© CRITERIOS DE ATRIBUCIÓN DE RESPONSABILIDAD PENAL A LOS PRESTADORES DE SERVICIOS E INTERMEDIARIOS DE LA SOCIEDAD DE LA INFORMACIÓN

Oscar Morales García
Profesor de Derecho Penal
Universitat Oberta de Catalunya

Sumario: I- INTRODUCCIÓN. 1. Origen y desarrollo de Internet. 2. La interpretación de la Sociedad de la Información desde el Derecho. 3. El rol de los intermediarios. II. COMUNICACIÓN TELEMÁTICA Y SERVICIOS DE INTERNET. Cuestiones técnicas. 1. La comunicación vía Internet. 2. Servicios de red. 2.1 WWW. 2.1.1. Webcasting. 2.2 FTP. 2.3. Telnet. 2.4 e-Mail. 2.5. News. 2.5.1. Listas de distribución. 2.6. Chat. III. LA DIRECTIVA DEL COMERCIO ELECTRÓNICO Y LOS CRITERIOS DE RESPONSABILIDAD JURÍDICA DE LOS PRESTADORES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN. 1. Mera transmisión y acceso. 2. Memoria tampón o *Caching*. 3. Alojamiento de datos. 4. La cláusula de cierre del artículo 15 de la Directiva. IV. CRITERIOS DE ATRIBUCIÓN DE RESPONSABILIDAD JURÍDICO PENAL POR CONDUCTAS AJENAS. 1. Sobre la aplicación del artículo 30 CP 2. Responsabilidad por comisión activa a título de autoría y participación. 3. La responsabilidad en comisión por omisión.. 3. *Locus comissi delicti*.

Este trabajo constituye un borrador (*work paper*) en el que se contiene una primera aproximación a la materia, realizada en el seno de una investigación más amplia sobre la responsabilidad de los Proveedores, que actualmente desarrolla el Grupo de Investigación E-Crime Prevention, del **INTERNET INTERDISCIPLINARY INSTITUT (IN3)**, en el que participan la Universitat Oberta de Catalunya (coordinación), la Università degli Studi di Trento; la Escuela Judicial (CGPJ), la Unidad de Delincuencia Tecnológica de la Policía Nacional española y la Fiscalía del Tribunal Superior de Justicia de Catalunya. La versión definitiva, una vez ordenadas y depuradas las reflexiones que en él se contienen, será publicada en el número correspondiente al mes de junio de la Revista de Derecho y Proceso Penal, Aranzadi, 2001. Entre tanto, y dadas las continuas modificaciones que se operarán sobre el mismo, queda limitado el derecho de cita, como es costumbre en la difusión de los trabajos preparatorios, a la expresa autorización del autor.
Si está Ud. interesado en recibir comentarios y noticias sobre Derecho y Sociedad de la Información, elaborados por los Estudios de derecho de la Universitat Oberta de Catalunya, envíe un mensaje al autor de este trabajo con su dirección de correo electrónico y sus preferencias temáticas y será incluido en la base de datos de nuestros próximos boletines informativos

CRITERIOS DE ATRIBUCIÓN DE RESPONSABILIDAD PENAL A LOS PRESTADORES DE SERVICIOS E INTERMEDIARIOS DE LA SOCIEDAD DE LA INFORMACIÓN

A mi hija Cristina

…cuando alguien del pueblo tuvo la oportunidad de comprobar la cruda realidad del teléfono instalado en la estación del ferrocarril, que a causa de la manivela se consideraba como una versión rudimentaria del gramófono, hasta los más incrédulos se desconcertaron. Era como si Dios hubiera resuelto poner a prueba toda capacidad de asombro, y mantuviera a los habitantes de Macondo en un permanente vaivén entre el alborozo y el desencanto, la duda y la revelación, hasta el extremo de que ya nadie podía saber a ciencia cierta donde estaban los límites de la realidad.

Gabriel García Márquez, *Cien años de soledad*

I. INTRODUCCIÓN

1. Origen y desarrollo de Internet

Cualquier aproximación a los delitos relacionados con las Tecnologías de la Información y la Comunicación, en cualquiera de sus formas de expresión, esto es, utilizando el ordenador como medio, objeto o finalidad de ataque, debe ir precedida de una reflexión sobre el impacto social de tales medios y su capacidad de transformación social; sobre las analogías y diferencias de dos espacios bien diferenciados, como son el lo que hoy conocemos como mundo real, por un lado, y realidad o mundo virtual, por otro. Debe efectuarse, asimismo, una valoración de futuro, siempre arriesgada en un sector como el tecnológico, sometido a una recurrente expansión horizontal pero también autoevolutiva, que permita fijar objetivos y, sobre ellos, construir el sistema de equilibrios entre libertad y control, si es que éstos no han de ser idénticos a los que conocemos en las relaciones clásicas. El camino, aquí, es el inverso al operado en la consecución y asentamiento de los derechos y libertades fundamentales en los países más desarrollados. En ellos, la conquista de espacios de actuación frente al Estado fue afirmada frente a los abusos del poder y el control absoluto sobre el ciudadano. En el campo de las Nuevas Tecnologías y particularmente en Internet, la máxima de libertad pierde terreno frente al aparato estatal, en un efecto paradójico. Por una parte, la pretensión de control absoluto desde los poderes Ejecutivos, redunda en perjuicio de garantías individuales, observadas ahora desde el punto de vista de sus homólogas en el mundo

real –privacy, intimidad, secreto de las comunicaciones, etc. Por otra, la reivindicación de una regulación expresa de Internet relaja el estado de naturaleza al que parecía dirigirse aceleradamente.

La inversión de la lógica evolutiva, según la conocemos en términos históricos en el ámbito clásico, debe buscarse en el origen mismo de Internet, la red por excelencia. Este sistema de interconexión surge como medida de contención de riesgos en el entramado de defensa norteamericano. La tensión derivada de la guerra fría y el crecimiento del arsenal nuclear multiplicaba el peligro de una confrontación bélica de consecuencias difíciles de evaluar. La interconexión de ordenadores de modo que la información logística y la relativa a ubicación de los sistemas de defensa pudiera encontrarse en todos y ninguno de los ordenadores distribuidos por el territorio, al mismo tiempo, permitía, en el peor de los casos, mantener intactas las vías de comunicación e información[1]. Relajadas las tensiones con la apertura del Este hacia modelos democráticos y de economía de mercado, la técnica puesta en marcha en la etapa anterior serviría para el intercambio de información entre entidades de carácter científico, básicamente, Hospitales y Universidades, aún dentro del ámbito territorial norteamericano. El sistema empleado para ello no se diferencia en gran medida al que subsiste en la actualidad –al menos, en el momento de redactar estas páginas- basado en el establecimiento de protocolos que permiten a las máquinas, por distintos que sean sus sistemas de funcionamiento interno, entenderse en el intercambio de datos[2]. De ahí surge el sistema de enrutación de los paquetes de información, básico en sus orígenes y que a medida que las conexiones fueron multiplicándose y los sistemas basados en entornos gráficos (no en comandos) evolucionando e implantándose de modo generalizado, derivó en el método alfanumérico que conocemos, en el que los números son sustituidos por letras que permiten no sólo localizar, sino identificar al usuario.

Hasta aquí, puede localizarse un nacimiento geográficamente localizado e igualmente expandido en el mismo territorio de origen. A la bondad del nuevo sistema fueron luego sumándose instituciones de otros países, sin que la extensión fuera acompañada de una cesión paralela de la gestión del modelo, íntegramente radicada en los Estados Unidos de América. En el origen, pues, el flujo de datos es *el pretexto para la libertad*; no es necesario el control, porque el uso ordinario sirve a un fin esencial: la coordinación de actividades científicas y militares. Aun sin

[1] De modo que ninguno de las máquinas controlara exclusivamente toda la información, sino que ésta, en su globalidad, pudiera ser accesible desde cualquiera de ellas. La red original, denominada *Arpanet*, fue creada en los años sesenta por el DARPA, denominación anglosajona en siglas del Servicio de Proyectos de Investigación Avanzada del Departamento de Defensa americano. Una información más detallada en **CASTELLS, M.,** *La era de la información. Economía, sociedad y cultura. Vol. I La sociedad red*, Traducción de Carmen Martínez Gimeno, 1997, pp. 32 y s.

[2] Baste apuntar aquí, de momento, que la única herramienta imprescindible para la interconexión es la incorporación en la máquina de un Protocolo universal de comunicaciones, el *Transfer Control Protocol* (TCP) que funciona, precisamente, sobre otro Protocolo, esta vez de red, el *Internet Protocol* (IP), lo que garantiza que la heterogeneidad de sistemas operativos que el mercado, la competencia y la investigación derivada de acciones I+D generan no constituya un obstáculo en la conectividad a Internet. Ampliamente sobre ello, **DE ANDRÉS BLASCO, J.,** *Internet*, Cuadernos del Senado, Serie Minor, nº 1, 1999, pp. 46 y ss.

eclosionar, los juicios de pronóstico sobre el futuro de un sistema tan singular sólo al alcance de potentes instituciones y fuera de la órbita de los particulares, carecen de relevancia: carecen de masa crítica suficiente, el medio es aún desconocido y la difusión de su contenido es limitada. Las instituciones universitarias no tardaron, no obstante, en convertirse en auténticos portales de acceso al sistema de ordenadores interconectados, y aunque de modo muy resumido, es la evolución del entorno gráfico, plasmado en las primeras versiones de los navegadores y la facilidad del sistema de enrutación entre máquinas, en cuanto sistema alfanumérico lo que cataliza la masificación en el acceso. El principio *pro libertate* aun no se resiente, pero la intuición sobre una posible extensión aún mayor de la que comienza a experimentarse remite al primer modelo de intervención, directamente imputable al gobierno americano. Se trata de la concesión a un órgano no gubernamental de la gestión de adjudicación de "direcciones" a las nuevas máquinas que pretendían unirse al nuevo modelo, todavía emergente. En definitiva, se trata de un método invasivo de la capacidad normativa de los diversos Estados que participan en el sistema a través de instituciones y particulares nacionales. El sistema de máquinas en red se define, precisamente, por la descentralización de la información; por la no existencia de máquinas centrales de las que dependa el resto. Sin embargo, la capacidad de organización del sistema tiene un único y exclusivo centro de poder al que sumarse o del cual desconectarse. Mas, en último término, constituye la primera medida normativa que regula la libertad absoluta imperante en el medio.

