de menores, y que de alguna manera tratan de neutralizar el valor de criterios habituales de imputación como la insignificancia o la adecuación social, si bien subordina esa neutralización a un juicio que, fundamentalmente, es de carácter valorativo y de pronóstico, sobre la dañosidad de tales hechos en orden a la evolución o desarrollo de la personalidad del menor.

[215] Cf. Muñoz Conde, como en la nota 197, p. 227.

[216] La misma solución para los dos supuestos en Orts/Roig, como en la nota 26, p. 130, que por otra parte entienden que la letra a) presupone el trato directo con los menores o incapaces.

ces, sin que el desconocimiento que admite el texto legal alcance más que al origen geográfico. En mi opinión, dada la dependencia de la letra b) con la letra a), esto vale tanto para el supuesto de que los materiales hayan sido elaborados con hipostasía del menor o de los menores por mayores[217], como para el caso de que sea la real actividad sexual del menor la que es hipostasiada mediante imágenes manipuladas o meramente digitales, pues en tal caso no se habría *utilizado* "a menores" como exige la letra a), sino sólo sus imágenes[218].

Para reforzar esta interpretación se podría acudir también al bien jurídico protegido, que, en mi opinión, como se indicó, no es otro que la libertad sexual, aunque indirectamente este bien jurídico pueda, sobre todo en el caso de menores, estar especialmente vinculado a la dignidad (a la llamada indemnidad o a la intimidad). De manera que si, en cambio, se quiere poner por delante del significado sexual la dignidad o la intimidad[219] se corre el riesgo de abarcar dentro del Título VIII a hechos cuya punición puede o debe ser planteada en otro contexto. De todos modos, no es necesario acudir a este argumento a la vista de que el texto legal exige la utilización de menores, cosa que además deberá ser acreditada, por lo que la imposibilidad técnica en muchos casos de distinguir la participación real del menor de su participación virtual no es, a mi juicio, razón suficiente para resolver en el sentido de su punición los supuestos de "pseudopornografía"[220]. Esto puede parecer insatisfactorio, pero creo que viene impuesto por el texto legal y por la necesidad de seguir reconociendo el alcance de la "imputatio facti". Respecto del alcance de la letra b) número 1 Orts/Roig[221] -que entienden que se protegen varios bienes jurídicos, cuales son los adecuados procesos de formación de unos y otros y su intimidad- incluso van más lejos y requieren que el papel desempeñado por los menores o incapaces en la cinta sea significativo, no bastando su aparición ocasional en alguna escena o secuencia sin inequívocas implicaciones sexuales y concluyen que el intercalado de imágenes de menores entre otras explícitamente eróticas no convierte sin más en pornografía infantil el producto así pergeñado.

En cuanto al tratamiento de los supuestos en que no sólo se utiliza al menor con los propósitos indicados, sino que el mismo sujeto produce, vende y/o distribuye, los materiales pornográficos, la solución debe ser el concurso de leyes, que a mi juicio constituye en un Estado de Derecho el sistema normal, aunque no único, para resolver los concursos, sobre todo si hay dudas, provocadas

[217] La impunidad de estos supuestos es reconocida con carácter general: Morales Prats/García Albero, como en la nota 189, p. 926; Orts/Roig, como en la nota 26, p. 133, que extienden la solución a los casos en que se trate de menores que lo sean conforme a nuestra legislación pero no conforme a la del país de origen.

[218] Requieren también una «intervención real de un menor», Orts/Roig, como en la nota 26, p. 133 (véase asimismo *supra* nota 216).

[219] Orts/Alonso, como en la nota 189, p. 51, creen que en el caso de la letra b) no es posible entender que el bien jurídico fuera la libertad sexual del menor o su indemnidad sexual, pues esto obligaría a considerar que estamos ante un delito de peligro abstracto, cuyo contenido de injusto sería tan remoto respecto de aquél, basado sólo en el eventual mantenimiento o incremento de la demanda del material sexual con menores, lo que supondría un intolerable adelantamiento de las barreras del Derecho penal. Todo ello les lleva a considerar que el bien jurídico protegido es la intimidad del menor (coincide en esto, Tamarit, como en la nota 187, p. 124 ss).

[220] A favor de la punición de estos supuestos Morales Prats/García Albero, como en la nota 189, p. 926.

[221] Como en la nota 26, p. 133.

fundamentalmente por el empeño del legislador de acoger nuevas figuras «cuyos ilícitos no aportan al elenco de delitos más que casuismo»[222].

F). En rigor, la consideración del Derecho penal sexual desde el punto de vista de las TIC, habría de ser más completa, pues, aunque hay delitos sexuales que cuya realización por Internet es inimaginable[223], cabe contemplar el recurso a las mismas con relación a otras figuras del Título VIII, como el acoso sexual, si bien será difícil, cuando no imposible, incriminar por tal título cuando la conducta se realice exclusivamente por aquel medio, ya que si bien es verosímil que la solicitud de favor sexual se haga, por ejemplo, por correo electrónico, el resto de elementos típicos requeridos por el artículo 184 imponen un contexto de interacción personal inmediata entre el solicitante y la víctima que no se daría en las comunicaciones de este tipo. Así que la virtualidad de la informática en este caso sólo tendría relevancia penal como coadyuvante (por ejemplo, como medio para provocar una situación objetiva y gravemente intimidatoria, hostil o humillante) de un contexto más amplio. En fin, la mera petición de tales favores por correo electrónico (que desde luego tendría que estar dirigida a persona específica) sin concurrir la relación típica (laboral, docente o de prestación de servicios, continuada y habitual) no podría integrar el delito del art. 184[224].

G). Entre los delitos de exhibicionismo y provocación sexual del capítulo IV, la modalidad de exhibicionismo se contempla en el artículo 185 que exige que la exhibición propia o de tercero inducida, además de obscena, se realice *ante* menores de edad o incapaces, esto es, "en vivo"[225], con lo que quedaría fuera de su círculo el supuesto en que la ejecución de la exhibición se hace por ejemplo vía Internet[226]. Por el contrario, Mata y Martín[227] cree posible la aplicación del art. 185, invocando que la exigencia de que los hechos deban realizarse ante el menor, en el sentido de una presencia física directa de los sujetos, no aparece en el texto y no se desprende del fin de tutela perseguido por esta norma. Estoy convencido de que acentuando la significación del tipo subjetivo, que no sería otro que el propósito del autor de involucrar a la víctima con su acción en un contexto sexual[228], se puede considerar que el delito de exhibicionismo es en realidad un acto preparatorio de una de las modalidades precedentes contra la libertad sexual de menores. Esto, a mi juicio, por otra parte, dificulta la consideración en el ámbito del artículo 185 de actuaciones no presenciales como las indicadas.

H). La variante "provocadora" vendría dada por la tipificación en el artículo 186, de la venta, difusión o exhibición de material pornográfico, cuya descripción contiene dos requerimientos que circunscriben las conductas punibles y que dificultan su aplicación a hechos vinculados con el contexto tecnológico apuntado. De un lado, el medio de venta, difusión o exhibición debe ser *directo*, lo que se entiende como dirigido a víctimas concretas o concretables[229], o que estén físicamente presentes[230], excluyéndose las labores de edición, impresión, grabación o análogas y cualquier clase de publicación de material (en soporte informático, en un CDRom o en la red) que no llegue al contacto directo con menores o incapaces[231]. Y, de otro, que tales conductas deben llevarse a cabo *entre menores o incapaces*. Creo también que el tipo subjetivo -esto es la tendencia lasciva, en última instancia provocadora en el sentido de dirigida a involucrar al menor o incapaz en un contexto sexual-, podría reforzar aquella conclusión.

I). En cuanto a los delitos relativos a la prostitución y la corrupción de menores, señalan Orts/Roig que también pueden tener cierta virtualidad los procedimientos informáticos para favorecer la prostitución de menores o incapaces, siempre que se usen intencionadamente para inducir a estas personas al ejercicio de la mencionada actividad, o para promoverla o

[222] Cf. Mapelli Caffarena, "Entre el homicidio y las lesiones", *CDJ*, 1995 (monográfico «Delitos contra la vida e integridad física», Dir. J. L. Díez Ripollés), p. 44. Llegan a la misma solución de castigar por un único delito Orts/Roig, como en la nota 26, p. 138 s.

[223] Orts/Roig, como en la nota 26, p. 124. Fundamentalmente porque presuponen un contacto corporal entre el autor y la víctima.

[224] *Ibídem*, p. 125.

[225] Orts/Alonso, como en la nota 189, p. 44.

[226] Así Orts/Roig, como en la nota 26, p. 124, salvando la eventual aplicación del art. 186 citado.

[227] Como en la nota 69, p. 104.

[228] En este sentido ya Díez Ripollés, 1982, p. 497-501. Le sigue, Muñoz Conde, como en la nota 197, p. 225.

[229] Orts/Roig, como en la nota 26, 125.

[230] Carmona Salgado, como en la nota 207, p. 238

[231] Muñoz Conde, como en la nota 197, p. 227. Parecido, Orts/Alonso, como en la nota 189, p. 44.

fomentarla, captando clientes, etc. E incluso creen que cabe imaginar algún ejemplo rebuscado de utilización de transmisiones electrónicas para hacer participar a un menor o un incapaz en un comportamiento de naturaleza sexual, que sólo podría ser subsumido en el artículo 189.3 haciendo una interpretación muy extensiva del mismo[232].

1.4. Estafa informática y otras defraudaciones

A). Ya en el seno de los delitos patrimoniales, una de las figuras más representativas[233] de la delincuencia que nos ocupa es la *estafa informática* (o "fraude informático"[234]), como la que se enjuició y condenó en la STS 22-9-2000, en que un cliente accedió a la contabilidad de un banco provocando transferencias desde dicho sistema a cuentas distintas. Es perfectamente concebible que tales accesos se lleven a cabo a través de redes[235]. La figura está prevista en el artículo 248, en cuyo número 2 ("también") *se consideran* como reos de estafa a quienes, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida del cualquier activo patrimonial en perjuicio de tercero.

Con ello el Código de 1995 trata de dar respuesta[236] a las dificultades advertidas para castigar estos hechos en base a figuras antes vigentes[237], como el hurto[238], la estafa[239], o, incluso la apropia-

[232] Como en la nota 26, p. 125 s. Véase también *supra* nota 214 y, para referencias sobre la corrupción de menores, nota 189.

[233] Cf. Mata y Martín, como en la nota 69, p. 37, remitiéndose a N. Schmid, *Computer sowie Check- und Kreditkarten- Kriminalität. Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches*, 1994, Zurich, p. 218.

[234] No obstante, apunta un concepto de éste más amplio que abarcaría también defraudaciones informáticas contra intereres macrosociales, Gutiérrez Francés, como en la nota 8, p. 254.

[235] Cf. Gutiérrez Francés, como en la nota 8, p. 264, indicando que estarían cubiertas por el art. 248.2. Vid. asimismo, Choclán Montalvo, "Estafa por computación y criminalidad económica vinculada a la informática", AP, 1997/47, p. 1.081; Herrera Moreno, como en la nota 95, epígrafe VI, D, 1; Moreno Verdejo, en Serrano Butragueño (coord.*), Código Penal de 1995 (Comentarios u jurisprudencia)*, 1999, Granada: Comares, p. 1.247, que habla de piratería informática. Ya antes Romeo Casabona, como en la nota 49, p. 50 s. Orts/Roig, como en la nota 26, p. 68, mencionan conocidos casos al respecto.

[236] Que, en general, la doctrina valora positivamente. Por todos, Suárez González, en Rodríguez Mourullo (Dir.), Jorge Barreiro (coord.), como en la nota 156, p. 710, aunque hubiera preferido una figura independiente. De otra opinión, Gutiérrez Francés, como en la nota 61, p. 264 s, partidaria de una intervención más incisiva o, para ser más exactos, de una auténtica opción criminalizadora, pues, a su juicio, con lo que ahora se tiene no se va más allá de lo que se podía ir con el Código anterior.

[237] Al respecto, ampliamente, por todos, Gutiérrez Francés, como en la nota 41, y Romeo Casabona, como en la nota 49, p. 51-87. Más resumidamente, el mismo "El Derecho Penal y las nuevas tecnologías", *Revista del Foro Canario*, 87, 1993, p. 210-219 (una versión prácticamente igual en lo que concierne a los aspectos patrimoniales fue publicada bajo el título "Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías, en *Poder Judicial*, 31, 1993, p. 163-204). Más recientemente, González Rus, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", *Revista Electrónica de Derecho Penal y Criminología* (http: //criminet.ugr.es/recpc/recpc_01-14.hmtl), p. 17 s; Herrera Moreno, como en la nota 95, epígrafe VI, B).

[238] Cf. la síntesis de Romeo Casabona, como en la nota 237, p. 211 s. Específicamente, Bacigalupo, *Estudios sobre la Parte especial del Derecho penal*, ²1994, Madrid: Akal, p. 197 s, señala que no hay hurto porque la máquina en tanto actúa automáticamente hace lo que su dueño quiere que haga (para otros, en cambio, ese automatismo es demostrativo junto con la manipulación de que no hay consentimiento o voluntad del dueño y por lo tanto base para considerar que hay hurto. Menciona este planteamiento, Conde-Pumpido Ferreiro, *Estafas*, 1997, Valencia: Tirant lo Blanch, p. 214). O, por resultar forzado equiparar las manipulaciones informáticas al apoderamiento característico (así, Orts/Roig, como en la nota

ción indebida[240] o la falsificación de documentos[241], cubriendo la laguna[242] de punibilidad respecto de la que en lo fundamental existía acuerdo tanto en la jurisprudencia como en la doctrina[243], de manera que como señalaba Romeo Casabona[244], la adecuación típica a una de esas modalidades delictivas, en general, no era factible y sólo dándose circunstancias muy contingentes, cuando no

26, p. 62). O, por no existir una cosa mueble en sentido jurídico-penal (específicamente, Gutiérrez Francés, como en la nota 8, p. 256). Véase además *infra* nota 247.