En este paisaje de libertad, entendida como ausencia de regulación específica, tanto respecto al medio en sí como al nuevo sistema de relación que genera, simultáneamente, surgen los primeros conflictos que revelan que la libertad en términos puros no es tampoco propugnable en la Red. La máxima de atribución *first come, first served (prior tempore, potior iure)*, por ejemplo, empleada en la asignación de dominios, es decir, de nombres mediante los que localizar una máquina y, en ella, un servicio determinado[3], genera colisiones de intereses que aún hoy no han podido ser superados mediante un sistema que satisfaga todos los intereses concurrentes pero, sobre todo, que guarde el equilibrio entre las diversas concepciones sobre el contenido/fin de Internet. La expansión cuantitativa de la Red, además, revela usos que en poco se parecen ya a los originarios. Cuanto mayor es el número de interesados en la participación en el sistema, mayor es la probabilidad de conflictos intersubjetivos.

Pero además, como con acierto se ha señalado, la denominada *Sociedad de la Información* que nace al abrigo de las tecnologías -no sólo de carácter telemático, también de otro tipo como el cable o la televisión digital- transforma las relaciones sociales y jurídicas de un modo incontestable e impresionante[4]. Los ejemplos que podrían concurrir ahora son múltiples y tal vez sea conveniente apuntarlos sin orden aparente. La confidencialidad de los mensajes mediante sistemas de encriptación

[3] Sobre este extremo, con detalle, cfr. *Infra*.

[4] La idea en general, se desarrolla con amplitud en **CASTELLS, M.,** *La era de la información, op. cit., passim. Vid.*, entre otros, **FERNÁNDEZ ESTEBAN,** *Nuevas Tecnologías, Internet y Derechos Fundamentales*, 1998, p. XXIII; **CAPELLER, W.,** *Not such a Neat Net. Some comments on virtual criminality*, 2000, p. 3

invulnerables y la posibilidad de certificar la identidad del emisor de modo tanto o más seguro que mediante los sistemas actuales de certificación (fe pública), ejerce de catalizador en la reflexión sobre el sistema democrático mismo y el sistema de elección de los representantes. Se habla así de *democracia electrónica*, queriéndose subrayar con ello el nacimiento de un nuevo modo de concebir la participación ciudadana, no sólo en la elección de los representantes, sino en la toma de decisiones por parte de éstos. La propia especulación sobre el particular genera la necesidad de estudios sociológicos sobre la repercusión que un sistema de participación cotidiano y directo conlleva en el modo de realización política de los principios básicos del Estado democrático. Y si los propios fundamentos del Estado se remueven con la irrupción de tecnologías capaces de comunicar todo el planeta en tiempo real y de acceder a cualquier género de información, las relaciones sociales primarias sufren el mismo efecto. En el ámbito laboral, la posibilidad de ejercer la función, pública o privada, lejos del habitual puesto de trabajo, sin necesidad de desplazamiento, abre un nuevo paradigma de las relaciones laborales, donde apremian las preguntas sobre los nuevos modelos de sindicación, control del desempeño de la actividad laboral (*Enforcement*), régimen de seguridad social, determinación de nuevas enfermedades laborales, compatibilidad de determinadas situaciones de incapacidad laboral según el sistema clásico con el desarrollo de la actividad desde el domicilio[5]. Del mismo modo, el sector empresarial se ve abocado a la adaptación tecnológica, hasta el punto de que la misma transforma los esquemas clásicos de organización, *marketing* e intercambio de productos. La supresión de intermediarios en la distribución, la comunicación *on-line* entre empresas (*Bussiness to Bussiness*, simbolizado como *B2B*) o entre particular y empresa, genera nuevas estructuras organizativas y, al tiempo, nuevos ámbitos necesitados de tutela primaria en el sostenimiento del nuevo modelo organizativo: trafico de datos, seguridad en las transacciones comerciales, prevención de daños en los centros de comunicación individual y colectivos de la empresa (*v.gr.* frente a programas informáticos como los virus, gusanos, etc.)[6].

2. La interpretación de la Sociedad de la Información desde el Derecho

Hasta aquí se comprueba cómo la evolución tecnológica permite un incremento cualitativo de la calidad de vida; pero, del mismo modo que se constatan cambios en la estructura y desarrollo social y económico, al tiempo se abre la puerta a nuevas formas de perjudicar los legítimos intereses ajenos, bien sean individuales o colectivos[7]. La cuestión entonces radica en determinar el alcance de los cambios y efectuar prognosis ponderadas sobre los que vendrán y los riesgos que llevarán

---

[5] *Vid.*, ampliamente, **THIBAULT ARANDA, J.,** *El teletrabajo. Análisis jurídico-laboral*, 2000, p. 125; Un interesante planteamiento de estas cuestiones, también, en **LEONES SALIDO,** *Razones urgentes para una regulación del teletrabajo en España*, en AJA, nº 431, 23 marzo 2000, pp. 3 y ss.

[6] *Vid*, en general, el informe de la KPMG's Assurance & Advisory Services Center, **VVAA** *E-Commerce and Cyber Crime: New Strategies for Managing the Risks of Exploitation*, junio 2000, en http://www.us.kpmg.com/assurance/New_strat/pdf/new_strat.pdf, pp. 2 y ss., última revisión, 22 septiembre 2000.

[7] Reflexión genérica que, en relación con la denominada *sociedad de riesgos* o *sociedad post-industrial* puede verse en **SILVA SÁNCHEZ,** *La expansión del Derecho Penal. Aspecto de la política criminal en las sociedades postindustriales*, 1999, p. 22.

aparejados, como punto de partida en la fijación de intereses fundamentales en el nuevo marco de relación. Sólo así pueden aventurarse conclusiones sobre la necesidad de intervención del Derecho Penal en un sector emergente y de apariencia caótica, en el que aun no han penetrado con decisión los instrumentos primarios de regulación, administrativo, civil, mercantil, etc. Y sólo así sabremos hasta que punto las normas penales existentes son suficientes o reclaman una tan urgente y demandada modificación y adaptación a las tecnologías existentes[8]. Pues, unas veces, las normas penales son suficientemente amplias para acoger lo que no son sino manifestaciones más sofisticadas de lo que ya se conoce y otras tantas, en cambio, el principio de legalidad no permite una extensa apertura hacia la absorción de nuevos comportamientos difícilmente conciliables con el ámbito de tutela de la norma; y no son pocas aquellas en las que la novedad de los intereses a tutelar y la violencia de los ataques -confirmado en el estudio criminológico- reclaman la presencia de normas penales específicas. Una respuesta que, a la luz de la brutalidad de los medios –privación de libertad y/u otros derechos-, exige una equilibrada ponderación de intereses con el consiguiente retraso de las normas sobre los hechos.

Ejemplos de todo ello no faltan en la denominada criminalidad informática. El Derecho tutela la vida en todas sus manifestaciones, y de ahí que la cooperación en la muerte de otro a través de medios informáticos no suscite dudas sobre su punición y, caso de haberlas, el debate giraría en torno al resultado y no a los medios o, a lo sumo, a las posibilidades de imputación del resultado al riesgo generado o incrementado mediante el empleo de medios informáticos y, singularmente, telemáticos. Sobre el segundo espectro de problemas planteados, el Código penal de 1973 permitió que la doctrina científica y la jurisprudencia debatieran ampliamente sobre la posibilidad de subsumir en el delito clásico de estafa conductas que se realizaban a través de medios informáticos, hipótesis rechazada por las plumas de corte clásico, sobre la base de una flagrante lesión del principio de legalidad: la máquina no puede ser engañada, ni sufrir error. Por último, la evolución de bienes jurídicos como la intimidad ha permitido el desarrollo de aspectos del mismo que, como el *habeas data*, eran desconocidos por el legislador penal y que, aún con retraso, han sido introducidos en el Código Penal para su mejor tutela[9].

---

[8] Se ha sugerido, incluso, que las conductas criminales en el ámbito de las comunidades virtuales, lesionan intereses del ciudadano en cuanto miembro de la comunidad virtual (*citizennet*), refiriendo entonces el análisis del impacto de las conductas criminales sólo a la afectación de las pautas de comportamiento como ciudadano red; sobre ello, cfr. **CAPELLER, W.,** *Not such a Neat Net, op. cit.*, pp. 5-6.