[239] Cf. la síntesis de Romeo Casabona, como en la nota 237, p. 212-215. Asimismo, Gutiérrez Francés, como en la nota 8, p. 257; Mata y Martín, como en la nota 69, p. 38-44. Valle Muñiz/Quintero Olivares, en Quintero (Dir.), como en la nota 107, p. 1.154, indican que se desfiguraría el engaño, convirtiéndolo en un genérico y amorfo mecanismo de lesionar el patrimonio, se renunciaría al error como elemento autónomo y se colmarían las exigencias del ineludible acto de disposición patrimonial mediante la presencia de cualquier respuesta automatizada a la manipulación informática. Específicamente, Conde-Pumpido Ferreiro, como en la nota 238, p. 215 y 217, rechaza la estafa por faltar el acto de disposición (parecido Matellanes Rodríguez, "Algunas notas sobre las formas de delincuencia informática en el Derecho penal" en Diego Díaz-Santos/Sánchez López [coords.], *Hacia un Derecho penal sin fronteras*, Madrid: Colex, 2000, p. 139), pero tilda de sofística la pretensión de excluir, en caso de máquinas, la estafa por faltar engaño o no ser involuntaria la entrega (p. 215 s); o, dado que estos hechos suponen el manejo de sistemas que operan con autonomía, sin intervención de personas físicas, o por lo menos sin intervención inmediata de ellas, «aquí no se engaña a otra persona» (Muñoz Conde, como en la nota 197, p. 406). No obstante, creen que no existen auténticas dificultades porque en última instancia hay un sujeto engañado que es el que está detrás de la máquina, entre otros: Bajo, en Cobo (Dir.), *Comentarios a la Legislación Penal*, tomo V, vol. 2, 1985, p. 1.197, refiriéndose a expendedores automáticos, teléfonos públicos y similares; Conde-Pumpido Ferreiro, como en la nota 238, p. 215, mencionando que la jurisprudencia francesa, desde una perspectiva prioritariamente proteccionista de la víctima, admite la *escroquerie aux appareils automatiques*; Mata y Martín, como en la nota 69, p. 56. Con todo, se estimaban estafas las manipulaciones de datos realizadas antes, durante, o después de la elaboración del programa de manera que los datos quedaran registrados de forma asequible directamente al conocimento del hombre (cf. sólo Corcoy/Joshi, "Delitos contra el patrimonio cometidos por medios informáticos", *RJC*, 1988/3, p. 142) o, dicho de otro modo, cuando el resultado de la manipulación informática es percibido y aprehendido por la persona física, que conoce la significación de los datos alterados, y que ordena una disposición patrimonial lesiva a consecuencia de la falsa representación mental a que se le induce (Gutiérrez Francés, como en la nota 8, p. 266). Véase *infra* nota 243.

[240] Cf. Romeo Casabona, como en la nota 237, p. 215. En la jurisprudencia es destacable la STS 19-4-1991, que resolvió en un caso parecido al citado antes (véase *supra* texto previo a la nota 235), negando la existencia de engaño. Apreció en su lugar apropiación indebida, dado que las alteraciones contables fueron realizadas por un empleado bancario, que consiguió la transferencia a otra cuenta de determinadas cantidades de clientes de la entidad, de las que de esta forma se apodera.

[241] Cf. Romeo Casabona, como en la nota 237, p. 215-217; Gutiérrez Francés, como en la nota 8, p. 257.

[242] Por todos, Calderón/Choclán, *Derecho Penal. Tomo II. Parte especial*, Barcelona, Bosch, p. 819.

[243] No obstante, tras analizar exhaustivamente la cuestión, Gutiérrez Francés, como en la nota 41, p. 336 ss, 341 ss y 409 ss (cf. igualmente, la misma, "En torno a los fraudes informáticos en el Derecho español", *Actualidad Informática Aranzadi*, 11, 1994, p. 7 ss), propugnaba una revisión crítica y actualización del concepto de engaño que, a su juicio, dada la indefinición del legislador, podría abarcar los casos de estafa informática, impugnando además la tesis de que aquí no hay engaño a una persona (todavía cree factible un entendimiento de la estafa que, basándose en una consideración de sus elementos estructurales abierta a reconocimientos ya alcanzados en el resto del ordenamiento jurídico, permitiría abarcar los fraudes informáticos: la misma, como en la nota 61, p. 265-270). En sentido parecido, De la Mata Barranco, "Utilización abusiva de cajeros automáticos: apropiación de dinero mediante la tarjeta sustraida a su titular", *PJ*, Número especial IX (Nuevas formas de delincuencia), 1986, p. 11 y también receptivo, ahora, Mata y Martín, como en la nota 69, p. 41-44.

[244] Como en la nota 238, p. 217.

azarosas, se hacía posible. Ciertamente, la discusión ha perdido trascendencia por la introducción del artículo 248.1[245], pero no es seguro que carezca por completo de interés si se postula dar a dicho precepto un alcance restrictivo que dejaría al margen ciertas operaciones informáticas. En cualquier caso, la opción del legislador habría de ser considerada una elección manifestamente agravatoria[246], sobre todo si se entiende que el parentesco de las estafas informáticas es mayor con el hurto[247], dado que en vez de situar la pena base entre los 6 y los 18 meses, como ocurre en el hurto, se ha optado por el marco punitivo de la estafa que en su base está entre los 6 meses y los 4 años.

B). Aquí lo que interesa más bien es poner de relieve hasta qué punto la técnica de tipificación no ha acentuado injustificadamente los problemas hermenéuticos, en comparación con la modalidad común de la estafa[248]. En el caso del artículo 248.2 la indeterminación es general, aunque se centra en el modo tan abierto en que ha quedado delimitada la acción típica, lo que podría llevar a plantear que habríamos pasado de un delito característico de medios comisivos determinados a uno cuasi-resultativo, con lo que, por cierto, según el criterio dominante, se acentúan la necesidad y posibilidades de recurrir a la teoría de la imputación objetiva. En particular, aquella indefinición se advierte en la expresión "u otro artificio semejante"[249], que, aparte de otras funciones, parece, en principio, configurada con el propósito de *dominar* con el tipo lo que se ha llamado «desarrollo tecnológico vertiginoso»[250], aunque alcanza, como se verá inmediatamente, a otros elementos del tipo.

[245] Conde-Pumpido Ferreiro, como en la nota 238, p. 216.

[246] Cf. Valle/Quintero, como en la nota 239, p. 1.157, subrayando, y avalando, por otra parte, el considerable aumento del rigor punitivo que comporta, con respecto al anterior Código y a otras infracciones patrimoniales, en particular, el hurto, incluso si se comparan sus respectivas agravantes específicas, o la falsificación de documento privado.

[247] Así, para Suárez González, como en la nota 236, p. 710, hay más semejanza con el hurto. El parentesco con el hurto es destacado por Calderón/Choclán, como en la nota 242, p. 819 s, porque en la estafa no sólo se requiere engaño determinante del error, sino que por esta vía, la víctima realice un acto de disposición patrimonial perjudicial, de manera que en el 248 se sustituye el apoderamiento por la manipulación informática. Pero, tiene razón Conde-Pumpido Ferreiro, como en la nota 238, p. 214, cuando afirma que hay casos vinculados con esta figura que no se dirigen a obtener la entrega de una cosa -dinero o mercancía- sino a evitarla, esto es, a disminuir el importe económico de un crédito o el total de la mercancía a entregar o el importe de una suma a pagar, con lo que no se produce una sustracción, sino un fraude.

[248] Cuya ambigüedad no es desconocida. Sobre ello, por todos, Muñoz Conde, como en la nota 197, p. 406 s.

[249] Suárez González, como en la nota 236, p. 711. Para algún autor la indefinición llegaría al extremo que lo mejor sería tener la cláusula por no puesta. Así, Queralt, *Derecho Penal español, Delitos contra los intereses individuales colectivos*, ^{3}1996, Barcelona: Bosch, p. 391.

[250] Valle/Quintero, como en la nota 239, p. 1.155. No obstante, la expresión parece tener su origen en el Informe del Consejo General del Poder Judicial emitido sobre el Anteproyecto de 1994 y estaría pensada para abarcar las manipulaciones de máquinas automáticas que suministran bebidas, billetes de transporte, o de cabinas y otros teléfonos públicos (cf. Choclán, *El delito de estafa*, 2000, Madrid: Bosch, p. 302 ss).

Estas fórmulas suelen considerarse inevitables[251], pero es dudoso que, al menos en este caso, no se hubieran podido suavizar los costes que implican en seguridad jurídica, pues la indefinición de la fórmula se acentúa en la medida en que la acción típica de referencia no es menos ambigua y polisémica. Así ocurre, en efecto, con el primer descriptor de la conducta típica (que en principio puede referirse al manejo manual, al control, o a la operación sobre algo desvirtuando su auténtico sentido de forma hábil e interesada: algo que aunque de modo muy difuso conlleva, de todos modos, más que una mera alteración), lo que además se resalta con el indefinido: "alguna manipulación". La evidencia de que el legislador opta por un lenguaje difuso[252] se recalca con la expresión "valerse de", que no deja de ser un circunloquio impropio de la gramática penal.

En esas condiciones, creo[253] que la opción técnica por una mayor concreción típica, como la que sigue el § 263 StGB[254], junto con la cláusula mencionada, resulta menos costosa sin dejar de abrirse al futuro, en la medida en que por lo menos se tiene algo más tangible con lo que establecer la relación de semejanza, aunque pueda comportar otros efectos secundarios[255].

Por otro lado, pese a la indeterminación, en la medida en que el descriptor conlleva una acción claramente positiva (incluso en el caso de valerse de artificio semejante), parece difícil[256] fundamentar la comisión por omisión hasta en los casos excepcionales en que se admite para la estafa común, esto es, según el punto de vista dominante, cuando la omisión va acompañada de actos positivos *concluyentes*[257]. Tiene razón, no obstante, Mata y Martín[258], al observar que, si se admite que también hay manipulación cuando se dejan de incluir datos que debieran haber sido procesados[259], se están abarcando ya formas omisivas. A mi juicio, aparte del inconveniente lingüístico referido, una asunción consecuente del art. 11, que mire particularmente al principio de proporcionalidad, como la que plantean entre otros Gimbernat Ordeig o Gracia Martín, debe conducir necesariamente una solución restrictiva, que además no puede conformarse con la idoneidad *ex ante* de la infracción de deber respecto del resultado, sino que demanda una comprobación *ex post* atendiendo particularmente a las circunstancias concurrentes.

[251] Específicamente respecto del caso de la estafa informática, Valle/Quintero, como en la nota 239, p. 1.155. Sobre ello cf. asimismo González Rus, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", *Revista Electrónica de Derecho Penal y Criminología* (http: //criminet.ugr.es/recpc/recpc_01-14.hmtl), p. 17 s.

[252] Dicen Valle/Quintero, como en la nota 239, p. 1.155: se «define la acción típica de forma conscientemente indeterminada».

[253] De otra opinión, Valle/Quintero, como en la nota 239, p. 1.155 respecto del precepto alemán (parecido Herrera Moreno, como en la nota 95, epígrafe VI, D) y González Rus, respecto de la fórmula planteada por el Proyecto español de 1992.

[254] No obstante, la doctrina alemana se ha pronunciado críticamente respecto de dicho parágrafo por las insuficiencias que plantea su redacción desde el punto de vista de las garantías que comporta el principio de legalidad: así Carsten, "Computerbetrug (§ 263 StGB)", en *Internet-Zeitschrift für Informatik* (http: www.jurpc.de/aufsotz), p. 12; Kindhäuser, "Der Computerbetrug (§ 263 StGB) – Ein Betrug?", *Gerald Grünwald-FS*, 1999, Baden-Baden, p. 285.

[255] Para consideraciones valorativas sobre las distintas posibilidades de tipificación, cf., sintético, Romeo Casabona, como en la nota 255, p. 189-191. Más ampliamente, el mismo, como en la nota 49, p. 89-118 mencionando el de que el uso de elementos normativos con alto grado de dependencia del mundo de la informática dificultaría la tarea del intérprete.

[256] A favor, aunque consciente de las dificultades que plantea el término "manipulación" y de la necesidad de requerimientos adicionales, Herrera, como en la nota 95, epígrafe VI, D, 1.

[257] Valle/Quintero, como en la nota 239, p. 1.156.

[258] Como en la nota 69, p. 54 s, precisando que en otras legislaciones se prevén conductas omisivas.

[259] Cf. Choclán, como en la nota 235, p. 1.080. En principio, conforme, Herrera, como en la nota 95, epígrafe V, D, 1, a.

C). De todas formas, las consecuencias de estos defectos -que no son simplemente "errores" técnicos, sino que, al menos, aparecen, como efectos secundarios de una política-criminal expansionista y flexibilizadora de los presupuestos de la responsabilidad criminal-, quizás puedan verse en parte aliviadas, mediante pautas interpretativas relativamente plausibles, aunque no concluyentes, para definir y delimitar el alcance del tipo. Pero también, a mi juicio, podrán orientar al juez en la individalización del amplio margen de determinación de pena, que como se dijo, en el tipo básico, va de los 6 meses a los 4 años, sin que en mi opinión tal opción se vea comprometida por la necesidad de atender a la regla específica de determinación de pena del artículo 249 que, junto al importe de lo defraudado, al quebranto económico y las relaciones entre el perjudicado y el defraudador, sino que se abre a otras consideraciones compatibles con aquellas orientaciones, al referirse a "los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción".

Una de esas pautas se apoya, de forma algo paradójica, en la eventualidad de ese propósito algo pretencioso del legislador de anticiparse al mañana[260]. Atendiendo al mismo, cabe entender que -como la manipulación informática- el artificio debe referirse a tecnologías avanzadas y, por lo tanto -lo que también valdría para la manipulación informática-, por echar mano de una recurrencia habitual en la doctrina y en la jurisprudencia, habrían de ser "sofisticados"[261], eufemismo que debe ser entendido no de manera que el avance tecnológico sea criminalizado, sino en el sentido de que tal "complejidad" en el caso concreto comporta circunstancias susceptibles de ser imputadas al sujeto que hagan merecedor al hecho del reproche penal propio de la manipulación informática -y, en últimas instancia, de la estafa-. Bajo tal premisa, ese nexo teleológico podría dejar fuera, al menos a priori, lo que podríamos llamar "manipulaciones convencionales", que, por ello, carecerían de la semejanza típica necesaria[262].

En tal caso, además, la discusión sobre particularidades de lo que deba entenderse por manipulación informática adquiere sentido y valor, aunque su ambivalencia y la infinidad de procedimientos informáticos manipuladores que la realidad ofrece[263] constituyan una barrera difícilmente franqueable para la delimitación de estas previsiones típicas.

Al respecto, recuperando una observación ya realizada, debe quedar claro que la "manipulación" no implica una simple alteración de datos o funciones informáticas, sino que conlleva algo

[260] Esta es la función que parece atribuirle Gutiérrez Francés, como en la nota 8, p. 264. Al desfase que los avances tecnológicos pueden dar lugar respecto de las previsiones penales cuando en sustitución del modelo de la ley penal en blanco, se emplean modelos de tipificación exhaustivos, por ejemplo para describir el objeto material del delito, como el utilizado en los delitos contra la propiedad industrial, se refiere Bajo en el "Prólogo" a Bajo/Bacigalupo (Silvina), *Derecho penal económico*, 2001, Madrid: Centro de Estudios Ramón Areces, S.A., p. XXVI s, considerando impropio de la legislación penal este detallismo y perturbadores y grotescos los resultados a que así se llega.

[261] O también se habla de operaciones de "ingeniería informática" (así, Bermúdez Ochoa citado por Moreno Verdejo, como en la nota 235, p. 1.247).

[262] Creo que en la SAP Madrid 24-1-1999 se viene a adoptar este punto de vista. En cambio, a mi juicio, en la dirección contraria, la SAP Lugo 9-7-1998. Resalta la importancia de la exigencia de una relación de semejanza entre los artificios y las manipulaciones Mata y Martín, como en la nota 69, p. 48 s.

[263] Por todos, ya Camacho Losa, *El delito informático*, 1987, Madrid, p. 32.

más, una actividad modificativa mendaz o subrepticia, una "utilización irregular" de un sistema informático, de sus presupuestos básicos o de las órdenes que recibe de modo que produzca resultados no previstos o que de conocerlos no se habrían autorizados[264].

Por otra parte, la doctrina se ha esforzado en identificar, a la vista del funcionamiento general de los sistemas informáticos, la operatividad de la manipulación típica[265]. En general, se han impuesto síntesis indicativas de que al no especificarse la tipología de maniobras informáticas, éstas comprenderían cualquier modificación del resultado de un proceso automatizado de datos, mediante la alteración de los datos que se introducen o de los ya contenidos en el ordenador, en cualquiera de las fases de su procesamiento o tratamiento informático[266]. O, dicho de otro modo, tanto las manipulaciones en la fase "in put", en el programa o en el "out put"[267]. Esto es, quedarían abarcadas[268] tanto la manipulación que afectara al programa, ya se lleve a cabo previamente durante la elaboración del programa, ya con posterioridad durante su ejecución, como la manipulación en la ejecución mecánica del programa, es decir, del procesamiento o tratamiento automatizado de datos[269], incluido el falseamiento o manipulación del resultado inicialmente correcto[270], es decir, incidiendo inmediatamente en el resultado[271], siempre y cuando no se produzca antes de la fase de entrada de los datos o después de la salida de los mismos[272]. Se ha afirmado que tampoco pueden quedar abarcadas aquellas conductas en las que el medio informático o telemático es meramente circunstancial o dicho de otro modo en que concurre una operación informática, pero no hay manipulación[273].

[264] Cf. Conde-Pumpido, como en la nota 238, p. 218 s, quien además cree que sólo dando al término manipulación un sentido amplio puede abarcarse la actividad de quien es el usuario habitual del sistema informático.

[265] Cf. Conde-Pumpido, como en la nota 238, p. 218-220.

[266] Orts/Roig, como en la nota 26, p. 64, siguiendo a Romeo Casabona, como en la nota 49, que más precisamente la expresión "*incorrecta* modificación".

[267] Cf. ya Romeo, como en la nota 49, p. 46-48. Más recientemente, Conde-Pumpido, como en la nota 238, p. 218-220; Gutiérrez Francés, como en la nota 8, p. 264. Suárez González, como en la nota 236, p. 711, entiende que las cometidas "fuera del sistema" pueden considerarse genuinas modalidades de estafa.

[268] Orts/Roig, como en la nota 26, p. 64. Sobre estas distinciones, cf. Choclán Montalvo, "Estafa por computación y criminalidad informática vinculada a la económica", *AP*, 1997, p. 1.082; Corcoy/Joshi, "Delitos contra el patrimonio cometidos por medios informáticos", *RJC*, 1988/3, p. 135 ss; Mata y Martín, como en la nota 69, p. 47-55; Pica, *Diritto penale delle tecnologie informatiche*, 1999, Turín: Utet, p. 145 ss. Para otras distinciones relacionadas con el lugar y el protagonista de la manipulación cf. Mata y Martín, como en la nota 69, p. 51 s, remitiéndose a N. Schmid [véase nota 233], p. 240 ss.

[269] Aquí entrarían los casos enjuiciados en la SAP Granada 23-3-1999 y en la STS 30-10-1998.

[270] Sieber, 1992; Moreno Verdejo, como en la nota 235, p. 1.247; Orts/Roig, como en la nota 26, p. 64.

[271] Mata y Martín, como en la nota 69, p. 51 se refiere al respecto a manipulaciones en el reflejo último de la visualización por pantalla, en la impresión en papel o en el registro en banda magnética cuando van a ser transmitidos a otros ordenadores.

[272] Mata y Martín, como en la nota 69, p. 51, siguiendo a N. Schmid, [véase nota 233], p. 227.

[273] Mata y Martín, como en la nota 69, p. 55.

Pérez Manzano[274] propone circunscribir las manipulaciones informáticas a las alteraciones del software. Ciertamente, eso dejaría fuera del concepto de "alguna manipulación informática" a otras comúnmente aceptadas como estafas informáticas, en que la alteración afecta a los datos sobre los que opera el sistema e incluso sobre los elementos materiales del mismo[275] -sin perjuicio de que pudiera calificarse de "otro artificio semejante", para lo que no cabe una respuesta dada de antemano por la semejanza general del proceso planteado, sino que hay que estar a circunstancias concretas de ese proceso-. Por otra parte, en el Derecho inglés Schmit & Hogan[276] plantean restringir el término "informática" de manera que quede vinculado con tres propiedades como guardar, recuperar y procesar información, evitando incluir manipulaciones de máquinas que tienen algunos componentes informáticos pero que no son capaces de realizar aquellas funciones.

En cualquier caso, estas orientaciones son suficientemente ilustrativas de que soluciones apriorísticas que coloquen dentro o fuera del tipo determinadas operaciones informáticas no pueden ser absolutamente concluyentes. Y de que, en última instancia, para cumplimentar la racionalidad jurídica de la ampliación del ámbito de lo penalmente prohibido en las estafas informáticas y eliminar los atisbos de arbitrariedad, hay que profundizar en aquellos aspectos de la dimensión informática que la hacen equiparable en términos de desvalor a los que fundamentan la severa punición de la estafa, en especial en la condición de engaño bastante y su vínculo con el perjuicio penalmente relevante y tratar de traducirlos a las reglas y presupuestos generales de imputación, de conformidad con lo que el tipo legal establece. Lo mismo ha de servir respecto de esos otros artificios semejantes. No obstante, las bases de ese desvalor (si el mayor peligro para el bien jurídico, si la mayor insidiosidad por la facilidad de la comisión y la desprotección de las eventuales víctimas, que además podrían aumentar, ...) no son seguras, pese a que un fundamento cualificador está claro. Por otra parte, si, como subraya la doctrina, en la estafa informática, la manipulación informática habría sustituido al engaño y al error de la estafa genérica[277], por la indefinición reseñada, habríamos pasado, como quedó antes reflejado, de un delito tan característico de medios comisivos determinados a uno cuasi-resultativo. Esto dificulta la identificación de ese fundamento material. Con todo, Valle/Quintero[278], a partir de la referencia a la transferencia no consentida de cualquier activo patrimonial, ofrecen una solvente restricción, que pone el énfasis más en la vinculación con el bien jurídico tutelado que en la identificación de las clases de manipulación informática típicamente adecuadas, y que en síntesis abunda en que sólo las manipulaciones informáticas que tengan por objeto -y sean adecuadas para- alcanzar una transferencia no consentida de activos patrimoniales suponen un riesgo intolerable para el patrimonio objeto de protección[279]. Y, a tal efecto, se indica que el tipo consumado no podrá eludir las exigencias de la relación de causalidad e imputación

[274] En Bajo (Dir.), *Compendio de Derecho Penal (Parte Especial)*, volumen II, 1998, Madrid: Ceura, p. 455, si bien, como destaca Mata y Martín, como en la nota 69, p. 48, en realidad luego termina aceptando el concepto propuesto por Romeo (véase supra).

[275] Mata y Martín, como en la nota 69, p. 49.

[276] Como en la nota 182, p. 708.

[277] Por todos, Orts/Roig, como en la nota 26, p. 63 s.

[278] Como en la nota 239, p. 1.155 s.

[279] Conforme con ello, Orts/Roig, como en la nota 26, p. 69.

objetiva del resultado[280]. La referencia citada se comportaría entonces como un elemento de enlace con el resultado (que no es otro que el perjuicio patrimonio de otro), que deja fuera del tipo las maniobras realizadas a través de ordenadores que no generen riesgos no permitidos de lesión patrimonial[281].

En cualquier caso, el tipo exige que se trate de una "transferencia no consentida", de manera que si concurriera la anuencia del sujeto pasivo el hecho sería atípico[282].

Por otra parte, la referencia a los activos patrimoniales permite una mayor espiritualización del suceso típico y una mejor cobertura típica de modernas operaciones financieras, ya que el desplazamiento que comporta la transferencia puede referirse a valores patrimoniales sin correspondencia con un objeto material[283], esto es, a valores meramente contables. Por otra parte, la mayoría de la doctrina considera que la transferencia abarca tanto la transmisión de bienes como la prestación de servicios[284].

D). Como en la común, para que se dé la estafa informática es preciso que haya un resultado consistente en un perjuicio patrimonial de otro, lo que habrá de entenderse como disminución del patrimonio, según comparación de la situación del sujeto activo antes y después del acto de disposición (STS 27-1-1999)[285]. En el Derecho español no basta, ni un relevante peligro para el patrimonio del sujeto activo, ni tampoco el beneficio de alguien siendo preciso un menoscabo patrimonial efectivo, ni siquiera la transferencia no consentida del activo patrimonial, de forma que si sólo estuvieramos ante una anotación contable únicamente cabría invocar la tentativa[286]. No es preciso, no obstante, que el beneficiario reciba materialmente nada, como ocurre cuando se salda una deuda[287], caso en que se produce un incremento patrimonial y el perjuicio consiguiente[288].

En todo caso, el perjuicio debe estar vinculado con una transferencia no consentida de activos patrimoniales, resultante de las manipulaciones informáticas o artificios semejantes antes contem-

[280] Valle/Quintero, como en la nota 239, p. 1.156.

[281] De todos modos, véase *infra*, apartado D (párrafo correspondiente a la nota 289).

[282] Para Suárez González, como en la nota 236, p. 711, la exigencia de que la transferencia no sea consentida es superflua.

[283] Cf. Choclán Montalvo, como en la nota 235, p. 1.083; Conde-Pumpido Ferreiro, como en la nota 238, p. 222.

[284] Pérez Manzano, como en la nota 274, p. 456 s. Le parece dudoso a Mata y Martín, como en la nota 69, p. 53, puesto que la fórmula legal española no parece que incluya actividades humanas, aun siendo económicamente evaluables, sino directa y exclusivamente elementos patrimoniales (remitiéndose para un análisis más detallado a N. Schmid, [véase nota 233], p. 245).

[285] Conforme, Orts/Roig, como en la nota 26, p. 69, matizando que la salvedad apreciada por Vives Antón/González Cussac, en Vives (Coord.), *Comentarios al Código Penal de 1995*, volumen I, 1996, Valencia: Tirant lo Blanch, p. 1.230 s, tratando de salvaguardar la diferencia entre el perjuicio típico -que sería la diferencia de valor entre lo que se atribuye a otro en virtud del acto de disposición y lo que eventualmente se recibe de éste como contraprestación- y el perjuicio civilmente indemnizable para los supuestos tratados escasa importancia.

[286] En dicho sentido, aunque refiriéndose siempre al incremento patrimonial del sujeto activo, Mata y Martín, como en la nota 69, p. 53 s (remitiéndose a Pica [*supra* nota 268], p. 148 y ss, respecto del Código penal italiano que exige la consumación de la realización del enriquecimiento injusto), pese a ser consciente de que el Código sólo exige el perjuicio.

[287] Orts/Roig, como en la nota 26, p. 68 s. En contra, Herrera, como en la nota 95, epígrafe VI, D, 3.

[288] Cf. Mata y Martín, como en la nota 69, p. 53.

pladas. En relación con ello, una aplicación consecuente de la teoría de la imputación objetiva, permitiría, valorando no sólo la perspectiva *ex ante* mencionada más arriba, sino también la perspectiva *ex post*, la concreción de si el perjuicio patrimonial se corresponde efectivamente o no con con los riesgos típicos mencionados, y si aquél está o no dentro del alcance del tipo. En este sentido, la intermediación entre la manipulación informática y el perjuicio patrimonial de intervenciones humanas puede llegar a excluir la aplicación del precepto[289].

E). En cuanto al tipo subjetivo, se trata de un tipo doloso en el que concurre un elemento subjetivo específico como es el ánimo de lucro, lo que a juicio del TS (S 2-4-1998) supone la «intención de enriquecimiento a costa del empobrecimiento de la víctima». Ello se entiende que conlleva una exigencia implícita de dolo directo, que se traduce específicamente en que no hay tal cuando el objetivo del autor no sea conseguir la cantidad "estafada", obtenida en el desarrollo de operaciones informáticas realizadas con otro propósito.

F). Las peculiaridades de los requisitos de imputación de esta estafa, que la convierten al menos formalmente en una estafa específica, junto con el hecho de que su semejanza material con el hurto no pueda ocultarse, llevan a plantearse si su consideración legal como estafa supone una remisión punitiva *in totum* no sólo a la regla punitiva básica, sino al resto de prescripciones penológicas, que presentan peculiaridades notables, como es el hecho, a mi juicio más significativo para el problema planteado, de que la individualización de la pena cuenta con una regla inusual como es la de que se tenga en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción. La opinión dominante es que son de aplicación a la estafa informática los artículos 249 (que, como se indicó, establece un sistema de individualización de la pena singularizado) y 250 (que contempla agravaciones específicas)[290], aunque en alguna ocasión se haya añadido la lógica salvedad de que la textura de aquellas circunstancias sea compatible con las manipulaciones informáticas[291]. Por otra parte, siendo consecuente con la exigencia de que la acción y el resultado deben estar unidos por un nexo que viene determinado por la causalidad y la imputación objetiva, los perjuicios patrimoniales que no respondan a ese nexo no podrán ser tomados en cuenta a los efectos previstos en el artículo 249, aunque el mismo hable no de perjuicio sino de quebranto económico, de manera que los perjuicios patrimoniales que en términos jurídico-penales no sean objetivamente-imputables no sólo no pueden computarse para la decisión sobre la tipicidad. Tampoco para determinar cualquier incremento punitivo, sea para individualizar la pena, sea cambiando el título de imputación de falta a delito[292/293].

[289] Admite excepciones, Mata y Martín, como en la nota 69, p. 54.

[290] Implícitamente, Orts/Roig, como en la nota 26, p. 71; Valle/Quintero, como en la nota 239, p. 1.154 y 1.156.

[291] Valle/Quintero, como en la nota 239, p. 1.156.