[9] En este contexto, y como patrón de medida, el último informe del Ministerio del Interior sobre los índices de delincuencia tecnológica arroja un saldo preocupante, según se observa en la fuente, consultada por última vez el 9-01-01 en http://www.expansiondirecto.com/2001/01/09/normas/segurida.pdf. Únicamente el Cuerpo Nacional de Policía, a través de la Unidad de Delincuencia Tecnológica investigó durante el año 2000, 581 supuestos asuntos relacionados con conductas lesivas en Internet, en principio reconducibles a los tipos penales existentes. De ellos, la difusión de pornografía infantil ocupa el primer lugar, con 354 actuaciones, al que le siguen las defraudaciones, en múltiples modalidades (mediante empleo de tarjetas de crédito falsas o sustraídas, en subastas virtuales, etc), que provocaron un total de 71 intervenciones. La difusión en red de contenidos lesivos del honor de las personas (calumnias e injurias) ocupa un lugar destacado en la actuación policial con 61 intervenciones, consistiendo el reto en la investigación de ataques contra la propiedad intelectual (24), estupefacientes (5), revelación de

Pero la tendencia expansiva del Derecho Penal postindustrial, de cuya inercia no está a salvo ningún país desarrollado, por supuesto tampoco España o cualquiera de los que integran la Unión Europea, también se manifiesta en relación con los delitos informáticos. Frente a la inicial situación de anomia y libertad autocontrolada, se ha generado con posterioridad la imagen de la informática como fuente permanente de peligro, cuyo control sólo puede ser asumido desde la intervención de las instituciones democráticas. Siendo cierta la segunda premisa –en cuanto las bases del funcionamiento social deben ser objeto de reflexión política y de la acción legislativa- la primera debe ser matizada. La noción de riesgo es siempre inherente al interés que trata de salvaguardarse[10] y, consecuentemente, sólo una vez definido el interés puede delimitarse el nivel de riesgos que el mismo puede soportar y aquellos cuya peligrosidad para su mantenimiento requieren técnicas de intervención jurídica, no siempre, ni necesariamente, de carácter penal. La reflexión en este ámbito es, en cambio, inversa, y no carecería de fundamento afirmar que la colosal capacidad de control de los medios informáticos, el denominado *poder informático*, hoy más amplio que en su acepción original, se encuentra detrás de las propuestas internacionales de armonización, que se presentan como necesarios instrumentos de control riesgos y prevención de la realización del delito informático, sacrificando un amplio elenco de garantías; garantías que lo son formales, materiales, generadas por analogía o simplemente asentadas en los usos que la comunidad de usuarios conforma con su práctica diaria. Así, el borrador de Propuesta del Consejo de Europa de 27 de abril de 2000, asume en cada uno de los ámbitos de afectación políticas de máximos en las que la cesión de garantías sobre los poderes públicos ha sido puesta de manifiesto desde una multiplicidad de instituciones[11]. Se planea así la cesión a las autoridades administrativas de parcelas de autogobierno en el uso de las tecnologías, como el acceso no autorizado a máquinas, a los solos efectos de la investigación criminal; la moralización de las tendencias sexuales con ocasión del fenómeno Internet. En este último sentido, la constatación del incremento de la difusión de pornografía infantil en las redes telemáticas se aprovecha para extender el concepto pornografía y el de su atributo, infantil, hasta estadios previos completamente

secretos (3) e intrusiones en sistemas ajenos sin consentimiento de su titular (31). A los datos anteriormente aportados deben sumarse las distintas intervenciones de la Unidad de Alta Tecnología de la Guardia Civil y las operadas por otros Cuerpos Autonómicos, como la Unidad de delincuencia informática de los Mossos d'Esquadra de Cataluña.

[10] Expresión, según recuerda **SILVA SÁNCHEZ,**,*La expansión del Derecho Penal*, *op. cit.*, p. 32, de "una ponderación de los costes y beneficios de la realización de una determinada conducta".

[11] En efecto, mediante escrito de 13 de octubre de 2000, la *Global Internet Liberty Campaign* integrada por un conjunto de agrupaciones de carácter civil con peso específico en los procesos de toma de decisiones, como la *American Civil Liberties Union*, o el *Electronic Privacy Information Center (EPIC)*, entre otros, manifestaron su desacuerdo con la redacción original del Borrador de 27 de abril, justo en el momento en que veía la luz la segunda versión de la Propuesta, hecha pública el 2 de octubre de 2000 inmediatamente rectificada en su tercera versión, de 19 de noviembre de 2000 ya sustituida por la 25ª de 9 de enero de 2001 (texto en inglés en http://conventions.coe.int/treaty/EN/projects/cybercrime24.htm). En el documento emitido se pone de manifiesto la política de control excesivo seguido en el borrador, y que se observa principalmente en la obligación de registros a los proveedores de servicios, la amplia acepción del concepto de dispositivos ilegales, la expansión del concepto "propiedad intelectual", etc. Puede consultarse el texto íntegro de la propuesta en: http://www.gilc.org/privacy/coe-letter-1000-es.html.

alejados de la libertad sexual y próximos a concepciones preñadas de carga moral sobre las tendencias sexuales, alcanzando así la criminalización de la posesión para el consumo personal o la difusión de pseudo-pornografía o de pornografía pseudo-infantil, ampliándose igualmente el número de operadores a los que atribuir cualquier tipo de responsabilidad (penal) por su aportación directa o indirecta al hecho. La previsión de sanción penal en el seno del intrusismo informático para las conductas de pura tenencia de tecnologías de doble uso, o la obligación de entrega de llaves privadas de los sistemas de cifrado, son sólo algunos de los ejemplos de la tendencia expansiva en la utilización del Derecho penal en esta materia, aprovechando la incertidumbre que rodea el vertiginoso cambio tecnológico. En esta dinámica, los diversos Estados nacionales y organizaciones gubernamentales supranacionales juegan un papel relevante, en la medida en que la socialización en el uso de las Tecnologías de la Comunicación y la Información significa, al margen de los riesgos objetivos, una pérdida de control sobre la planificación social, política y económica y de ahí el interés en presentar determinadas conductas como ataques intolerables a la convivencia y que en realidad son tan solo la punta de lanza de la necesaria reflexión previa sobre el uso de las TIC[12].

3. El rol de los intermediarios

La incertidumbre que genera la expansión de Internet como medio aún cargado de un cierto grado de anarquía en su gestión, se proyecta igualmente sobre el papel que desempeñan los distintos operadores de la Red. En cambio, el desarrollo actual de la sociedad de la información, apoyada en la utilización de la TIC, reclama reglas de juego precisas en el intercambio de datos, en general, y en el flujo de datos entendido, además, como prestación de servicios, actividad económica, negocio, etc. El marco de actuación debe ser preciso y los límites en la actuación de los operadores también, no sólo como garantía de los consumidores cuando se trata de operaciones de carácter comercial, sino más ampliamente, de la totalidad de bienes jurídicos que pueden entrar en colisión y del funcionamiento eficaz del sistema mismo de comunicación. El régimen de responsabilidad de los distintos operadores de la sociedad de la información debe ser, en consecuencia, diáfano, y evitar así que los problemas derivados de la innovación tecnológica se acumulen a la incertidumbre jurídica. Desde una perspectiva como la apuntada, el régimen de responsabilidad de los intermediarios de la Sociedad de la Información ha sido objeto de atención por

[12] La situación, no obstante, tiende a cambiar en los últimos tiempos, de manera que son ya múltiples las vías de reflexión abiertas en relación con la sociedad de la información, los riesgos que presenta, las barreras preventivas y las vías primarias de contención de riesgos. Desde el Plan de Acción adoptado por el Consejo JAI en mayo de 1997 para combatir la delincuencia organizada y en el que se preveía la elaboración de un informe sobre la delincuencia informática, hasta el Plan de Acción *e*Europa 2002, mediante el que se emprenden acciones para aumentar la seguridad en la red y establecer un enfoque coordinado de la delincuencia informática; el Foro de la UE, surgido a raíz de la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, con la finalidad de debatir las necesidades inherentes a una Sociedad de la Información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos; o, por último, la aprobación de la aprobación por el Consejo JAI de la UE en marzo de 1998, de los 10 principios básicos para combatir la delincuencia informática sugeridas por el G8, especialmente preocupado en la materia.

las instituciones con capacidad para marcar el régimen jurídico de las redes telemáticas, hasta ahora centradas en los sistemas clásicos de comunicación y, sectorialmente, en algunas de las modalidades más recientemente importadas, como la comunicación por cable o satélite. Así, desde los iniciales procesos de reflexión sobre la autorregulación del sector[13], finalmente el 8 de junio de 2000 el Parlamento Europeo aprobaba la *Directiva 2000/31/CE, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior*[14], actualmente en proceso de trasposición al Derecho español[15]. La especial arquitectura de Internet determina que las relaciones entre los distintos intervinientes en la comunicación, la posición de dominio o no de cada uno de ellos, la diversa capacidad de almacenamiento o utilización posterior de contenidos ajenos, reclamen reglas específicas para determinar el grado de responsabilidad que puede alcanzar cada uno de ellos cuando alguno de los intereses en juego entra en situación de riesgo. Por ello, la determinación de los límites a la responsabilidad penal en el seno de Internet constituye hoy uno de los temas de mayor interés en el binomio Derecho Penal-Nuevas Tecnologías. La circulación en red de información que excede los límites de las libertades fundamentales (libertad de expresión e información) para atacar algunas otras de igual importancia (honor, libertad sexual, seguridad), ha despertado desde un primer momento la alarma social en la que, como se ha señalado, los medios de comunicación juegan un papel de extraordinaria importancia en el efecto amplificador[16] tanto de la relevancia de ciertas conductas lesivas como del grado de responsabilidad exigible a los operadores. De cualquier forma, contenidos sexuales indiscriminados y masificación de la información sobre los riesgos han sido, en primer término, los ingredientes fundamentales para proceder al análisis con trazo fino del reparto de responsabilidades en el orden penal.