[292] Queralt, como en la nota 249, p. 392, entiende que la autonomía de la estafa informática (véase *infra* el apartado siguiente) comporta la impunidad de este fraude informático cuando la cuantía es inferior a las cincuente mil pesetas.

[293] A las consideraciones penológicas precedentes habría que añadir cómo, dadas las características de los delitos infomático-cibernéticos, con frecuencia, los perjudicados serán múltiples y, por lo tanto, habrá lugar a aplicar las previsiones del art. 74.2 del CP (cf. Herrera, como en la nota 95, epígrafe VI, D).

G). Tras las consideraciones precedentes se vislumbra claramente que la mayor parte de los problemas indicados dependen en una medida significativa de la discusión sobre la naturaleza de la figura y sus relaciones con la estafa común[294]. Vives/González Cussac[295] creen que no hay sino una modalidad de estafa con idéntica estructura a la común, aunque falten el engaño y el error. La mayoría, no obstante, se debate -sin que las posiciones estén definidas con claridad meridiana[296]- entre quienes defienden que es una estafa específica con particularidades destacadas[297] y quienes le niegan su condición de estafa le atribuyen una naturaleza autónoma[298]. De todos modos, a mi juicio, no hay que exagerar el valor de este debate, de manera que, por ejemplo, la mayor parte de las restricciones planteadas se pueden alcanzar cualquiera de sea la solución elegida de las tres indicadas. De igual manera, tampoco creo que la compleja cuestión en torno al bien jurídico protegido[299] resulte decisiva en términos generales con relación a las cuestiones concursales y, en especial, respecto de las falsificaciones documentales. Aunque una respuesta concluyente sobre tal menester debería ser provisional, por la versatilidad de estos ataques informáticos, mi impresión es que las relaciones entre las estafas informáticas y las falsedades documentales no dependen tanto de los bienes jurídicos protegidos que, en efecto, serán normalmente diversos aunque no carentes de nexos estrechos, como del modelo de ataque, en el sentido de que, generalmente, las defraudaciones informáticas contempladas en el artículo 248.2 implicarán alteraciones documentales. Siendo así, debe plantearse como prioridad ese concurso y no el ideal o el real[300]. Como es sabido, la solución jurisprudencia, básicamente, resuelva como concurso de normas a favor de la falsedad (salvo mayor pena de la estafa) en el caso de de documentos privados y real, atendiendo al artículo 77 CP, en el caso de documento público, oficial o de comercio.

H). Los tipos defraudatorios no acaban aquí su relevancia en términos de delincuencia informática. No tanto porque el artículo 255 castigue con pena de multa de tres a doce meses al que «cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes: 1º. Valiéndose de mecanismos instalados para realizar la defraudación. 2º. Alterando maliciosamente las indicaciones o aparatos contadores. 3º. Empleando cualesquiera otros medios clan-

[294] Cf., por todos, Conde-Pumpido Ferreiro, como en la nota 238, p. 216 s.

[295] En Vives/Boix/Orts/Carbonell/González Cussac, *Derecho Penal. Parte Especial*, [3]1999, p. 454.

[296] Conde-Pumpido Ferreiro, como en la nota 238, p. 217, la califica como una estafa especial y analógica independiente del tipo básico y con sus propios elementos constitutivos.

[297] Choclán, como en la nota 235, p. 1079.

[298] Pérez Manzano, como en la nota 274, p. 454; Choclán, como en la nota 250, p. 297; Herrera, como en la nota 95, epígrafe VI, D; Queralt, como en la nota 249, p. 391. Probablemente, deba situarse en este terreno el planteamiento de Valle/Quintero, como en la nota 239, p. 1.153, cuando, pese a reconocer importantes similitudes con la estafa, afirman que se trata de un tipo defraudatorio que no comparte la dinámica comisiva de la estafa tradicional, cuya estructura conceptual no desempeñaría aquí una función de criterio rector interpretativo, y que la "ratio legis" del precepto habría sido precisamente castigar lesiones del patrimonio ajeno extramuros de la dinámica comisiva del engaño, aunque a continuación señalan, con referencia particularmente a las cuestiones penológicas, que se trata de una estafa específica (p. 1.154).

[299] En este sentido se cuestiona la configuración del art. 248.2 por su connotación patrimonial individualista, que habría dejado al margen los fraudes informáticos macrosociales (el sistema de cotizaciones bursátiles, la Hacienda Pública, el sistema de la Seguridad Social, etcétera). Cf. Gutiérrez Francés, como en la nota 8, p. 265.

[300] Si no me equivoco, en sentido parecido, Quintero, como en la nota 174, p. 1.824, al indicar que estimar posible la consunción «en relación con defraudaciones y alzamientos ... (en tanto que) el delito-fin incorpore necesariamente un elemento de mendacidad en su estructura típica y, por lo mismo, su dinámica comisiva deba pasar por ella». A favor del concurso ideal, aunque con reservas: Herrera, como en la nota 95, epígrafe VI, D, 4; Orts/Roig, como en la nota 26, p. 71. Cf., en todo caso, la reflexión de Romeo Casabona, como en la nota 49, p. 83 s.

destinos»[301], sino por la criminalización como modalidad defraudatoria análoga del *uso ilegítimo y utilizaciones abusivas de terminal*.

Sin duda, una palpable manifestación de que el legislador no se ha resistido a criminalizaciones muy discutibles, pensadas para supuestas macrodesviaciones por la trascendencia pública de determinadas hipótesis extremas y coyunturales[302], es el artículo 256 CP, que, con pena de multa de tres a doce meses, castiga al que «hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento del titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas»[303]. Se trata de uno de los excepcionales casos en que determinadas utilizaciones ilícitas, de los llamados hurtos "de uso" o "de tiempo"[304] son punibles en nuestro Derecho penal, si bien en este caso la descripción es tan amplia que podría, en una primera lectura, llevar a la conclusión de que todo uso no consentido es punible, lo que obviamente es incompatible con todas y cada una de las manifestaciones de la fragmentariedad y subsidiariedad del derecho penal. Lo segundo porque hay mecanismos suficientes (jurídico-privados o disciplinarios) para abordar estos ilícitos[305] y lo primero porque, por ejemplo, ni siquiera se ha contemplado el requerimiento previsto en el Anteproyecto

[301] El precepto se dirige a defraudaciones cometidas por consumidores en perjuicio de los suministradores, mientras que aquellas de las que pueden ser víctimas los usuarios se derivarían al ámbito de la estafa o los delitos relativos al mercado y a los consumidores (cf. González Rus, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", *Revista Electrónica de Derecho Penal y Criminología* [http: //criminet.ugr.es/recpc/recpc_01-14.hmtl], p. 16 y Orts/Roig, como en la nota 26, p. 72 s). En el contexto que aquí se toma en cuenta, se incluirían en el art. 255 las defraudaciones manipulativas a proveedores de acceso a Internet (al respecto, con especificaciones casuísticas, *ibídem*, p. 73 s). Tan sólo quiero poner de relieve que la formulación de la tercera variante ("empleando cualesquiera otros medios clandestinos") desmiente en no poca medida el punto de partida fijado en la entradilla del precepto de castigar defraudaciones utilizando los suministros indicados "por *alguno* de los medios siguientes". Por lo menos esos "otros medios", además de clandestinos, deberán ser equiparables a los que relatan los dos primeros números.

[302] Valle/Quintero, como en la nota 239, p. 1.196. Parecido Orts/Roig, como en la nota 26; Muñoz Conde, como en la nota 197, p. 433, considera que el precepto obedece a la proliferación del abuso de las llamadas telefónicas desde teléfonos de instituciones públicas para usos privados; y Vives/González Cussac, como en la nota 285, p. 1.270, a la vista de los debates parlamentarios, a los abusos telefónicos del personal doméstico. Además, el precepto estaría desfasado tanto tecnológica como sociológicamente (Gutiérrez Francés, como en la nota 41, p. 304) y su operatividad sería prácticamente nula (así, respecto de ambos aspectos, Morón, como en la nota 6, p. 47 s). Probablemente esto es cierto desde la perspectiva que la autora plantea, esto es, desde el punto de vista de la efectividad jurídico-penal. Pero, como es sabido, las normas penales tienen otros alcances sociales y políticos. Resulta a todas luces evidente que aún con todas las carencias técnico-jurídicas y político-criminales descritas, el precepto proporciona al titular del terminal informático y a las agencias de control penal de un poder "adicional" que desnaturaliza las claves del conflicto, que en la mayoría de los casos, si te atiende a lo que parece ser la ratio del precepto, suele ser un conflicto jerarquizado.

[303] A pesar de que el artículo 623.4 no se refiere expresamente a esta modalidad (castiga con arresto de dos a seis fines de semana o multa de uno a dos meses a quienes cometan defraudación de electricidad, gas, agua u otro elemento, energía o fluido, o en equipos terminales de telecomunicación en cuantía no superior a cincuenta mil pesetas) Orts/Roig, como en la nota 26, p. 76, recurren al mismo cuando el perjuicio es inferior a cincuenta mil pesetas. Igual González Rus, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", *Revista Electrónica de Derecho Penal y Criminología* (http: //criminet.ugr.es/recpc/recpc_01-14.hmtl), p. 16; Vives/González Cussac, como en la nota 295, p. 481.

[304] Morón, como en la nota 6, p. 47.

[305] Valle/Quintero, como en la nota 239, p. 1.195 s. Coincidentes, Morón, como en la nota 6, p. 47; Orts/Roig, como en la nota 26, p. 76; Suárez González, como en la nota 236, p. 728.

de 1994 de que la conducta se lleve a cabo subrepticiamente. Además se pone en duda la efectiva operatividad del precepto por las dificultades técnicas que conlleva y los problemas probatorios[306].

Sin embargo, la generalidad de la criminalización puede ser limitada en algunos aspectos, aunque -aparte de las dificultades hermenéuticas[307]- los resultados no evitarán la falta de racionalidad y legitimidad del precepto, pero que para algunos anulan por completo la virtualidad del precepto[308]. Por una parte, hay que subrayar un aspecto presente en el propio texto legal, a saber, que se trata de un delito patrimonial[309], por lo que la tutela se contrae a este aspecto del abuso, de manera que ataques a otros bienes jurídicos caen fuera de los límites materiales del precepto, en especial el mero intrusismo informático. Más concretamente, aunque esto pudiera ser más discutible, el precepto protege específicamente la propiedad, de manera que, a pesar de la ubicación del precepto, los usos no autorizados cuando el terminal es normalmente accesible al sujeto activo, no son típicos[310].

Pero, al margen de estas concreciones derivadas directamente del alcance del bien jurídico protegido, hay otras que se corresponden más específicamente con el desvalor de la acción. En primer lugar, porque el precepto se contrae al uso de terminales de telecomunicación, lo que naturalmente excluye la tipicidad del uso ordenadores no conectados o conectados pero con la conexión no operativa[311]. El precepto hace hincapié en la descripción típica en la ausencia de autorización por parte del titular, lo que debe interpretarse en el sentido más bien de que conste la falta de autorización por parte del titular.

Como expresión del desvalor del resultado se presenta específicamente la explícita y rotunda exigencia de perjuicio, que para la concurrencia de delito, debe ser superior a cincuenta mil pesetas. No hay duda, pues, que el perjuicio patrimonial causado al titular del terminal de telecomunicación[312] es, como resultado, un elemento estructural del tipo, lo que hace que escape a este precepto, por lo menos a su forma consumada, el mero acceso al sistema y posterior abandono del mismo, sin aquel perjuicio, que por lo demás planteará problemas en orden a su evaluación. Ciertamente, a efectos de la confirmación de si el hecho es o no típico basta con contabilizar perjuicios por encima de la cantidad antes expresada, pero tales perjuicios deben guardar con la acción un nexo típica-

306 Morón, como en la nota 6, p. 49.

307 Gutiérrez Francés, como en la nota 8, p. 303.

308 Cf. Gutiérrez Francés, como en la nota 8, p. 304.

309 Cf. Gutiérrez Francés, como en la nota 8, p. 304.

310 En tal sentido, raro será que se pueda plantear (Muñoz Conde, como en la nota 197, p. 433) si es o no aplicable el art. 434 cuando el que utiliza indebidamente el terminal es un funcionario o autoridad. En cambio, para Gutiérrez Francés, como en la nota 8, p. 304, sujeto activo pueden ser tanto los empleados como que utilizan los ordenadores más allá de lo autorizado como los terceros.

311 González Rus, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", *Revista Electrónica de Derecho Penal y Criminología* (http: //criminet.ugr.es/recpc/recpc_01-14.hmtl), p. 17 s. Quizás para excluir la tipicidad en tal caso baste simplemente invocar la falta de lesividad, que a mi juicio servirá también para excluir aquellos casos en que no hay un perjuicio patrimonial conectable con el uso (no autorizado) del terminal. De igual manera, creo que es atípico el uso no autorizado de equipos conectados en una red interna.

312 Vives/González Cussac, como en la nota 285, p. 481, aclarando que ello no supone que sea dueño, como ocurre en casos de alquiler.

mente relevante. Otra cosa será la cuestión de la responsabilidad civil, que podría dar lugar a que con fines de resarcimiento se atribuyeran al responsable penal perjuicios adicionales. Con todo, de estos daños adicionales, algunos pueden tener efectos penales, particularmente en orden a la individualización de la pena, concretamente en orden a la fijación, conforme al inciso primero del número 5 del artículo 50 del CP, de la extensión en días de la multa. De todas formas, volviendo al modelo de cálculo del perjuicio, se entiende generalmente que podría integrarlo el coste del servicio telefónico para el titular o usuario legítimo del equipo o terminal, el coste del alquier, si se trata de un ordenador en régimen de *leasing*, o el coste de la tarifa contratada con el proveedor de acceso a Internet.

Subjetivamente, la imputación sólo es viable en caso de dolo, que supone que el autor abarque el perjuicio patrimonial exigido por el tipo[313]. A mi juicio, es discutible, para lo que se puede invocar su naturaleza defraudatoria, y el ánimo de lucro que resulta implícito en ella, que pueda castigarse la variante de dolo eventual[314].

También puede plantear problemas su delimitación de figuras con las que guarda cierta afinidad. Así, por ejemplo, con la variante de daños informáticos del número 2 del artículo 264. La tesis más razonable es pensar que el artículo 256 debe dejarse para aquellos supuestos residuales en que el perjuicio patrimonial provenga de perturbaciones, molestias o alteraciones. Por otra parte, con relación al art. 197.2, si se admitiera la interpretación de Carbonell y González Cussac en el sentido de que dicha figura tutela junto con la *privacy* la integridad de los ficheros o soportes informáticos, también se plantearía una colisión del precepto planteado.

1.5. Espionaje *informático* empresarial.

A). En el capítulo XI del Título XIII del Código penal, en la sección tercera nominada "De los delitos relativos al mercado y a los consumidores", concretamente en el artículo 278, se contemplan una serie de conductas igualmente concernientes al objeto de este trabajo, tanto desde la perspectiva estrictamente informática, en la medida en que las empresas almacenan en soportes informáticos datos que desean mantener reservados, como desde la perspectiva propiamente cibernética, en tanto que las mismas están conectadas a redes de información y comunicación, de las que hacen uso para transmitir los datos. Esto ciertamente hace a las empresas vulnerables ante ataques que afecten a la salvaguarda de exclusividad de tales datos, lo que puede tener graves consecuencias que inciden particularmente en su capacidad competitiva. Son estas consideraciones las que han sido tenidas en cuenta por el legislador en el precepto indicado y en los que le siguen. Desde este punto de vista, lo que se protege no es tanto el secreto empresarial o industrial, ni desde luego, el secreto por sí mismo, como los intereses económicos ligados a la competitividad empresarial que tienen los secretos[315]. Por lo tanto, para que se pueda hablar de secretos en el sentido del tipo, y más precisa-

[313] Cf. Morales Prats/Morón Lerma, en Quintero (Dir.), como en la nota 107, p. 1.255 ss.

[314] Lo admite en cambio Orts/Roig, como en la nota 26, p. 77, si el autor no está seguro de la producción del perjuicio pero prosigue con su propósito asumiendo el que se genere.

[315] Cf., al respecto, Carrasco Andrino, *La protección penal del secreto de empresa*, 1998, Barcelona: Cedecs, p. 139; González Rus, en Cobo del Rosal (Dir.)/Carmona/González Rus/Morillas/Polaino/Portilla, *Curso de Derecho Penal español. Parte*

mente de secretos de empresa[316], es preciso que los datos a los que afecta el secreto -esto es, el conocimiento reservado de unos y oculto a otros[317]-, además de concernir a aspectos industriales o comerciales[318], estén ligados a la capacidad competitiva de la empresa. Apoyándose en tal requerimiento, que pone en relación el "secreto de empresa" con el bien jurídico protegido, en particular, si la acción recae sobre documentos que no contienen ningún secreto[319], esto es, son por ejemplo datos notorios o, existiendo la reserva, no afectan a la capacidad competetiva de la empresa[320], entonces, la conducta no será punible por este precepto, del mismo modo que si concurre el consentimiento del sujeto pasivo[321]. Parece clara en cualquier caso, la relatividad que rodea a estas exigencias y a sus límites[322].

B). La técnica de tipificación se asemeja a la desplegada en los delitos contra la intimidad. En primer lugar, en el artículo 278.1, se contempla el descubrimiento de secreto de empresa, castigando con prisión de dos a cuatro años y multa, al «que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados

especial, I, , p. 797 s y 800; Gutiérrez Francés, como en la nota 8, p. 286; Martínez-Buján Pérez, en Vives Antón (Coord.), como en la nota 285, p. 1.359 s, destacando la necesidad de que el secreto sea evaluable económicamente y que indirectamente se protegen los intereses socioeconómicos de los consumidores; Morales/Morón, como en la nota 313, p. 1278-1280; Muñoz Conde, como en la nota 197, p. 479; Orts/Roig, como en la nota 26, p. 103, respecto del artículo 278.1. Ya antes, Romeo, como en la nota 49, p. 168-170, subrayando el valor económico de la información en el ámbito industrial, comercial y financiero; Terradillos Basoco, *Derecho penal de la empresa*, 1995, Madrid: Trotta, p. 168 s, destacando, no obstante, con relación al antiguo art. 499, el carácter indirecto de la protección de la libre competencia.

316 Sobre todo ello, ampliamente, Bajo/Bacigalupo (Silvina), como en la nota 89, p. 482-488 y 498-502. Cf., asimismo, Morales/Morón, como en la nota 313, p. 1.280 (en general) y 1.286 s (respecto del art. 278.1).

317 Para González Rus, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", *Revista Electrónica de Derecho Penal y Criminología* (http: //criminet.ugr.es/recpc/recpc_01-14.hmtl), p. 8, esto comporta implícitamente unas medidas mínimas destinadas a mantener la reserva que expliciten una voluntad de exclusión por parte del titular.

318 Al respecto, Bajo/Bacigalupo (Silvina), como en la nota 89, p. 498-502; González Rus, como en la nota 315, p. 798; Martínez-Buján Pérez, *Derecho Penal económico. Parte especial*, 1999, Valencia: Tirant lo Blanch, p. 70-72, refiriéndose también a los relativos a la organización interna y relaciones de la empresa, y matizando que también serían típicos los relativos a la situación económica o financiera que fueran relevantes en términos de competitividad empresarial.

319 Orts/Roig, como en la nota 26, p. 107. Cf., asimismo, Muñoz Conde, como en la nota 197, p. 480.

320 Cf., no obstante, Morales/Morón, como en la nota 313, p. 1281. Además, este parámetro teleológico sirve a algunos autores para resolver el tratamiento del supuesto en que el secreto recae sobre un objeto ilícito -por ejemplo, un método de adulteración de alimentos, el hecho sería impune-, haciendo depender la solución de que tal secreto sobre objeto ilícito sea o no compatible con el bien jurídico, esto es, en este caso con el objetivo de mantener la competencia en términos de lealtad y los derechos de los consumidores. Cf. ibídem, p. 1.288, con relación al art. 278.2. Asimismo, ampliamente, Bajo/Bacigalupo (Silvina), como en la nota 89, p. 503-506, llegando a la conclusión de que en general resultaría impune (se daría una causa de justificación del art. 20, num. 7) en la medida en que el secreto de empresa o industria que versa sobre objeto ilícito no lesiona ni pone en peligro el bien jurídico protegido. Cf., igualmente, Carrasco Andrino, como en la nota 315, p. 278 ss.

321 Sobre esto y sobre el sujeto pasivo, cf., por todos, Bajo/Bacigalupo (Silvina), como en la nota 89, p. 485 s y 490-493.

322 Cf., por ejemplo, Bajo/Bacigalupo (Silvina), como en la nota 89, p. 487.

en el apartado 1 del art. 197». En realidad, se advierten dos conductas diversas[323], sin restricciones en cuanto al sujeto activo[324]: por un lado, el apoderamiento de datos, soportes u objetos referidos a un secreto de empresa; por otro, el empleo de artificios técnicos a que se refiere el artículo 197.1.

En cuanto a la primera (*descubrimiento de secreto de empresa mediante apoderamiento*), creo, contra la opinión dominante, que el apoderamiento[325] conlleva que el sujeto activo no sólo proceda a la aprehensión[326] de los documentos, soportes u otros objetos[327], sino que acceda a los contenidos de los mismos[328], aunque no se llegen a comprender[329], siempre que fueren entendibles. Es verdad que las razones invocadas para semejante restricción, se debilitan considerablemente respecto de las que la justifican en los delitos contra la intimidad, pero queda alguna, que, a mi juicio, resulta suficiente, como es que el número 2 se refiera a secretos *descubiertos* (o que el art. 280 requiera no haber tomado parte en el *descubrimiento*[330]).

[323] Por lo que el delito se configura como un tipo mixto alternativo, de modo que si el sujeto recurre a las dos conductas alternativas el delito continúa siendo único (Martínez-Buján, como en la nota 315, p 1.360. Conforme, Orts/Roig, como en la nota 26, p. 106).

[324] A diferencia de lo que ocurría con el art. 499 del anterior Código penal (cf., por todos, Martínez-Buján Pérez, como en la nota 318, p. 72).

[325] Que, según Bajo/Bacigalupo (Silvina), como en la nota 89, p. 494, comprende la retención.

[326] Entienden que no es preciso un apoderamiento físico con el consiguiente desplazamiento de cosa aprehensible, y que basta la captación mental o intelectual sin desplazamiento físico, Morales/Morón, como en la nota 313, p. 1.281, abarcando, por lo tanto, la anotación de los datos (ibídem, p. 1.282). Cf. asimismo, Carbonell Mateu, en Vives/Boix/Orts/Carbonell/González Cussac, como en la nota 295, p. 520; González Rus, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", *Revista Electrónica de Derecho Penal y Criminología* (http: //criminet.ugr.es/recpc/recpc_01-14.hmtl), p. 8; Gutiérrez Francés, como en la nota 8, p. 289 s. En particular, en cuanto a supuestos como la visualización y memorización del contenido de la pantalla, considera el hecho punible: Matellanes, como en la nota 239; Morales/Morón, como en la nota 313, p. 1.282. En contra, Gutiérrez Francés, como en la nota 8, p. 288 s. Orts/Roig, como en la nota 26, p. 105 s, aún partiendo de lo discutible del caso, opta por la posibilidad del castigo cuando la memorización vaya precedida de un acto ilegítimo del sujeto activo (coincidente, Martínez-Buján, como en la nota 318, p. 73, que subraya el caráter ilícito que en general debe tener el medio de apoderamiento), no así cuando sólo se aprovecha del que con descuido deja los datos a su alcance.

[327] La pretensión de dominio del futuro es aquí nuevamente palpable.

[328] Entre otros siguen la opinión dominante: Bajo/Bacigalupo (Silvina), como en la nota 89, p. 498; Carbonell Mateu, como en la nota 326, p. 520, que lo califica como delito de resultado cortado o mutilado de dos actos (igual Martínez-Buján, como en la nota 315, p. 1.360 s y el mismo, como en la nota 318, p. 74 s, aunque cree que se trata de una forma de ejecución imperfecta elevada a delito independiente, lo que no impide la apreciación de la tentativa), pero también de peligro (coinciente en esto último, Gutiérrez Francés, como en la nota 8, p. 289 s); Morales/Morón, como en la ºnota 313, p. 1.282 s, consideran que se trata de un delito de peligro y que no es preciso que los secretos hayan sido descubiertos efectivamente; Orts/Roig, como en la nota 26, p. 105 s, a propósito del alcance del elemento subjetivo del injusto (ver *infra* al respecto), indican que su presencia adelanta la consumación al momento de la apropiación de los datos o documentos o la utilización de los instrumentos señalados, sin precisarse que efectivamente llegue a desvelarse la información reservada. González Rus, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", *Revista Electrónica de Derecho Penal y Criminología* (http: //criminet.ugr.es/recpc/recpc_01-14.hmtl), p. 8, afirma que es un delito de consumación anticipada.

[329] Cf. Bajo/Bacigalupo (Silvina), como en la nota 89, p. 507.

[330] Cf., no obstante, Bajo/Bacigalupo (Silvina), como en la nota 89, p. 514.

En cuanto a la segunda, denominada *interceptación de secretos de empresa* (o control audiovisual clandestino y control ilícito de señales de comunicación), el Código no hace más que remitirse al supuesto equivalente del artículo 197.1, por lo que el alcance de éste viene a determinar el ámbito típico de tales controles[331], si bien habrá que acomodar dicho alcance a las particularidades del bien jurídico protegido. En particular, no basta la instalación de los artificios, siendo preciso además que se capte el sonido o la imagen[332].

En ambos casos se trata de hechos dolosos, pero es preciso que el sujeto actúe para descubrir un secreto de empresa (lo que no comprende la finalidad de revelación[333]), un elemento subjetivo[334] -aunque en coherencia con la interpretación aquí pretendida no sería más que un aspecto del dolo- que impide el castigo de la variante eventual-dolosa[335] y que debe darse en el momento de la acción[336].

Se ha suscitado la cuestión de la falta de un precepto equivalente al número 2 del artículo 197, que, como se vio, protege el *habeas data*. A la vista de la opción del legislador, la respuesta no puede ser otra que reconducir las correspondientes conductas a las hipótesis planteadas anteriormente, aunque cuidando de no forzar el texto legal, porque es evidente que, por el momento, el legislador no ha querido extender la protección adicional de la privacidad informática a los secretos empresariales[337].

C). Siguiendo la pauta de tipificación de la protección penal de la intimidad, se castigan además conductas de difusión, revelación o cesión de secretos[338], distinguiendo varios supuestos[339]. En

[331] Cf., no obstante, Martínez-Buján, como en la nota 315, p. 73.

[332] Bajo/Bacigalupo (Silvina), como en la nota 89, p. 497, para quienes los simples actos de instalación quedarían como formas imperfectas. Según Suárez, Bajo (Dir.), como en la nota 284, p. 535, son atípicos.

[333] Cf. Bajo/Bacigalupo (Silvina), como en la nota 89, p. 494 s, precisando que en cambio sí tiene el *animus scienci* típico tanto quien trata de conocer el secreto como el que entrega un soporte informático a un tercero sin acceder al mismo, pero no quien se apodera del documento y a continuación lo destruye o lo vende como material de deshecho. En cambio, Muñoz Conde, como en la nota 197, p. 480, lo vincula con el propósito de revelar a otros y no sólo de saber para sí.

[334] Cf. Bajo/Bacigalupo (Silvina), como en la nota 89, p. 495 s.

[335] Así Orts/Roig, como en la nota 26, p. 106. Parecido Bajo/Bacigalupo (Silvina), como en la nota 89, p. 496.

[336] Por esta razón es pertinente la especificación de Orts/Roig, como en la nota 26, 106 s, en el sentido de que si no consta tal propósito inicialmente y los datos se descubrieron por casualidad, el hecho queda al margen del tipo aunque después se revelen en perjuicio de las posibilidades competitivas de la empresa (en mi opinión, tal revelación, puede no obstante ser un dato indicativo de la finalidad descubridora, pero ya esto resulta más propiamente una cuestión de prueba de lo subjetivo). Cf., asimismo, Martínez-Buján, como en la nota 315, p. 74 y Morales/Morón, como en la nota 313, p. 1.287.

[337] No obstante, cf. Orts/Roig, como en la nota 26, p. 106.

[338] Que, para Martínez-Buján, como en la nota 315, p. 1.361 constituyen (con relación al art. 278.2) el "resultado material", si bien el delito (como el del art. 279.1. Ibídem, p. 1.364. En cuanto a dicho delito, similar Carbonell, como en la nota 326, p. 521 s., p. 522) no requiere la efectiva lesión de la capacidad competetitiva de la empresa, pero sí su puesta en peligro, por lo que a tales efectos se trataría de delitos de peligro hipotético o de aptitud: requiere la efectiva peligrosidad (*ex ante*) de esas acciones, unida a la posibilidad de que se produzca un resultado peligroso en la situación concreta. Lo que acerca este planteamiento a la consideración de que se trata de un delito de peligro concreto respecto de la capacidad competititva de la empresa, defendida por Morales/Morón, como en la nota 313, p. 1.288 (respecto del mismo supuesto).