La exigencia de responsabilidad penal a los prestadores de servicios de la sociedad de la información, especialmente a quienes operan en el ámbito de Internet, a través de cualquiera de los medios técnicos que lo permiten (cable, teléfono, etc.) no está, sin embargo, exenta de preocupación política, en general, y político-criminal en

---

[13] Ampliamente, **FERNÁNDEZ ESTEBAN,** *Nuevas Tecnologías, op. cit.* pp. 102 y ss.; cfr., también, las referencias en **DE MIGUEL ASENSIO, P. A.,** *Derecho Privado de Internet, op. cit.*, pp. 489 y s. Sobre la denominada *Autorregulación regulada*, híbrido utilizado para una mayor vinculación de la autorregulación de los proveedores, cfr., **WIDE, I.,** *Legal Regulation, Law Enforcment and Self-regulation. A new Alliance for fighting Illegal and Harmful Contents on the Internet*, Lecture for the Conference on "Diritto Penale dell'informatica nell'epoca di Internet", pp. 19 y ss. (este trabajo se halla actualmente en prensa en, la Editorial CEDAM, bajo el mismo título de la conferencia citada)

[14] En adelante, Directiva del Comercio Electrónico. DOCE L 178/1, de 17 de julio de 2000.

[15] En la actualidad el Ministerio de Ciencia y Tecnología trabaja en el Anteproyecto de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, cuya última versión es de 18 de enero de 2001, texto que puede consultarse en http://www.setsi.mcyt.es/

[16] Sobre el papel de los medios de comunicación, junto a otros factores, en la tendencia expansiva del Derecho penal y la asunción por el colectivo del sentimiento de necesidad de intervención masiva mediante esta herramienta jurídica, *vid.*, **SILVA SÁNCHEZ,** *La expansión del Derecho Penal, op. cit.*, pp. 27 y ss.; También en este sentido, particularmente referidos al ámbito de la responsabilidad de los operadores de Internet, **WIDMER, U/BÄHLER, K.,** *Strafrechtliche und aktienrechtliche Haftung von Internet Providern*, Computer und Recht, 1-12, 1996, p. 178; **PICOTTI, L.,** *Fondamento, op. cit.*, p. 380.

particular. Los operadores, tanto aquellos que proveen el acceso al servicio cuanto aquellos que facilitan la difusión de contenidos alojados en sus servidores, cumplen indubitadamente una función jurídico-social y económica de primera magnitud[17]. En el primer sentido, como facilitadores de la libre difusión del pensamiento y las ideas, contribuyendo de este modo a una mayor distribución del conocimiento y acceso a la información, en general. Desde la segunda perspectiva, es innegable también el importante papel económico que desempeñan los servicios telemáticos en la denominada "nueva economía", por lo que el definitivo esclarecimiento de los límites en que debe desenvolverse la actividad del prestador del servicio es singularmente importante, en cuanto muestra en positivo los fines de política general perseguidos a través de la utilización de nuevas tecnologías. En esta tarea, además, la depuración de responsabilidades debe enfrentarse a la distinción de la multiplicidad de operadores con que cuenta Internet. Evidentemente, ningún problema especial plantea la autoría de conductas lesivas realizadas en el ámbito de la red de redes[18]. En cambio, los problemas se suceden cuando trata de averiguarse la relevancia penal de las acciones u omisiones de otros intervinientes en la comunicación, como es el caso de los *Access Providers*[19] y los *Service Providers*[20] (en adelante Access/Service providers, según el caso). ¿Deben responder proveedor de acceso y de servicio jurídico penalmente por los contenidos ilícitos ajenos?; y, en todo caso, debe responder el proveedor de acceso igual que aquél que difunde la información ilícita o aquél que desde la red piratea el *software* de un tercero?. ¿Y el proveedor de servicios?.

No faltan desde luego los casos en que se ha planteado la responsabilidad penal del proveedor de servicio. En mayo de 1998, el Tribunal Superior de Munich, en lo que hasta ahora constituye la principal referencia empírica sobre la materia, condenaba a un proveedor alemán a la pena de dos años de prisión por difusión de pornografía (delito según los casos en Alemania) a título de autor, a pesar de que el sujeto en cuestión no era autor material de las noticias sobre pedofilia difundidas –gracias a su

---

[17]**SIEBER, U.,** *Strafrechtliche Verantwortlichkeit (I), op. cit.*, p. 2; **PICOTTI, L.,** *Fondamento, op cit.*, pp. 378 y s.; **ZENCOVICH, Z.,** *La pretesa estensione alla telematica del regime della stampa*, en http://www.beta.it/edit/zencovich.html, p. 1;**FORNASARI, G.,** *Il ruolo della esigibilità nella definizione della responsabilità penale del provider*, en "Diritto penale dell'informatica nella epoca d'Internet", texto de la ponencia presentada en el Congreso del mismo nombre celebrado en Trento, Italia, los días 14 y 15 de abril de 2000, p. 3 (actualmente en prensa).

[18] Aquí, por problemas de autoría debe entenderse, en sentido estricto responsabilidad *a título de autor* por los contenidos propios.

[19]Por *proveedor de acceso* debe entenderse el operador técnico que únicamente facilita al cliente la conexión a un entorno de red. Dicha conexión puede ser en red local (LAN o *Local Area Network*), o a través de servicios telefónicos (analógica o digitalmente –RDSI-). En ocasiones el proveedor de acceso ofrece, además, determinados servicios (alojamiento de páginas en formato Web, grupos de noticias propios, coreo electrónico, etc). En tal caso asume la doble condición de proveedor de acceso y de servicios.

[20]El *proveedor de servicios* es aquél que además de facilitar (en su caso) el acceso al entorno de red, ofrece contenidos propios o crea los medios para que los contenidos ajenos puedan ser accesibles al resto de la comunidad. Dicha infraestructura puede consistir en alojamiento de páginas en formato hipertextual (sistema web), grupos de noticias propios –conocidos como *news* en entorno *usenet*-, creación de cuentas de correo electrónico individuales, etc. Normalmente la canalización de esta ofertase efectúa a través de un ordenador o conjunto de ellos denominado *servidor*.

servidor- bajo el grupo de noticias (alt.pedophilia.sex). El administrador del servicio era responsable de la empresa *Compuserve Deutschland*, filial al 100% de la matriz *Compuserve America*, cuyo servidor general radicaba en la Universidad de Ohio. El administrador del sistema disponía, pues, de la exclusiva de acceso a los contenidos que la matriz difundía desde Estados Unidos, mas no se hallaba técnicamente capacitado para cerrar el acceso sólo a uno o varios de los contenidos ofrecidos por la matriz[21]. En esta compleja tarea, algunos países han tratado unilateralmente, con mayor o menor fortuna, los problemas derivados de la responsabilidad de los proveedores de acceso y servicios. En Alemania, la *Teledienstgesetz* Ley de Servicios Telemáticos[22], contiene en su § 5 las reglas para la determinación de la misma, diferenciando entre proveedores de acceso y servicio. Para los primeros, la responsabilidad queda formalmente excluida, según se establece en el párrafo tercero. En cambio, cabe diferenciar dos supuestos diferentes en relación con los proveedores de servicio. De una parte, son siempre responsables, como no podía ser de otro modo de los contenidos propios alojados en su servidor, es decir, aquellos contenidos con los que tratan de captar la atención del usuario, ventilándose la responsabilidad conforme a las disposiciones generales. De otra, en los casos en que el servidor hospede contenidos ajenos, el proveedor del servicio será responsable de los mismos siempre que los mismos: 1) hayan sido alojados para su utilización; 2) haya tenido conocimiento de ellos; y 3) le sea técnicamente posible impedir su utilización por el usuario[23].

A falta de normas penales específicas sobre el particular, la delimitación de la responsabilidad de los Access-Service Providers se ha ensayado desde la aplicación de las categorías e institutos generales de la disciplina y tomando como referente las específicas normas que regulan la responsabilidad general y específicamente jurídico penal en otros ámbitos de la comunicación, como la prensa, radio, televisión, cable, o satélite. Desde el primer punto de vista, las vías que pueden llegar a ofrecer instrumentos dogmáticos satisfactorios para el análisis de posibles responsabilidades en la actuación del proveedor de servicios que aloja en su servidor contenidos ilícitos se reducen prácticamente al empleo de la cláusula de comisión por omisión del

[21]Como lo demuestra el hecho de que, al primer requerimiento de la policía para la suspensión de pedophilia.sex, el autor suspendió de inmediato dicho grupo de noticias pero, al tiempo, más de trescientos grupos más que se hallaban ligados al mismo. Sobre ello *vid* el comentario efectuado a la Sentencia por **SIEBER, U.,** *Multimedia und Recht*, Cuaderno 8, pp. 429 y ss., 1998, actualizado a 19 de agosto (versión en inglés bajo el título "*The Compuserve Judgment of the local Court Munich dated May 28, 1998*). *V.*, asimismo, otros ejemplos de la jurisprudencia suiza e italiana en **PICOTTI, L.,** *Fondamento e limite*, *op. cit.*, p. 385.

[22] *Teledienstgesetz*, contenida en el Art. 4 de la legislación marco en materia de telecomunicaciones, la *Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz –IuKDG-*)

[23]En los estados Unidos de América, la *Decency Act* del Congreso, aprobada en 1996, proclamaba la responsabilidad indiscriminada del proveedor (de acceso o servicio) de todos los contenidos ilícitos que circularan bajo su radio de influencia técnica. La Ley fue declarada inconstitucional por el Tribunal Supremo americano, dos años después, por vulneración de la libertad de expresión e información.Sobre ello, de especial interés, **SIEBER, U.,** *Die Rechtliche Verantwortlichkeit im Internet. Grundlagen, Ziele und Auslegung von Paragraph 5 TDG und paragraph 5 MDStV*, en http://www.jura.uni.wuerzburg.d/lst/sieber/mmr/5mmrbei_dt.HTM También en Multimedia und Recht, 2, 1999, con independencia de los comentarios que serán efectuados más adelante.

artículo 11 CP y, dados los límites de legalidad a los que la aplicación de la comisión por omisión se somete, a la participación criminal en el delito. Son precisamente los requisitos inherentes al artículo 11 CP los que motivaron en un primer momento la búsqueda de analogías entre la actuación de los prestadores de acceso y servicio en Internet y la desarrollada por los profesionales de medios de comunicación "tradicionales" o, en otras palabras, más ampliamente regulados.

La adjudicación de responsabilidades por contenidos ajenos trasciende a la política general, y las dificultades y el coste económico inherente a la adopción de medidas técnicas eficaces y la asunción de posiciones genéricas de garantía sobre la licitud del tráfico de datos circulante repercuten en la configuración de los servicios telemáticos, pues obligando a los operadores a la asunción de funciones con capacidad de afectación de bienes jurídicos ajenos, no solo se presume una especial cualificación en el agente que lo capacitaría para efectuar una censura previa de contenidos que, en función de las circunstancias de presión social puede significar una desmesurada limitación de la libertad de expresión[24]; sino que, igualmente, se condiciona el mercado de los prestadores de servicios concretando los requisitos de capacitación de los mismos. El flujo de datos, por otra parte, se ve sometido a límites técnicos cuya posible realidad puede ser poco menos que utópica, pues el control de la información depende en último término de la instalación de sistemas de rastreo de la información que puede considerarse ilícita o lesiva de intereses ajenos, cuando no, simplemente, irreal[25]. Es conveniente, en consecuencia, analizar los mecanismos técnicos con que actualmente opera el intercambio de información en red y el rol que en función de ello desempeñan cada uno de los operadores o prestadores de servicios y el control que desempeñan sobre los procesos de transmisión de datos[26], para contrastar posteriormente la aptitud de la legislación vigente para disciplinar su régimen de responsabilidad y las propuestas de Derecho Comparado y europeo sobre el particular.

II. COMUNICACIÓN TELEMÁTICA Y SERVICIOS DE INTERNET. CUESTIONES TÉCNICAS

1. La comunicación vía Internet

[24]**FORNASARI, G.,** *Il ruolo della esigibilità, op. cit.*, p. 4. Precisamente, el autor señala como uno de los mayores condicionantes del establecimiento de responsabilidades penales que exigir a los proveedores de contenidos, el que "se pueda consentir una limitación, proveniente además de un sujeto no institucional, a la libre circulación de las ideas y las opiniones; delimitación que se presenta siempre peligrosa en ordenamientos democráticos, incluso cuando se trata de ideas u opiniones de contenido desagradable o repugnante". *Vid.*, también, **ZENCOVICH, Z.,** *La pretesa estensione alla telematica del regime della stampa*, en http://www.beta.it/edit/zencovich.html, p. 2; **PICOTTI, L.,** *Fondamento, op. cit.*, p. 380.

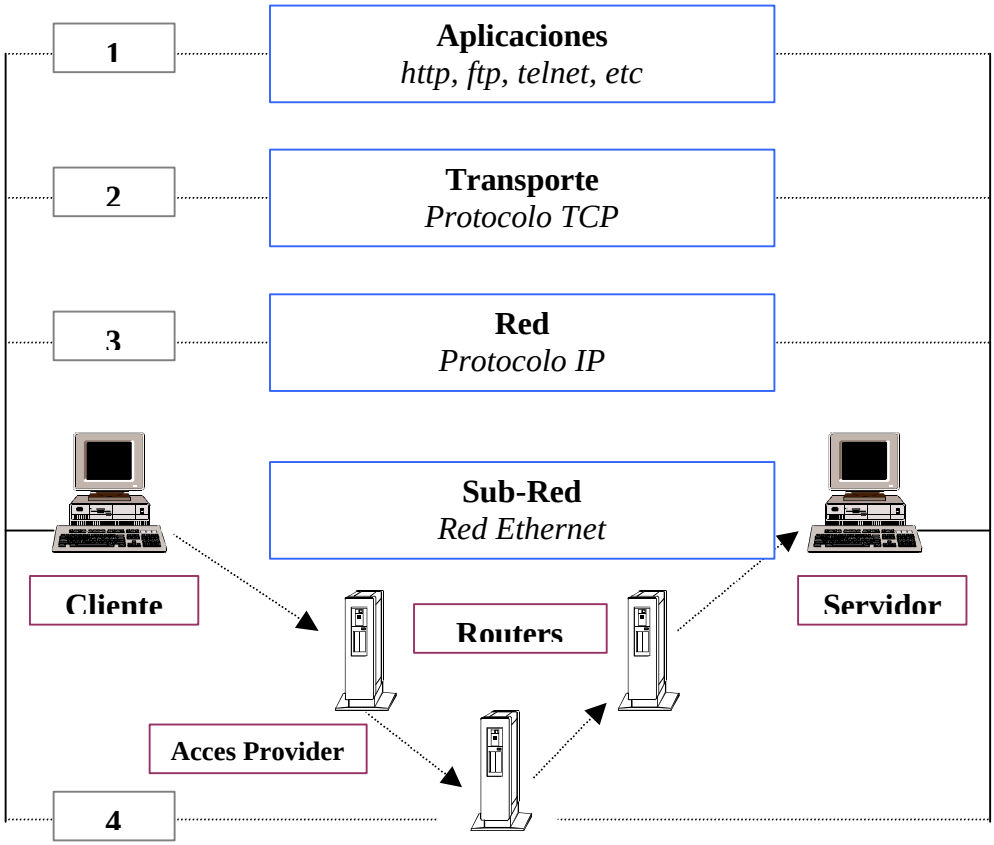
[25]Cfr., sin perjuicio de que posteriormente será objeto de análisis detallado, **SIEBER, U.,** *Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I)*, en http://www.jura.uni-wuerzburg.de/sieber/Kontrolle/KONTROLLE_DT(1).HTM, pp. 8 y ss.; **SEMINARA, S.,** *La responabilità penale degli operatori su Internet*, en "Il Diritto dell'Informazione dell'Informàtica", nº 4-5, 1998, pp. 755 y ss.; **WIDE, I.,** *Legal Regulation, op. cit.*, pp. 5 y s.

[26] Así, **SIEBER,** *Kontrollmöglichkeiten (I), op. cit.*, p. 5.

A diferencia de lo que sucede en una conexión telefónica, que establece una comunicación directa entre el punto de origen y destino, sin intermediarios, la conexión en las redes telemáticas utiliza un sistema de fragmentación o conmutación en paquetes de la información (Kbytes) que son tratados individualmente y procesados en lo que se denominan *nodos de transmisión* o ***Routers***. Esta diferencia entre la conexión telefónica y la telemática, lejos de constituir una anécdota de carácter exclusivamente técnico, desempeña un rol esencial en la materia objeto de análisis. El hecho de que la información deba discurrir, en el modo técnico que a continuación se desarrollará, por diversos nodos en los que el tráfico de información, los paquetes en los que se fragmenta el contenido de lo comunicado, es almacenado y procesado constituye la fuente de los interrogantes sobre el grado de responsabilidad de cada uno de los intervinientes en el proceso de comunicación. Lo que no sucedería, en principio, con la pura comunicación telefónica, donde la información viaja en un único paquete, sin intermediarios, entre el punto de origen y el destino final de la misma.

El funcionamiento de la comunicación en las redes, para su comprensión, requiere diferenciar cuatro niveles básicos, cada uno de los cuales ejecuta o permite la ejecución del conjunto de secuencias necesarias para el correcto envío y recepción de los datos, según el gráfico[27]:

[27] Sobre el gráfico y su desarrollo, de especial interés, **GRIERA, J. I.,** *Seminario de seguridad en Internet*, en Materiales del Curso de Seguridad en Internet, impartido por el es-CERT, 1999.



1. En el nivel **aplicaciones**, mediante un Lenguaje específico (http; ftp; telnet[28]; etc.), el cliente trata de enviar una información al servidor. Utilizando para ello cualquiera de las aplicaciones a través de las cuales obtener un servicio específico: mensaje de correo electrónico, petición de conexión a una página web, transferencia de archivos, etc.

2. Para que esta operación sea viable, las máquinas utilizan el siguiente nivel, es decir, el de **transporte**, en el que una vez efectuada la orden de comunicación específica del nivel **aplicaciones**, entra en funcionamiento el Protocolo de Control de la Transferencia ***(TCP: Transfer Control Protocol)***. Mediante este protocolo se garantiza la integridad electrónica del envío de información, dado que su principal utilidad consiste, precisamente en recoger la orden y fragmentarla en paquetes de información, numerando cada uno de ellos. De este modo, el ordenador que hace las veces de servidor sabrá, en el mismo nivel, si la información es completa o si falta

[28] Sobre el sentido de este tipo de aplicaciones, cfr. *Infra*.

algún paquete, en cuyo caso, y a través del mismo nivel de red, reclamará a la máquina cliente que vuelva a efectuar la petición.

3. El Protocolo de control de la transmisión viaja (envía los paquetes) sobre el tercer nivel, es decir sobre el nivel de **red**, que a su vez utiliza un protocolo específico, denominado Protocolo de Internet ***(IP: Internet Protocol)***. Es decir, ***TCP*** viaja sobre ***IP***, lo que gráficamente se acostumbra a designar como ***TCP/IP***. El Protocolo de Internet permite conocer al servidor, en este caso, cuál o quien es el destinatario final de la información, en función de la dirección impresa que lleva la máquina cliente así como la dirección que dicha máquina reclama. Por último, en relación con los niveles red y **sub-red**, si se tiene en cuenta que en éste se encuentran las conexiones concretas y los ***Routers*** que escuchan los paquetes de información numerados por el nivel de transporte (***TCP***) cobra mayor sentido el nivel de red: el Protocolo ***IP*** posibilita al ***Router*** del nivel sub-red su función en el nivel inferior y definitivo, pues al llevar ***IP*** una dirección impresa, interconecta los ***Routers*** entre sí, para que cada uno pueda ir enviando sucesivamente los paquetes de información[29]. El IP, en definitiva, es una sucesión de números que identifican tanto la máquina cliente como la del servidor al que ésta reclama un servicio determinado. Como sucesión numérica el IP contenía una dificultad intrínseca para la expansión de Internet como sistema, consistente en la complejidad numérica asociada a los servicios para ser memorizada.