[339] Según González Rus, como en la nota 315, p. 800 s, en ambos casos el dolo del sujeto debe abarcar la idoneidad de la conducta para afectar la capacidad competitiva de la empresa (requerimiento que extiende al art. 279).

primer término, en el número 2 de artículo 278, que constituye un tipo cualificado (la pena se eleva a prisión de tres a cinco años) del número 1 y que se refiere a sujetos que han participado en la conducta anteriormente referida, comportándose entonces como un tipo compuesto[340].

> No tiene parangón en la protección penal de la intimidad, la cuestionada -por innecesaria o, incluso, quizás peor, por perturbadora[341]- previsión concursal del número 3 del artículo 278, que salvaguarda la virtualidad de los correspondientes delitos y penas, por el apoderamiento o destrucción de los soportes informáticos, salvedad, que, cualquiera que sea la interpretación que se haga de la misma, sólo se refiere a soportes informáticos, por lo que para otros objetos materiales esta regla no tiene validez, sin perjuicio de que deba recurrirse a las reglas del concurso de leyes[342].

D). También se sigue el mismo patrón antes mencionado cuando se cualifican, en el artículo 279, la difusión, revelación y el tráfico por parte de sujetos obligados legal o contractualmente a guardar reserva («La difusión, revelación o cesión de un secreto de empresa llevada a cabo por quien tuviere legal o contractualmente obligación de guardar reserva, se castigará con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses»). En su actual configuración[343], que mantiene el carácter doloso de las agresiones al secreto empresarial[344], el sujeto activo no tiene que ser necesariamente un dependiente, siendo títulos posibles otros vínculos con la empresa de los que nazca la obligación de sigilo (por ejemplo, empleados de otra empresa encargada del mantenimiento de los equipos).

La infracción por parte del sujeto activo de deberes legales o contractuales que le incumben constituye un presupuesto del tipo, que en cualquier caso sólo abarca a los secretos que son conocidos en función de la relación que fundamenta la obligación de sigilo[345] y a los que se ha tenido acceso de modo lícito[346]. Ahora bien, en mi opinión no toda difusión o tráfico con infracción de tales deberes de reserva sin más constituye delito pues los deberes indicados deben ser cualificados y específicos. La singularidad y cualificación del deber de reserva, impedirá en general que un deber tan inespecífico como el que se contempla en la legislación laboral se tenga por título suficiente para invocar la tipicidad del hecho[347]. La relativización de deberes formales como base para la imputación lleva también a que ceda autonomía la discusión sobre los casos de cesación de la relación

[340] Martínez-Buján, como en la nota 318, p. 75 s, indicando además que siendo un delito de resultado material, no entraña la efectiva lesión del bien jurídico protegido (la comptetividad empresarial), sino su simple puesta en peligro (que no es concreto, sino genérico). Para algunos detalles problemáticos, en especial, las formas imperfectas, cf. Bajo/Bacigalupo (Silvina), como en la nota 89, p. 509 s.

[341] Así, Morales/Morón, como en la nota 313, p. 1.289. González Rus, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", *Revista Electrónica de Derecho Penal y Criminología* (http: //criminet.ugr.es/recpc/recpc_01-14.hmtl), p. 9, la califica de sorprendente.

[342] Cf. Martínez-Buján Pérez, como en la nota 315, p. 77; Orts/Roig, como en la nota 26, p. 108; Suárez, Bajo (Dir.), como en la nota 284, p. 536. En cambio, Bajo/Bacigalupo (Silvina), como en la nota 89, p. 495; González Rus, como en la nota 315, p. 799 creen que no debe limitarse a tales soportes.

[343] Que según algunos autores (Martínez-Buján, como en la nota 315, p. 1.364; el mismo como en la nota 318, p. 80 s; Morales/Morón, como en la nota 313, p. 1.291) permite la comisión por omisión. En contra, a la vista del carácter activo de los verbos típicos, Carbonell, como en la nota 326, p. 521 s.

[344] Cf. Martínez-Buján Pérez, como en la nota 315, p. 81, que no obstante estima suficiente el dolo eventual.

[345] Cf. Bajo/Bacigalupo (Silvina), como en la nota 89, p. 513.

[346] Martínez-Buján Pérez, como en la nota 315, p. 77

[347] En este sentido, la SAP Madrid 28-4-1999.

que unía al sujeto con la empresa[348], de manera que lo que importará es si existen previsiones legales o contractuales que extienden más allá de la cesación de dicha relación tales deberes de reserva[349] y sobre todo que tales deberes tengan relevancia penal, de manera que si el conflicto puede ser soslayado con criterios meramente reparatorios o disciplinarios se excluiría la imputación penal (aquí podrían entrar en juego los criterios de adecuación social y similares[350]). De otra parte, bajo las mismas directrices habrá de resolverse la hipótesis de que el sujeto activo no sea un dependiente. Es evidente que el Derecho penal no puede ser un instrumento genérico de aseguramiento de cualesquiera derechos o deberes civiles, laborales o mercantiles.

Por otra parte, no toda difusión o tráfico unida a la infracción de deberes penalmente relevantes es delictiva. Por de pronto, sólo es punible en su modalidad dolosa. Pero, además, hay que corroborar antes la lesividad respecto del bien jurídico protegido, de manera que, en principio, si no resulta otra cosa del tipo legal, dicho sea sin ánimo de precisión, la teoría de la imputación objetiva podría proporcionar bases adecuadas para resolver tal trámite[351]. Esto significa que se habrá de constatar, para la forma consumada, que *ex ante* y *ex post* la revelación o la cesión reunían condiciones adecuadas para menoscabar de forma penalmente relevante la competitividad empresarial[352]. Esta comprobación en muchos casos -lo que es un dato estadísticamente significativo, e incluso penalmente ilustrativo, pero no concluyente- reafirmará que la difusión o el tráfico comportan esa lesividad, pero en otros casos mostrará su insignificancia, su inadecuación, ... o, incluso, la existencia de condiciones concretas en el caso que permiten advertir que el menoscabo competitivo, en realidad, nunca o muy remotamente tendría que ver con la cesión o difusión, sino más bien con otros acontecimientos no dominables fáctica y normativamente. Por lo demás, como suele ocurrir también en la dogmática penal secuencialista, las magnitudes antes expresadas no son independientes, de forma que la especificidad y la entidad del deber de reserva condicionan el segundo aspecto.

E). Bien significativa[353] es la previsión del inciso segundo del artículo 279, que constituye un supuesto de autoaprovechamiento de secretos empresariales ajenos: «si el secreto se utilizara en

[348] Cf., al respecto, Bajo/Bacigalupo (Silvina), como en la nota 89, p. 511 ss.

[349] Cf., al respecto, el art. 13 de la Ley de Competencia Desleal, de 10 de enero de 1991, el art. 21.2 de del Estatuto de los Trabajadores, según la redacción de 1995.

[350] Cf. Morales/Morón, como en la nota 313, p. 1.291.

[351] En mi opinión, este delito permite advertir la insuficiencia de la tesis, cada vez más extendida, de reformular los delitos comisivos con las claves de la omisión, y sobre todo con ayuda de la posición de garante. Para este asunto cf. la propuesta en aquella línea de Pérez del Valle, "La revelación de secretos de empresa por persona obligada a reserva", *CDJ*, 1997/XIV, p. 115 ss, no obstante mantener un criterio restrictivo respecto del asunto específico antes planteado (p. 117 s).

[352] Este planteamiento, si no me equivoco, no se distancia demasiado del punto de vista de Martínez-Buján, como en la nota 318, p. 81, conforme al cual aun tratándose de un delito de resultado material (la difusión) no perdería su condición de delito de peligro (o de aptitud) con relación al bien jurídico protegido, o al de Morales/Morón, como en la nota 313, p. 1.291 s, o de Prats Canut, "Descubrimiento y revelación de secretos de empresa en el Código penal de 1995", *CDJ*, 1997/XIV (monográfico Delitos relativos a la propiedad industrial, al mercado y a los consumidores), que, tomando como referencia el mismo bien, lo califican de delito de peligro concreto.

[353] Y, para González Rus, como en la nota 315, p. 802 y Muñoz Conde, como en la nota 197, p. 481 cuestionable por el privilegio que comporta.

provecho propio, las penas se impondrán en su mitad inferior». El tenor legal además puede plantear algunas dudas interpretativas y de coordinación con el primer inciso (y, sólo aparentemente, con el artículo 278 y en particular con la interpretación aquí defendida), que aquí no serán objeto de atención. No obstante, debe destacarse que si, con la doctrina dominante, supone una atenuante específica del primer inciso[354], son trasladables al mismo gran parte de las consideraciones precedentes.

La particularidad de este delito radica en que en este caso el sujeto activo, en vez de difundir a terceros los secretos empresariales a los que ha tenido acceso (lícitamente), los utiliza en provecho propio, esto es, con lucro propio[355]. Por lo tanto, la utilización en provecho propio sustituye a la difusión, interpretándose mayoritariamente que la razón de la rebaja punitiva[356] es que, más allá de perjuicios o beneficios efectivos, genéricamente, en términos de puesta en peligro de la competitividad empresarial, en el pfo. primero el peligro queda abierto, mientras que en la variante atenuada queda circunscrita a la que pueda resultar afectada por la utilización que de los secretos haga el sujeto activo. Esto es similar a lo que plantea Terradillos[357], en el sentido de que la atenuación obedece al menor perjuicio que supondría para el titular del secreto el hecho de que no se diera una difusión indeterminada, que daría entrada a varios competidores[358], pero creo que la utilización que del secreto hace el sujeto activo del pfo. segundo del artículo 279 debe suponer una entrada en competencia con la empresa damnificada. Por otra parte, se impone la conclusión de que si el mismo sujeto cede los datos, con provecho o sin provecho propio se aplicaría el inciso primero. Si además de conocerlos los utiliza en beneficio propio, pero sin cederlos, se aplica el segundo inciso. Si los cede y además los utiliza en beneficio propio, se aplicaría un concurso de leyes.

F). Otra modalidad difusora de secretos empresariales se contempla en el artículo 280 (castigado con pena de prisión de uno a tres años y multa de 12 a 24 meses), que sólo pueden protagonizarla terceros ("sin haber tomado parte en su descubrimiento") «con conocimiento[359] de su origen ilícito»[360], lo que entre otras plantea la duda -que a mi juicio debe resolverse a favor de la primera opción[361]- de si esta modalidad presupone que se haya cometido un delito de descubrimiento o basta un acceso ilícito y naturalmente el sujeto activo del artículo 280 lo conoce. Por otra parte, está fuera de lugar la indicación del Código de que la conducta punible es la realización de alguna de las

[354] Mantiene este criterio Martínez-Buján, como en la nota 318, p. 83.

[355] Según González Rus, como en la nota 315, p. 802, no tiene que ser necesariamente de naturaleza económica.

[356] Que se ha sido cuestionada: Muñoz Conde, como en la nota 197, p. 481.

[357] Terradillos Basoco, como en la nota 315, p. 173, con relación a una previsión similar del Proyecto de Código Penal de 1994.

[358] Parecido Martínez-Buján, como en la nota 318, p. 83.

[359] Sin que baste la sospecha ni la mera previsión de posibilidad de dicho origen (Muñoz Conde, como en la nota 197, p. 481). Martínez-Buján, como en la nota 318, p. 90 requiere al menos dolo eventual.

[360] Adviértase que, a diferencia de tal previsión, la receptación se refiere al conocimiento de la comisión de un delito contra el patrimonio o el orden socioeconómico, el art. 298, y el 299 a hechos constitutivos de falta contra la propiedad. Asimismo en el blanqueo de capitales, aunque la acción de ocultación o encubrimiento se refiera a origen ilícito de los bienes, el ámbito penal queda restringido a bienes provenientes de delitos graves (art. 301.1 pfo. primero) o contra la salud pública (pfo. segundo).

[361] Como aquí, González Rus, como en la nota 315, p. 803.

conductas descritas en los dos artículos anteriores, porque en realidad su virtualidad no alcanza al número 1 del artículo 278 (ni al inciso segundo del artículo 279)[362].

G). Afectan a las conductas anteriormente mencionadas las peculiaridades penológicas previstas, por un lado, en el artículo 287, que en su número 1, restringe la perseguibilidad de estos hechos requiriendo denuncia de agraviado o su representante legal (o del Ministerio Fiscal cuando aquél sea menor, incapaz o persona desvalida), restaurando el régimen general, en el supuesto de que «la comisión del delito afecte a los intereses generales o a un pluralidad de personas». Por otro lado, en el artículo 288, que contempla, en su primer párrafo, la publicación a costa del condenado de la sentencia en periódicos oficiales (o, con carácter potestativo, en cualquier otro medio informativo, a requerimiento del perjudicado). Y, en el segundo, adoptar las consecuencias accesorias previstas en el artículo 129[363].

1.6. Impactos en el modelo penológico

I). En general, aunque no sin excepciones significativas, como la estafa, la toma en cuenta por el Derecho penal del uso de tecnologías de la información y de la comunicación ha supuesto, aparte de la creación de nuevos tipos penales o la ampliación del ámbito de lo punible respecto de tipologías precedentes, una agravación de las penas y, en algunos casos, la implementación de consecuencias jurídico-penales adicionales. En mi opinión, es díficil establecer orientaciones concluyentes, aunque hay atisbos significativos de que el modelo penológico anuncia cierto desgajamiento de fines resocializadores en beneficio de propósitos preventivo-generales, con frecuencia meramente simbólicos, que se intercambian con cierta facilidad con propósitos retributivos[364].

II). Llama la atención que el impacto de dichas tecnologías no haya supuesto una transformación específica del sistema de consecuencias jurídicas. En este sentido, a diferencia de lo que ocurrió con formas delictivas relativamente novedosas, como la delincuencia del tráfico viario, que dio lugar a la aparición de penas específicas, como la prohibición del derecho a conducir vehículos de motor, aquí no se ha llegado a contemplar sanciones penales específicas adaptadas, como sería la inhabilitación, suspensión o limitación de acceso a sistemas informáticos y, sobre todo, a redes de comunicación.

III). Con todo, en algún caso, mediante meras adaptaciones, puede lograrse una relativa adecuación de las previsiones penológicas al entorno cibernético. En este sentido, llama la atención que el art. 120.2 del CP establece un sistema de responsabilidad civil solidario[365] de titulares de editoriales, periódicos, revistas, estaciones de radio o de televisión o de cualquier otro medio de difusión es-

[362] Cf. Bajo/Bacigalupo (Silvina), como en la nota 89, p. 514, con referencias; González Rus, como en la nota 315, p. 803; Morales/Morón, como en la nota 313, p. 1.294.

[363] Como medidas cautelares (cf. Orts/Roig, como en la nota 26, p. 111) sólo cabe acordar la clausura temporal y la supensión previstas en las letras a) y c), respectivamente, del número 1 del art. 129.