Surge así el Sistema de Nombres de Dominio (***Domain Names***) que consiste en la conversión del IP numérico en una sucesión alfanumérica que facilite, como recurso mnemotécnico la asociación del IP con el destino elegido en el *host* por el usuario (cliente). Para facilitar dicha conversión en las dos vías (alfanumérica, para la mejor comprensión del usuario y numérica, pues el sistema continúa utilizando números en la lectura del origen y destino de la comunicación) fue creado el denominado **DNS**: ***Domain Name System***, el Sistema de Nombres de Dominio. Los nombres de dominio, por lo tanto, se limitan a facilitar la conexión de los usuarios de la red; pretenden su identificación en la misma, pero no su distinción. El Nombre de Dominio se estructura en tres niveles.
El ***Top Level Domain Name*** o Nombre de Dominio de Primer Nivel indica la localización territorial o genérica del servicio buscado. Se subdivide, pues, en dos clases, aunque funcionalmente idénticas: TLD territorial y TLD genérico. El primero responde a un determinado territorio estatal, expresado por dos letras, cuya regulación general se encuentra en la norma ISO 3166[30]. Los TLD territoriales

[29] Los *routers* pueden responder a una doble naturaleza. En ocasiones el sistema de enrutación se configura como mero conductor de la información y, otras tantas, cumple la doble función de encaminador y almacén de datos o Servidor de contenidos. En ambos casos la información que discurre a través suyo se almacena temporalmente en lo que se denomina *Memoria Tampón* o *Catching*, que permite mantener la carcasa general en la que se contiene la información que pasa a través suyo, con la finalidad de que si ésta es nuevamente solicitada el *host* no tenga que devolver nuevamente toda la información, sino sólo la que específicamente la individualiza.

[30]Puede accederse a la relación de códigos territoriales existentes hasta la fecha a través de web o vía ftp. Las direcciones en las que se puede consultar la relación son: Vía web: http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1.html. Se encuentra actualizado a 7 de abril de 1999. Vía ftp: ftp://ftp.ripe.net/iso3166-countrycodes. En España, el dominio**.es** se encuentra

pueden dividirse, a su vez, en abiertos o restringidos, en función de las condiciones de registro impuestas a los usuarios en la normativa concreta que cada país efectúa respecto a su Código Territorial. Lo mismo sucede con los TLD genéricos, que serán abiertos o restringidos en función de la capacidad de los usuarios para poder operar con ellos[31].
El dominio de segundo nivel identifica propiamente el producto solicitado, es decir, el nombre que el usuario ha pretendido obtener al registrar un Nombre de Dominio. Por último, el nombre de dominio de tercer nivel identifica el tipo de servicio buscado, es decir, si se trata de una página web (www), una transferencia de archivos (ftp), de una actuación remota (telnet), etc[32].

4. En el nivel sub-red, por lo tanto, lo que cabe analizar es el tipo de conexión establecida, esto es, conexión a través de ***Red de Área Local (LAN)***, o conexión ***Punto a Punto*** entre dos ***Routers***, o la línea telefónica, que sustentará la comunicación desde un punto específico de la red.

2. Servicios de red

Así entendida la comunicación vía Internet, conviene aún clarificar la diferencia entre los servicios, aplicaciones y herramientas que pueden obtenerse o aplicarse en dicho entorno. De una parte, el nivel de aplicaciones al que se ha hecho referencia anteriormente, permite, mediante el empleo de Protocolos específicos, la obtención de servicios de diversa clase que, en general, hoy no se entienden sin el empleo de una herramienta fundamental, como los ***Navegadores***, programas informáticos que permiten el intercambio de información bajo entorno gráfico, ocultando el verdadero lenguaje máquina utilizado entre los ordenadores que intercambian la información. El desarrollo de este tipo de programas, ha permitido que su empleo multiplique exponencialmente el fenómeno Internet en todo su sentido socioeconómico, en tanto instrumental en la utilización de otro tipo de servicios de Internet. En efecto, los navegadores convierten desde el entorno gráfico las instrucciones emitidas por el ordenador cliente al código máquina utilizado en la transmisión de información. Particularmente, en el nivel aplicaciones, los navegadores soportan los protocolos

---

regulado por la Orden Ministerial de 21 de marzo de 2000, cuyo texto se encuentra disponible en http://www.setsi.mcyt.es:81/legisla/internet/o210300/sumario.htm

[31] Actualmente funcionan siete ***Top Level Domain Names***,de carácter genérico, de los cuales son abiertos, en cuanto cualquiera que cumpla los requisitos podría registrar un nombre bajo dicho dominio:**.com:** previsto para entidades de carácter comercial;**.org:** cuya utilidad se limita a entidades no gubernamentales ni comerciales; y **.net:** para entidades que desarrollan una función directamente relacionada con el ámbito de la red.
Por el contrario, quedan reservados al ámbito territorial norteamericano y a las instituciones de aquél país que se ajustan al TLD concreto: **.gov:** previsto para entidades de carácter gubernamental; **.edu:** principalmente previstas para entidades de carácter educacional (colegios, universidades, etc.); y **.mil:** específica para instituciones de carácter militar. Por último, reservado a intstituciones creadas en virtud de Tratado Internacional queda el dominio **.int**

[32] En general, **BARDALES MENDOZA, E.,** *Conflicto entre los nombres de dominio en Internet y los Derechos sobre Marcas*, en Revista Electrónica de Derecho Informático, nº 1, p. 4 y ss.; **CARBAJO CASCÓN**, *Conflictos entre Signos Distintivos y Nombres de Dominio en Internet*, Aranzai, 1999, pp. 28 y ss.

más importantes de los servicios de Internet, servicios que básicamente son los siguientes[33]:

2.1. WWW (World Wide Web): Es, posiblemente, el servicio más importante que puede obtenerse en Internet. Como su traducción literal indica, consiste en una gran telaraña (red) mundial de recursos sistemáticamente organizados a los que acceder mediante un sistema de enlaces. En la medida en que los recursos así organizados pueden adoptar diversas formas y contenidos, cada expresión de los mismos requerirá un Protocolo universal de comunicación capaz de rescatar la información solicitada por la máquina cliente. De ahí que, en el cuarto nivel señalado en el gráfico, aplicaciones, se detallen los distintos Protocolos de comunicación que cumplen la función de rescatar los servicios solicitados. En el entorno de los servicios web, el protocolo que permite la comunicación entre el *host* (ordenador que contiene el servicio solicitado) y el cliente (ordenador que reclama la información es el **HTTP (*Hipertextual Transfer Protocol)***. Es el Protocolo de Transmisión de Hipertexto diseñado para hacer inteligible la petición de emisión y recepción, a través del sistema anteriormente descrito, de texto e imágenes. La referencia al Hipertexto indica el tipo de interconexiones que los distintos documentos requieren entre sí para su visualización. En el entorno web, es preciso, además, utilizar un lenguaje específico sobre el que opera el Protocolo, y que en el caso de las páginas web, se trata básicamente del lenguaje **HTML: *Hipertext Markup Language***. Por último, el complejo diseñado necesita un sistema para encaminar o enrutar la información, y que de nuevo debe ser de carácter universal, lo que se denomina **URL**: ***Uniform Resource Locator: localizador Uniforme de Recursos***. La particularidad de este sistema, y lo que asimismo le aleja de los Protocolos, es que el localizador, si bien es uniforme, en el sentido de que funciona con el mismo sistema para cada página insertada en la web, consiste en que el URL es único para cada página concreta. El URL funciona de modo equivalente para cada uno de los servicios de Internet, razón por la cual, la explicación que ahora se ofrece es válida para el resto de servicios que posteriormente se mencionan. Así, necesita la ubicación, en primer lugar, del protocolo de comunicaciones que el cliente desea utilizar, es decir, si se trata de un recurso que se encuentra en la web, el protocolo que deberá adjuntar es el http; a ello debe seguirle el DNS, es decir, la dirección completa del lugar (primer nivel), nombre (segundo nivel) y servicio (web) y, por último, la máquina, directorio y fichero en que se encuentra el documento solicitado.

---

[33] En general, sobre las aplicaciones y servicios de Internet, *Vid.* **SIEBER, U.,** *Strafrechtliche Verantwortlichkeit (I), op. cit.*, pp. 4 y ss.; **SMITH, G.,** *Internet Law and regulation*, 2ª ed., Londres, 1997, pp. 5 y ss.; **SEMINARA, S.,** *La pirateria su Internet e il Diritto penale*, en "Rivista Trimestrale di Diritto Penale dell'economia, nº 1-2, 1997, pp. 78 y ss.; **DE ANDRÉS BLASCO, J.,** *Internet*, en Cuadernos del Senado, Serie Minor, 1999, pp. 96 y ss.; **JOFER, R.,** *Strafverfolgung im Internet. Phänomenologie und bekämpfung kriminellen Verhaltens in internationalen Computernetzen*, Frankfurt am Main, 1999, pp. 21 y ss.; **OHLIGER, L.,** *Technische Grundlagen*, en Multimedia und Recht, 2000, Cuaderno 1, pp. 14 y ss.; **FERNÁNDEZ ESTEBAN,** *Nuevas tecnologías, op. cit.*, p. 25; **PICOTTI, L.,** *Profili penali delle comunicazioni illecite via Internet*, en "Il Diritto dell'informazione e dell'informatica", nº2, 1999, pp. 294 y ss.; **DE MIGUEL ASENSIO, P. A.,** *Derecho Privado de Internet*, 2000, pp. 26 y ss.; últimamente, también, **LLANEZA GONZÁLEZ, P.,** *Internet y Comunicaciones digitales. Régimen legal de las Tecnologías de la información y la comunicación*, Bosch, 2000, pp. 41 y ss.

En general, el servicio que genera la red mundial de recursos se basa en un sistema por el cual el usuario toma la información que él mismo solicita, si bien dicha técnica evoluciona hacia el sistema inverso a través de lo que podríamos denominar el servicio paralelo de

2.1.1. Webcasting,

Este servicio podría definirse como el "grupo de servicios emergentes que utilizan Internet para la entrega de los contenidos a los usuarios, de una forma muy similar a los servicios de comunicación". La especialidad del webcasting (también denominada ***multidifusión, multicasting*** o ***Broadcast***) radica en el hecho de que la información no es buscada por el usuario, sino que ésta es puesta a su disposición.

Para entender cómo funciona realmente el multicasting es preciso tener en cuenta algunas cuestiones técnicas. En primer lugar, la información es lanzada desde un punto de la red, es decir, desde un servidor, hasta un grupo de usuarios que, a diferencia de aquellos suscritos a una lista de distribución, no tendrán que solicitar al servidor –al *host*- que les envíe la información depositada en su buzón personal –que en todo caso radica también en un espacio físico del servidor-. Para que ello sea posible, es preciso que la información enviada por el *host* a su lista de *multicasting* sea procesada en nodos especiales que o bien son puntos multicast (es decir, que enrutan más de una IP simultáneamente) o que soportan un software capaz de emular un sistema multicast. Ello significa que enviarán directamente la información al nivel sub-red del usuario correspondiente, capturando entonces el cliente dicha información. Esta operación es reconocida como operación de multicasting por los *routers* o servidores de redireccionamiento porque la información viaja en flujo contínuo (lo que se conoce como ***streaming***, es decir, en un único paquete y no fragmentado en varios, aunque la apariencia de ese único paquete es la que tendría una información que viaja y que por su escaso tamaño ha sido fragmentada en un único paquete de datos. Una vez que el cliente accede a la información, en cuanto ésta no permite su disgregación en paquetes, sino que éstos son enviados en flujo contínuo según hemos visto, ésta se almacena en cantidad suficiente en el bufer del sistema, de modo que el *software* que la rescata la reproduce en el formato audio o video específico mientras se produce una descarga y reproducción permanente de la información. Precisamente este tipo de servicio es el que en mayor medida utiliza plataformas tecnológicas como el cable o la televisión digital para hacer llegar la información al usuario final. Programas como Realaudio o Realplayer, utilizan este sistema para la reproducción de la información que viaja en multicasting"[34]

2.2 Transferencia de archivos. Fuera del entorno web, aunque no es infrecuente su emulación en la misma, es posible, mediante la aplicación del **FTP *(File Transfer***

[34]Sobre la relevancia jurídica del servicio de webcasting, ampliamente, **BISBAL/CASAS/PEGUERA,** *Continguts audiovisuals en el marc de la convergència tecnològica*, en "Cuaderns del Consell de l'Audiovisual de Catalunya", nº 7, 2000, p. 6. Sobre el funcionamiento técnico de este servicio, son de especial interés las explicaciones contenidas en, http://www.arrakis.es/~aikido/interdic/articul2.htm y en la página de la OCDE (www.oecd.org) en el documento *Webcasting and Convergence: Policy implications*, especialmente pp. 16 y ss.

***Protocol)*:** Protocolo de Transmisión de Archivos, el intercambio de ficheros entre máquinas, generalmente ordenados en directorios por materias que a su vez contienen los archivos pertenecientes a la categoría correspondiente. De nuevo el desarrollo de los navegadores ha permitido la evolución en paralelo de este servicio bajo entorno gráfico, sin necesidad de que el cliente ejecute la petición mediante el empleo de comandos.

2.3. Telnet. Es el protocolo que permite la conexión remota a otra máquina, convirtiendo al ordenador cliente en una máquina de reproducción de los contenidos situados en el *host*.

2.4. Mail. Correo, lógicamente en su versión electrónica ***(e-mail: electronic mail)***. Se sostiene básicamente a través de dos tipos de Protocolos, el **POP3** y el **SMTP** para el envíos del cliente al servidor cuando aquél reclama la visualización de su correo y entre servidores cuando un mensaje es enviado de uno a otro cliente, respectivamente. Mediante correo electrónico es posible hoy el envío no sólo de texto sino también de imágenes o archivos, que en todo caso se almacenan en la memoria del *servidor* que ofrece el servicio –que no directamente en la máquina cliente- y de la que son recuperados por los clientes. Derivados del servicio de correo, en la medida en que depende de su estructura de comunicaciones son algunos de los servicios más populares y empleados, por la sencillez en su funcionamiento.

2.5. Grupos de noticias. Comúnmente denominados ***News Groups, Usenet***, etc., no se diferencian estructuralmente del correo electrónico. Son, de hecho, un servicio basado en el e-mail, mediante el cual el usuario puede participar en foros de debate, creando grupos u opinando sobre las materias recogidas en los ya existentes. Los grupos de noticias residen en el servidor y no en la máquina cliente, por lo que sus contenidos serán asignados, bien por el propio proveedor de contenidos del *host*, de modo que el cliente únicamente puede participar, pero no crear sus propios grupos, bien por el proveedor, pero facilitando a los usuarios la creación de grupos no controlados por el administrador del sistema, es decir, no moderados. Se diferencia del correo electrónico en el protocolo utilizado para la transmisión y recuperación de la información **TNP:** ***Network News Transfer Protocol***, que en cuanto debe permitir el acceso a la totalidad de los mensajes almacenados en cualquiera de los grupos radicados en el servidor, es diferente. El modo de acceso a la información, lógicamente, utiliza el mismo sistema que la búsqueda de documentos de hipertexto en la web, basado por lo tanto en el Sistema Uniforme de Localización.

2.6. Listas de distribución. Se trata de cadenas de direcciones de correo mediante las cuales hacer llegar a los interesados noticias sobre una determinada materia. Como se ha señalado, las listas de distribución se encuentran técnicamente a medio camino entre el correo electrónico y las listas de distribución[35]. En sentido técnico, ciertamente, son correo electrónico; en cuanto utilizan listas de usuarios con intereses comunes, se asemejan al servicio de News, con la diferencia de que los mensajes no

[35] **SIEBER, U.,** *Strafrechtliche Verantwortlichkeit, op. cit.*, p. 7; de la misma opinión, **PECORELLA, C.,** *Il diritto penale dell'informàtica*, CEDAM, Padova, 2000, p. 31.

llegan a un receptor común al que accedería cualquier usuario, sino a los buzones individuales de cada uno de los incluidos en el mensaje. Su importancia radica básicamente en la propia base de datos que sustenta la cadena de direcciones electrónicas, dado su valor estratégico en la publicidad de productos de toda clase.

2.7. Discusión en tiempo real. Generalmente denominado ***Chat***, como abreviatura de ***Internet Really Chat***, protocolo necesario para su utilización, permite la comunicación oral o escrita en tiempo real.

III. LA DIRECTIVA DEL COMERCIO ELECTRÓNICO Y LOS CRITERIOS DE RESPONSABILIDAD JURÍDICA DE LOS *PRESTADORES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN*[36]

Una vez se conoce el modo técnico en que funciona Internet es posible efectuar una ponderación equilibrada sobre los deberes de diligencia que pueden esperarse de cada uno de los operadores en función del servicio prestado y el modo en que éste se lleva a cabo. Conviene pues, con carácter previo, efectuar algunas anotaciones sobre las condiciones impuestas en materia de responsabilidad por la normativa europea y centrar la última parte de este trabajo en la proyección al ámbito penal de las conclusiones extraídas, a efectos de la posible responsabilidad penal de los distintos prestadores de servicios de la sociedad de la información.

La Directiva del Comercio electrónico no sienta las bases de responsabilidad de los prestadores de servicios de la sociedad de la información, entre los que incluye a los intermediarios. Por el contrario, exige a los Estados miembros el establecimiento de parcelas de impunidad necesarias para que la denominada Sociedad de la Información desarrolle el rol que le corresponde. En materia de responsabilidad la Directiva del Comercio electrónico se refiere a supuestos que hasta la fecha han centrado la atención de la jurisprudencia comparada y otros de compleja interpretación, si no tortuosa. En concreto se refiere a servicios de la sociedad de la información consistentes en la mera transmisión (*mere conduit*) de datos o facilitación de acceso; reproducción en memoria caché en los supuestos de servicios de la sociedad de la información que mediante dicha reproducción traten de hacer más eficaz el servicio *ulterior* al mero acceso o transmisión de datos; alojamiento de datos; finalizando con una cláusula de cierre sobre la inexigibilidad de supervisión de contenidos ajenos. Son varios ya, los conceptos que deben aclararse si no quiere construirse un castillo de responsabilidad jurídico penal en el aire. Sociedad de la Información, Servicios de la Sociedad de la información, Prestadores de Servicios de la Sociedad de la Información, Intermediarios, son sólo algunos de ellos, a los que

[36] El análisis de los criterios de responsabilidad jurídico penal de los intermediarios debe partir, lógicamente, de los límites impuestos en la Directiva del Comercio Electrónico, por lo que es necesario efectuar una análisis detallado de la misma. Me limitaré en este trabajo, no obstante, a una labor eminentemente descriptiva, remitiéndome en general al estudio de la misma contenido en **PEGUERA POCH, M.,** *Responsabilidad civil de los proveedores de servicios en Internet*, en este mismo portal, *passim*; **RICCIO, G. Mª.,** *Anonimato e responsabilità in Internet*, en DIR-INF, 2000, nº 2, pp. 316 y ss.; **GARROTE FERNÁNDEZ-DÍEZ,** *La responsabilidad civil, op. cit.*, pp. 36 y ss.

habrá de sumarse el de destinatario del servicio o el de consumidor para entender correctamente la filosofía de la Directiva y el alcance de sus disposiciones[37].