[364] Esto viene a ser moneda corriente en el Derecho penal del riesgo o, por lo menos, en algunas de sus manifestaciones. Cf. Mapelli, *El delito de publicidad engañosa*, 1999, Valencia: Tirant lo Blanch, p. 89 s, subrayando cómo se da prioridad a fines retributivos.

[365] El propio número hace la salvedad de lo previsto en el art. 212 que contempla un sistema de responsabilidad subsidiario.

crito, hablado o visual por los delitos o faltas cometidos en sus medios, que por ello mismo no alcanza, como tales, a proveedores de Internet, sin perjuicio de la responsabilidad civil directa que pueda corresponderles como responsables penales.

IV). Por otra parte, como ha podido comprobarse, para algunos de los delitos antes relacionados se contempla la posibilidad de imponer consecuencias accesorias, lo que constituye una particular preocupación del Convenio sobre ciberdelincuencia, cuyo artículo 13.2 (en relación con el artículo 12) establece que las partes signatarias se asegurarán de que puedan imponerse sanciones o medidas penales o no penales, incluida la multa, eficaces, proporcionales y disuasorias a personas jurídicas que puedan ser consideradas administrativa, civil o penalmente responsables respecto de infracciones penales contempladas en el Convenio cometidas en su beneficio por sujetos que actuan individualmente o como miembros de un órgano de la persona jurídica en la que disponen de una posición principal, basándose en un poder de representación de la persona jurídica, en su autoridad para tomar decisiones en nombre de la persona jurídica o para ejercer mando en ella. Como supuesto adicional se contempla la responsabilidad de quien, por su falta de vigilancia, haya posibilitado la comisión por quienes actúan bajo la autoridad de la persona jurídica de uno de los delitos referidos.

V). No obstante, en el ámbito penitenciario pueden advertirse signos más claros de actualización motivada por la implantación de nuevas tecnologías[366]. Con carácter simplemente enumerativo cabe citar, en primer lugar, las previsiones de los artículos 6 al 9 del Reglamento Penitenciario de 1996, que regulan la protección de los datos de carácter personal de los ficheros penitenciarios, y en especial, en el artículo 6, la limitación del uso de la informática penitenciaria. En segundo lugar, la posibilidad de que, en base a lo previsto por el artículo 86.4 del mismo Reglamento, la pena de prisión se cumpla, en caso de que el interno esté clasificado en régimen abierto, sin necesidad de acudir al Centro Penitenciario, sustituyendo las estancias en el Centro penitenciario por estancias domiciliarias supervisadas electrónicamente[367], y que, a mi juicio, constituyen un ejemplo más de la tendencia a la "privatización"del sistema penitenciario[368]. A propósito de esta cuestión, la Dirección General de Instituciones Penitenciarias ha aprobado la Circular 13/2001, de 10 de diciembre[369].

En general, el sistema penitenciario, por razones de diverso tipo, se encontraba ya inmerso en cierto proceso de modernización en el que dichas tecnologías habrían mostrado una clara funciona-

366 Para una reflexión general sobre el futuro del sistema penitenciario cf. Arloth, "Über die Zukunf des Strafvollzug", G'A, 2001, p. 307-324.

367 Sobre esto, cf. Hudy, *Elektronisch überwachter Hausarrest. Befunde zur Zielgruppenplanung und Probleme einer Implementation in das deutsche Sanktionensystem*, 1999, Baden-Baden: Nomos; Wittstamm, *Elektronischer Hausarrest?. Zur Anwendbarkeit eines amerikanischen Sanktionsmodells in Deutschland*, 1999, Baden-Baden: Nomos. Para una recensión de estos trabajos cf. Groß, G'A, 2000, 602-606; Asimismo, cf. Kawamura, *Elektronisch überwachter Hausarrest: Alternative zum Strafvollzug?*, 1997, Bonn: BAG-S; Schlömer, *Der elektronisch überwachte Hausarrest: eine Untersuchung der ausländischen Erfahrungen und der Anwendbarkeit in der Bundesrepublik Deutschland*, 1998, Frankfurt del Meno: Lang.

368 Para precisiones, Hayo Bernsmann, *Elektronisch überwachter Hausarrest unter besonderer Berücksichtigung von Privatisierungstendenzen*, 2000, Gotinga: Cuvillier.

369 Agradezco al Director del Centro Penitenciario de Huelva, Don Francisco Sanz García, la inforación sobre el particular.

lidad con orientaciones generales del mismo, que se habrían visto reforzadas (piénsese en la debatida cuestión sobre los FIES). En este sentido, cierta tendencia del sistema penitenciario a "neutralizar" y "homogeneizar" el contacto con los internos se habría visto impulsada por la implementación de medidas electrónicas, permitiendo un incisivo modelo de control asegurativo inmediato. No obstante, al menos por el momento, nuestro sistema penitenciario se muestra, en general, impermeable al acceso de los internos al correo electrónico y a Internet.

1.7. Apuntes sobre cuestiones policiales y procesales

I). Como se ha indicado, la impunidad es una característica central de la delincuencia informática y de la cibercriminalidad, que en parte se atribuye a insuficiencias de la Justicia penal ordinaria, de manera que son relativamente frecuentes propuestas que en mayor o menor grado implican cierta especialización de las instancias encargadas de la persecución, sobre todo en el ámbito policial[370] -en particular, a través de las "patrullas cibernéticas"- y de la fiscalía[371], aunque no han faltado demandas de creación de juzgados especiales que estén en mejores condiciones de enfrentarse a la complejidad que aquella delincuencia comporta. Al mismo tiempo se pretende afrontar la naturaleza transnacional de la delincuencia informática, reforzando los mecanismos de cooperación penal internacional[372], lo que incluso ha llevado a reivindicar la creación de tribunales internacionales para la persecución de la delincuencia cibernética[373], si bien donde más intensamente se ha desarrollado la cooperación[374] ha sido en el ámbito policial, aunque no faltan algunos mecanismos de colaboración entre fiscalías y juzgados de instrucción[375].

Precisamente a la cooperación internacional dedica el Convenio sobre ciberdelincuencia el Capítulo III, exhortando a la más amplia cooperación en investigaciones y procesos concernientes a infracciones penales ligadas a sistemas y datos infromáticos o para recoger pruebas en soporte electrónico de una infracción penal (art. 24), previsión a la que siguen unos principios relativos a la extradición, centrándose de nuevo en las infracciones penales definidas en los artículos 2 al 11 del Convenio (art. 24). A continuación, se establecen normas relativas a la ayuda mutua: en el artículo 25 se contemplan los principios generales; en el 26, la información espontánea; en el artículo 27, se regulan los procedimientos a los que, a falta de acuerdos internacionales, habrán de atenerse las demandas de ayuda mutua; contemplando el artículo 28 las condiciones de confidencialidad y res-

370 Cf. Mata y Martín, como en la nota 69, p. 156 s; Schwarzenegger, como en la nota 68, p. 113.

371 Sobre ello, no sin reservas, Marchena, como en la nota 14, p. 66-68.

372 Respecto de la extradición, Mata y Martín, como en la nota 69, p. 150-152, subrayando las limitaciones que en estos casos suponen para la misma la exigencia de doble incriminación, el *ne bis in idem* o de mínima sanción y la exclusión por razón del *ne bis in idem*.

373 Al respecto, también con reservas, Marchena, como en la nota 14, p. 68-70.

374 Desde luego, esto se advierte en el aluvión de acuerdos y recomendaciones internacionales, más acusado en el ámbito de la Unión Europea, si bien también se ha traducido en una efectiva cooperación. Por ejemplo en la creación de bases de datos policiales internacionales. De todas formas, se ha llamado la atención a propósito de ciertas disfunciones en el proceso de institucionalización de esa colaboración, pues en ocasiones las instancias creadas se superponen o incluso se interfieren.

375 Sobre todas estas cuestiones cf. Hernández Guerrero/Álvarez de los Ríos, "Medios informáticos y proceso penal", *EJMF*, 1999/IV, p. 471-602 (*passim*).

tricción de la utilización que la parte requerida puede imponer al requirente; los artículos subsiguientes refieren específicamente la ayuda mutua con relación a datos almacenados en sistemas informáticos ubicados en el territorio de la Parte requerida a la conservación (art. 29), a la consiguiente comunicación (art. 30), al acceso, obtención y su comunicación (art. 31), así como a la "real-time collection" de datos sobre el tráfico (art. 33) y la "real time collection or recording" de datos relativos al contenido de comunicaciones específicas transmitidas por un sistema insformático (art. 34); el artículo 32 habilita a las Partes signatarias a acceder, con independencia de su localización geográfica, a los datos almacenados accesibles al público o a otros de acceso restringido con el consentimiento de la persona que esté legalmente autorizada a divulgarlos; y el artículo 35 contempla el llamado "24/7 Network".

II). Ya se puso de relieve que los avances tecnológicos que comporta la Sociedad de la Información también se ponen a disposición de la Justicia penal, ofreciendo a ésta posibilidades en la persecución y lucha contra la criminalidad (no sólo la informática) desconocidas hasta ahora, aunque no se ignore que estos instrumentos conllevan graves riesgos para derechos individuales y de alteración del equilibrio de poderes estatales, y provocan recelos no sólo en sectores significativos de la opinión pública, sino entre las propias víctimas, que se muestran remisas a la aceptación de controles "difusos" en manos de instituciones públicas.

En especial, facilitan también a las instancias de control penal mayores posibilidades de vigilancia tecnológica y de almacenaje y gestión de información, lo que facilita que dichas agencias se arroguen papeles propios de los servicios secretos, una tendencia que se une a la relativa asunción por el proceso penal de roles policiales, que igualmente se ve favorecida por aquellas tecnologías, en tanto posibilitan una permanente y discreta vigilancia electrónica preventiva, esto es, anterior a la comisión de hechos delictivos[376]. Estas tendencias plantean complejas cuestiones, respecto de las que aquí sólo llamaré la atención sobre un aspecto particular, referido a la primera de las tendencias citadas, a saber, que la "cualificación" que implica se traduce en cierta impermeabilidad al control jurídico. Suponiendo que la tendencia esté justificada, deben arbitrarse medios que neutralicen estos efectos secundarios, pues en modo alguno es admisible que por esta vía y con esta excusa la acción estatal tienda a quedar al margen del Estado de Derecho.

La puesta a disposición de las agencias de control de estas tecnologías ha suscitado cuestiones específicas como el tratamiento jurídico de las intervenciones de las llamadas "patrullas cibernéticas". Al respecto, se plantea distinguir entre aquellas actuaciones que se llevan a cabo respecto de contenidos accesibles al público, que en general se considera que no son atentatorias a los derechos fundamentales, y aquellas que se dirigen a contenidos de acceso restringido, distinguiéndose a tal efecto entre intervenciones de carácter represivo, fundamentadas en la posible comisión de un

[376] Sobre algunos aspectos relativos a estas tendencias, cf. Hernández Guerrero/Álvarez de los Ríos, "Medios informáticos y proceso penal", *EJMF*, 1999/IV, p. 477-480, 492, 494, aparte de otras referencias más específicas (en especial, respecto de la vigilancia electrónica, p. 505-509, y sobre la videovigilancia, p. 509-522).

hecho delictivo, y las que se fundamentan en la prevención de riesgos públicos, que plantean problemas más arduos desde el punto de vista indicado[377].

III). Uno de los instrumentos a que se recurre con más frecuencia en las investigaciones criminales en la actualidad es la *intervención de comunicaciones*[378], que, como todos los medios de investigación, está subordinada a su función probatoria[379]. Pese a no estar previstas específicamente en el art. 579.2 de la LECrim, la jurisprudencia -como hiciera antes de la reforma de 1988 con las intervenciones telefónicas, que hasta entonces no tenían cobertura legal expresa- ha legitimado las intervenciones de comunicaciones informáticas, tanto la intervención del contenido de la comunicación, como el simple control de las comunicaciones realizadas, que, al igual que ocurre con las intervenciones telefónicas, no requieren la interrupción de la comunicación. A partir de ahí la cuestión reside en determinar el régimen aplicable a las mismas, dado que en nuestro sistema procesal rigen normas distintas según el tipo de comunicación. Ciertamente, lo ideal sería contar con previsiones legales específicas, pero siempre se plantearían problemas respecto de medios de comunicación nuevos. En realidad, es posible que la evolución de las comunicaciones termine anulando el problema en la medida en que se tiende a la convergencia de los sistemas de comunicación y a formas híbridas de ésta. Desde este punto de vista, lo más significativo no van a ser las especificaciones legales para cada modelo de comunicación, sino que el régimen jurídico sea lo suficientemente flexible para que se adecue a las particularidades, pero al mismo tiempo se garantice un mínimo de seguridad jurídica. En definitiva, de lo que se trataría es de alcanzar una síntesis entre certeza y proporcionalidad[380], que permita atender las diferencias materiales y valorativas[381] e incluso las meramente circunstanciales. Estas premisas, que al objeto de obtener resultados eficaces deberán ser completadas con requerimientos técnicos como el empleo de programas o dispositivos discriminadores, deben garantizar en cualquier caso que queden salvaguardadas determinadas exigencias que son manifestación de un *fair process*, que impide en particular intervenciones generalizadas,

[377] Al respecto, con relación al Derecho alemán, cf. Zöller, "Verdachtslose Recherchen und Ermittlungen im Internet", GA, 2000, p. 568-577 (esta última para las conclusiones).

[378] Subraya esto Weßlau, "Gefährdungen des Datenschutz durch den Einsatz neuer Medien im Straftprozess", *ZStW*, p. 681, indicando que en particular las intervenciones de las comunicaciones telefónicas habrían pasado a ser una "medida estándar", que difícilmente se atiene al principio de *ultima ratio*.

[379] Con ello se pone de manifiesto que en un Estado de Derecho, es básico articular el proceso penal funcionalmente, en el sentido de que las actuaciones procesales no constituyen un fin en sí mismo, sino que se orientan a hacer posible la pretensión procesal y el telos propio de cada una de sus fases y actos. Al fin y al cabo prácticamente todos los actos procesales son adjetivos. Esto explica específicamente que la obtención de pruebas de cargo que desvirtúen la presunción de inocencia junto con la consecución de la verdad material limitada gobierne no sólo el ritual probatorio ordinario sino otras actuaciones procesales, como actos de investigación (si no me equivoco, este planteamiento coincide con lo que Weßlau, como en la nota 378, *passim* [p. 707 s, en las conclusiones], plantea respecto de las intervenciones de las que se ocupa). Por ello, la teleología probatoria se extiende más allá del juicio oral.

[380] Respecto de particularidades (o sea, si se trata de comunicaciones telefónicas digictales, correos electrónicos, chats, videoconferencias, etcétera) y su asimilación al régimen de les intervenciones telefónicas o al de las telegráficas, fundamentalmente, cf. Hernández/Álvarez, como en la nota 376, p. 496-498; Mata y Martín, como en la nota 69, p. 157 s.

[381] Consciente de ello, Mata y Martín, como en la nota 69, p. 157 s, siguiendo a Hernández Guerrero/Álvarez de los Ríos, "Medios informáticos y proceso penal", EJMF, 1999/IV, p. 496 ss.

"ilimitadas" en el tiempo y arbitrarias, ajenas al control judicial y que anulen la efectividad del derecho de defensa y la naturaleza contradictoria del proceso[382]. Estas consideraciones remiten en última instancia a un juicio de ponderación, respecto del que aquí sólo se hará mención a una sugerente tesis[383] que trae a colación los peligros que comporta para el Estado de Derecho en su conjunto el uso estatal de tecnologías avanzadas de control, de manera que en tanto existe un interés comunitario en mantener bajo control el potencial de poder que las funciones de control y vigilancia con aquéllas relacionadas, el juicio en cuestión habría de atender también ese interés y no sólo los parámetros habituales de la "dogmática de las medidas de intervención".

IV). La naturaleza organizada de algunas de las manifestaciones de la criminalidad informática permite que se puedan aplicar a éstas las previsiones contempladas respecto de aquéllas. Esto en particular se plantea respecto del *agente encubierto*, al que se refiere la LO 5/1999, que introdujo el artículo 282 bis de la LECr, que, entre otros supuestos, contempla la posibilidad de recurrir a esta institución en casos de estafa informática y pornografía infantil.

Por otra parte, cabría plantear la cuestión de si existiría provocación policial al delito y, en su caso, delito provocado, cuando en funciones de investigación la policía, por ejemplo, abona una contraprestación por asisitir a un espectáculo pornográfico en el que participan menores o cuando la policia descarga una página con contenidos punibles dando lugar a la distribución de estos.

V). Aunque, como se ha indicado, la funcionalidad probatoria se extienda más allá del juicio oral -y no sólo respecto de los casos de prueba anticipada y preconstituida-, el núcleo del régimen probatorio reside en esa fase, lo que avala la necesidad de acreditar plenamente -salvo excepciones como las indicadas- en dicho acto el material de prueba.

Ciertamente, las nuevas tecnologías comporta un haz muy extenso de problemas también respecto de esta cuestión, del que aquí sólo se harán mención telegráfica a algunos aspectos puntuales.

(a) La configuración del sistema español de prueba permite la admisión de pruebas no explicitadas por el legislador. Esto en particular hace posible el acceso al proceso, aunque no sin cumplir requerimientos adicionales -que para algunos medios resultan bastante problemáticos-, de documentos digitales, infografías y otros soportes informáticos. El problema es, pues, no qué instrumentos pueden ser considerados medios de prueba, sino bajo qué condiciones pueden llegar a serlo.

[382] Consideraciones que a mi juicio son válidas frente a todos, incluso los que se han denominado enemigos. Convendría advertir que en un Estado de Derecho la categoría del Derecho penal del enemigo no tiene cabida, en el sentido de que no es posible construir un sistema penal paralelo. Se debe comprender que las peculiaridades, por ejemplo, del terrorismo son, como tales, especificidades respecto de instituciones particulares. Además un Derecho penal del enemigo pugnaría con una previsión constitucional específica como es la que establece la temporalidad de los estados de escepción, alarma y sitio (cf. Gimeno Sendrá, en Gimeno Sendrá/Moreno Catena/Cortés Domínguez, *Derecho procesal penal*, 1997, Madrid: Colex, p. 463).

[383] Weßlau, como en la nota 378, *passim* (p. 706 s, en la síntesis). Para una síntesis del debate que estos planteamientos suscitaron entre algunos procesalistas alemanes (Wolter, Hamm, Nelles, Welp, Rex y Prittwitz), cf. Jeßberger/Kreuß, como en la nota 34, p. 833-838.

(b) En cuanto al documento digital se plantea su equiparación al documento. Al contrario de lo que ocurre en Derecho penal sustantivo, donde en principio se les ha llegado a equiparar[384], la legislación procesal no lo contempla. Con todo la jurisprudencia penal admite en determinadas condiciones la equiparación. Una de ellas es que el documento digital reúna las condiciones de autenticidad exigidas procesalmente. La cuestión abre la puerta a la posibilidad de considerar la firma digital como medio equiparable a tales efectos[385] a la firma manuscrita. En tal sentido es muy dudoso que no sólo la incertidumbre que comporta la firma electrónica sino también su alcance efectivo (en el sentido de que más que a la identidad del sujeto, sirve a la identidad de la clave) puedan ser cargados negativamente. Se debe considerar a tales efectos que desvirtuar la presunción de inocencia es una sutil atribución jurídica que responde a un equilibrio difícil. El hecho de que en determinadas condiciones se llegue a proteger la firma electrónica penalmente no es indicativo de que le estuviera reconocida esa legitimidad.

(c) Las nuevas tecnologías pueden proporcionar también cambios significativos en la fase clave del proceso penal, esto es, en el juicio oral[386]. En efecto, pueden permitir que se neutralicen algunos de los aspectos más negativos de ciertas medidas procesales tomadas con motivo del Derecho procesal penal del enemigo, especialmente en lo que se refiere a la protección de testigos. Desde esta perspectiva, la introducción de estas tecnologías puede abrir perspectivas positivas desde el punto de vista incluso el imputado, del mismo modo que posibilita la realización en esta fase de la cooperación penal internacional. Pero al mismo tiempo introduce riesgos evidentes, en la medida en que puede servir de coartada para restaurar un modelo procesal que relativizara el peso que debe tener el juicio oral o, como se dice, en la terminología alemana el *Hauptverhandlung* (vista o juicio principal), cercano a nuestro *plenario*. Este sentido no debe perderse.

VI). Para terminar sólo una breve síntesis de otras previsiones procesales del Convenio sobre ciberdelincuencia[387], que, dejando de lado las particularidades, se extienden no sólo a los específicos ciberdelitos a los que se refiere el Convenio, sino también a cualesquiera otras infracciones penales cometidas mediante un sistema informático y respecto de la recogida de pruebas electrónicas de cualquier infracción penal (art. 14.2). En primer lugar, en el art. 16, que las autoridades competentes puedan ordenar la preservación inmediata de datos informáticos especificados por el Convenio -incluidos los de tráfico- guardados en un sistema informático, en tanto existan razones para pensar que son particularmente susceptibles de pérdida o modificación, imponiendo para ello la obligación, a quien los guarde o bajo cuyo control estén, de proteger su integridad durante el tiempo que sea necesario, hasta un máximo de 90 días, susceptibles no obstante de prórroga. En segundo lugar, en el art. 17, con relación a los datos relativos al tráfico, que se establezcan las medidas adecuadas

[384] Véase supra.

[385] Aparte de ello la firma puede contribuir a garantizar la integridad, entre otras.

[386] Sobre algunos aspectos de esta cuestión, cf. Beulke, "Empirische und normative Probleme der Verwendung neurer Medien in der Hauptverhandlung", *ZStW*, 2001, p. 709-836, así como Jeßberger/Kreuß, como en la nota 34, p. 838-844, donde se referencia el debate celebrado en el Encuentro de catedráticos de Derecho penal celebrado en la Universidad de Passau (Alemania) el 25-5-2001 a partir de la ponencia en que se basa el artículo antes citado.

[387] Cf. supra nota y texto.

para asegurar la preservación inmediata de tales datos con independencia de que hayan participado en la transmisión uno o varios proveedores de servicios y la difusión inmediata a la autoridad competente de los datos de tráfico que sean precisos para identificar los proveedores de servicio y la vía a través de la cual se transmitió la comunicación. En tercer lugar, en el artículo 18, la habilitación a las autoridades competentes para ordenar a quien dentro del territorio posea o tenga bajo su control datos informáticos especificados por el Convenio guardados en un sistema informático o en un soporte de almacenamiento informático que los comunique a aquéllas, o a un proveedor que ofrezca sus servicios en el territorio que comunique los datos que posea o estén bajo su control "relativos a los abonados" concercientes a dichos servicios. El art. 19 plantea la habilitación a las autoridades competentes para investigar o acceder directamente a un sistema informático, a una parte del mismo y a los datos allí guardados o a un sistema de almacenaje informático (num. 1), o bien a otro sistema que pueda contener dichos datos y al que se pueda acceder desde el primero (num. 2). El número 3 extiende la legitimación a la aprehensión/apoderamiento/embargo de los datos mismos, copiado, preservación de la integridad de los datos guardados o hacer inaccesible o borrar tales datos del sistema informático objeto de la pesquisa. En el número 4 habilita para requrir a quienes tengan conocimientos sobre el funcionamiento del sistema informático o de los mecanismos de protección del mismo para que proporcionen toda la información razonablemente necesaria para hacer posible las actividades previstas en los números 1 y 2. El artículo 20, con relación a datos de tráfico asociados a comunicaciones determinadas transmitidas en su territorio por medio de un sistema informático, habilita a las autoridades competentes para que en tiempo real los archiven o graben directamente o bien obligen al proveedor de servicios para que dentro de sus posibilidades técnicas a hacerlo o a prestar su ayuda o asistencia para que las autoridades puedan realizarlo. En el número 3 se contempla la posibilidad de obligar al proveedor del servicio para guardar reserva sobre estas actividades así como de la información que tenga al respecto. Paralalemente en el artículo 21 se contempla la interceptación de datos relativos al contenido de comunicaciones determinadas, estableciendo un sistema similar de habilitaciones a las autoridades y de obligaciones de los proveedores de servicios, exigiendo no obstante que se trate de infracciones graves.

CONCLUSION

Parece claro que, aunque la Sociedad del Riesgo, sigue organizándose entorno a "valores materiales" y, en cambio, en la Sociedad de la Información se acentúa el peso de los "valores virtuales", existe una estrecha relación entre ambas, que también se manifiesta en las respectivas formas de criminalidad, aunque en las de la Sociedad de la Información se habría acentuado la lejanía del autor respecto del escenario del crimen. En todo caso, una afirmación de estas características se ve obstaculizada por la heterogeneidad de manifestaciones de la delincuencia informática y de la cibercriminalidad, lo que, junto con las carencias analíticas dificulta una explicación homogénea. La estrecha relación con la Sociedad del Riesgo se evidencia también en la respuesta jurídico-penal y más aún en las orientaciones político-criminales. También las que se plantean para la Sociedad de la Información tienen a ampliar el ámbito de lo punible y apuntan a formas de imputación desformalizado-

ras, integrantes de estatuto jurídico-penal autónomo respecto de la Sociedad de la Información[388], a medio camino, junto con el Derecho penal del riesgo, entre el Derecho penal nuclear y el Derecho penal contra los enemigos.

Estas observaciones dejan entrever una actitud crítica respecto de ese eventual Derecho penal de la Sociedad de la Información, pero no cuestionan en modo alguno la observación de que "something must be done"[389], sino principalmente que, de nuevo, ese algo deba ser necesariamente el Derecho penal y que se ignore el principio de proporcionalidad, en el sentido de que la respuesta penal da la impresión de que no matiza como sería preciso su respuesta orientándose más bien por una percepción macrimonológica del fenómeno, ignorando, de un lado, la heterogenedad indicada, de otro, que una cosa son los aspectos criminológicamente relevantes y otra el ámbito más bien preciso y agravado que debe ser prohibido y perseguido mediante las normas penales. Estas dos salidas son completamente unilaterales y desconocen en una medida similar el papel y la naturaleza del Derecho penal, al que es inmanente la antinomia entre la protección de la sociedad y la salvaguardia de la libertad, a través de la mayor protección posible de los derechos del delincuente[390]. No obstante esta actitud crítica, se ha intentado exprimir en lo posible aquellos instrumentos que ofrecen la ley y la dogmática penales para aminar los costes que esta tendencia conlleva para los principios del Estado de Derecho.

Las consideraciones precedentes valen para las cuestiones procesales. Pero aquí se acentúa un rasgo genuino de la moderna política criminal: la pretensión de instaurar modelos de control universalizados e indiscriminados, productos fáciles, unilateralmente sesgados por las demandas de eficacia, que en el mejor de los casos sólo se pueden cuantificar por su limitada capacidad de contención. Con ello, se renuncia a respuestas jurídicamente avanzadas y precisas que combinen adecuadamente las exigencias garantistas y de eficacia[391].

Para terminar, del mismo modo que a propósito de la criminalidad de la Sociedad del Riesgo se ha replanteado, aunque sin cuestionarlo en su núcleo, el papel del Derecho penal, la cibercriminalidad da pie a considerar estos interrogantes. Aquí, no obstante, se plantean algunas particularidades. Por de pronto, el problema no radica tanto en optar por una solución jurídica como la del Derecho de Intervención o del Derecho penal de segunda velocidad (que no obstante aquí se manifiestan parcial y puntualmente por ejemplo a través de algunos regímenes sancionadores como los de la protección de datos o la regulación que se pretende establecer sobre la contratación en la Sociedad de la Información), como dos soluciones "extrajurídicas": una la de las soluciones técnicas y otra la autoregulación, esto es, el abandono del control a las máquinas y a las fuerzas individuales y sociales. Pero, tampoco esto supone una respuesta particularmente meritoria por su imaginación y rigor.

[388] Crítico respecto de esta orientación, Hoyer, según la referencia de Jeßberger/Kreuß, como en la nota 34, p. 828.
[389] Ashworth, *Principles of criminal law*, ²1999, Oxford-Nueva York: Oxford Unisersity Press, p. 67.
[390] Sobre la síntesis y su carácter antagónico, por todos, Roxin, *La evolución de la Política criminal, el Derecho penal y el Proceso penal* (trad. M.C. Gómez Rivero), Valencia: Tirant lo Blanch, 2000, p. 31 s.
[391] Así ya en mi trabajo "Crónicas Iberoamericanas. Informe sobre Criminalidad Organizada. España", *RP* 2, 1998, p. 103.

RESUMEN: En la delincuencia de la Sociedad de la Información se acentúan algunos de los rasgos característicos de la criminalidad de la Sociedad del Riesgo. Lo mismo ocurre con los respectivos sistemas de control penal. Con todo, parece todavía posible acudir al arsenal garantista para limar algunos de los aspectos más enfrentados con los principios penales del Estado de Derecho.

ABSTRACT: In the deliquency of the Information Society some of the characteristics of criminality of the Risk Society are intensified. The same ocurrs with the respective systems of penal control. However, it still seems possible to resort to the range of juridics guarantees to lessen some of the most controversial aspects with respect to the penal principles of the State of Law.