1. Mera transmisión o facilitación de acceso.

El artículo 12 DCE contiene las exenciones básicas de responsabilidad para la transmisión de datos y la facilitación de acceso a red. Deben distinguirse en él en consecuencia, como supuestos claramente diferenciados, la pura transmisión en una red de comunicaciones de los datos *facilitados por el destinatario del servicio* y la facilitación del acceso a red.

En relación con el primero de ellos, la excepción de responsabilidad alcanza sentido en cuanto la administración del servicio, allí donde el intermediario es un puro transmisor de datos, requiere en múltiples ocasiones el traslado de la información residente en memoria o los datos que previamente le ha hecho llegar el destinatario del servicio respecto de un servicio ya prestado y concluido. Pensando, en primer lugar, en clave de protección de datos, la transmisión de la información por cuenta del intermediario podría no cumplir con las prescripciones legales en materia de seguridad (básicamente contenidas en el Reglamento de Medidas de seguridad de 1999). La asunción del rol de transmisor directo y no de intermediario sitúa al prestador del servicio frente a las obligaciones genéricas –comunitarias y traspuestas a las diversas legislaciones nacionales- de protección de datos, de modo que la infracción de las medidas de seguridad legalmente establecidas *podrá* originar, si así se encuentra previsto en la normativa correspondiente, responsabilidad por el conocimiento de dichos datos por terceros no autorizados. Claro que, en este punto, la norma se vuelve tautológica: el intermediario no podrá ser responsable por la información transmitida, por los datos transmitidos, excepto cuando no actúe como intermediario, sino como origen de la transmisión, en cuyo caso no es un intermediario y, lógicamente, no se halla amparado necesariamente por la exención. La cuestión radica ahora en dilucidar si en aquellos supuestos en que el prestador de servicio no cumple con los requisitos técnicos de seguridad establecidos para la transmisión de datos que pueden ser de carácter personal pero no es él quien origina la transmisión sino al contrario, la transmisión se origina según los presupuestos de exención de responsabilidad a petición individual del destinatario del servicio, puede exigirse responsabilidad por el conocimiento de dichos datos por terceros no autorizados o, de otro modo, la exención general del artículo 12.1 DCE ampara igualmente su actividad. La respuesta debe hallarse en la interpretación de la

[37] Este trabajo tiene un marcado carácter introductorio. Baste ahora señalar, pues, que *destinatario de servicio* se corresponde, básicamente con el concepto de *máquina cliente* acuñada por los tecnólogos, y con la cual quiere significarse al usuario, es decir, a aquél que reclama un determinado servicio de acceso, alojamiento, etc.; asimismo, en cuanto este artículo centra su atención en la responsabilidad de los operadores e intermediarios de *Internet*, no cabe duda que nos hallamos dentro del concepto *Servicio de la Sociedad de la Información*, y que los operadores a los que se referirá la parte jurídico penal, en cuanto proveedores de acceso, transmisión o alojamiento de datos, igualmente pueden subsumirse dentro del concepto general de *prestadores de servicios e intermediarios*. Sobre el sentido y alcance general de los conceptos aludidos, *vide*, **PEGUERA POCH, M.,** *La responsabilidad civil, op. cit.*, pp. 14 y ss.

expresión "*por los datos transmitidos*": El intermediario, cuando sólo es un intermediario, no será responsable por los datos, es decir, por su contenido, aunque podrá quedar sometido a responsabilidad en los distintos Estados miembros por los problemas que origine sobre ellos en cumplimiento de su función como intermediario, de manera que el incumplimiento de las medidas de seguridad sobre los datos de carácter personal que puedan viajar a través suyo originará la responsabilidad recogida en la normativa sectorial y permitirá asimismo la proyección sobre el incumplimiento de los criterios de imputación jurídico penal, allí donde existan tipos penales que lo permitan[38].

Si se piensa en clave de contenidos, la falta de cobertura de la exención general en los casos en que el intermediario no se comporte como tal, es decir, en los casos en que es él mismo quien origina la transmisión facilita a los Estados miembros la imposición de deberes de garantía sobre el prestador del servicio (que ya no será de intermediación como puro transmisor) cuyo alcance deberá estar íntimamente unido a las previsiones en materia de exenciones contenidas en el resto del articulado, pues carecería de sentido imponer al intermediario reconvertido en punto de origen de la transmisión deberes de vigilancia o supervisión de mayor entidad que los exigidos para el intermediario que presta servicios de alojamiento.

En el caso de la facilitación del acceso a red, la norma debe necesariamente abarcar la transmisión de datos facilitados por el destinatario del servicio así como los devueltos por el destinatario de la transmisión: en definitiva, los datos de ida y vuelta que atravesarán la puerta abierta por el proveedor de acceso. Pues, en definitiva si como veremos más adelante el proveedor que facilita el alojamiento de datos no puede quedar sometido a deberes de vigilancia o supervisión, de nuevo carecería de sentido otorgar a los estados carta de naturaleza para la imposición de dichos deberes a los facilitadores de acceso en relación con la información de vuelta, es decir, la facilitada por el destinatario de la información (por ejemplo, una página web en la que se encuentran contenidos de pornografía infantil).

2. Memoria tampón o *Caching*

El tráfico de datos en Internet aconseja en ocasiones a los servidores de información que operan como intermediarios, la reproducción de parte de los contenidos alojados en otro servidor. Con ello se consigue una notable agilización del servicio, especialmente cuando el servicio en cuestión (acceso a portales, por ejemplo) es ampliamente demandado por los usuarios que utilizan su servidor como intermediario dado que, reproduciendo en memoria la parte de información estática del servicio demandado el servido intermediario no tiene que descargar del destino toda la información solicitada por el destinatario del servicio sino sólo aquella que

[38] No es el caso, por ejemplo, de la legislación penal española, en la que no se contiene en materia de protección de datos personales un precepto penal que, a semejanza de lo dispuesto en el artículo 601 CP para la información legalmente clasificada como reservada o secreta, prevea el descubrimiento de datos de carácter personal por terceros con origen en la negligencia grave del administrador del sistema o de quien se encuentra en todo caso habilitado para su gestión, como por ejemplo el simple intermediario.

personaliza la demanda. Para este tipo de supuestos la Directiva impone a los Estados miembros la prohibición de exigir responsabilidades al intermediario, de nuevo bajo ciertos condicionantes que a contrario pueden ser interpretados como obligaciones de hacer y que se resumen, a los efectos que aquí interesan, en el cumplimiento de las condiciones de acceso a la información (es decir, que el intermediario no prescinda de mecanismos de acceso condicional o establezca links profundos que trasciendan la publicidad de las páginas previas, etc.); el cumplimiento de las de las normas relativas a la actualización de la información (de modo que el intermediario no continúe reproduciendo en memoria caché datos que no aparecen ya en el servidor en que se encentra la información). Íntimamente relacionada con esta obligación se encuentra la de retirar la información que ya no se encuentre en la fuente una vez tenga conocimiento de dicha circunstancia y, en un efecto escalera, queda abierta la posibilidad de que autoridades administrativas o judiciales obliguen al intermediario a poner fin a una infracción o impedirla. La interpretación de esta cláusula, en todo caso, deberá ser interpretada teniendo en cuenta lo establecido en el artículo 12 para los facilitadores de acceso y meros transmisores de la información; pues, en definitiva, en los supuestos de reproducción en memoria caché lo normal es que el intermediario se comporte como mero transmisor de la información, razón por la cual no deberían imponerse obligaciones en la trasposición de la directiva que superen el marco de lo dispuesto en el artículo 12 DCE.

3. Alojamiento de datos

Sin duda los supuestos de almacenamiento de datos son los más problemáticos, dado el mayor nivel de diligencia que podría ser exigible a los prestadores de este servicio. En efecto, la contratación de servicios de alojamiento implica por quien ofrece el servicio la asunción de un determinado nivel de riesgo en función del contenido de los datos hospedados. La delimitación del nivel de riesgo soportable por el intermediario es nuevamente definida en la Directiva de forma negativa, impidiendo a los estados la depuración de responsabilidad por los datos alojados siempre que destinatario del servicio y prestador del mismo no sean una misma persona o aquél actúe bajo el control directo de éste, en cuyo caso, al igual que sucedía con lo dispuesto en el artículo 12 para los transmisores de información, no estamos ante meros supuestos de alojamiento de datos ajenos, sino propios. La Directiva describe las situaciones en que, no obstante lo anterior, el alojador de contenidos –*stricto sensu*- podrá responder de acuerdo a lo que se disponga en las diversas legislaciones nacionales permitiendo, la construcción de criterios para su ventilación allí donde el proveedor del servicio conozca la ilicitud de los datos alojados o, en relación con acciones por daños y perjuicios, conozca hechos o circunstancias que revelen el carácter ilícito de aquellos[39]; asimismo la Directiva permite la instauración a nivel

[39] Esta disposición será sin duda esencial a efectos de la responsabilidad civil derivada de delito, pues la DCE parece establecer dos niveles distintos de conocimiento. En primer lugar, con carácter general se refiere al conocimiento en sentido estricto y éste ha de ser efectivo, es decir, constatable en todos sus extremos, lo que, como se verá más adelante, será esencial a la hora de extraer conclusiones jurídico penales sobre posibles conductas de autoría o participación del proveedor. En segundo término, se refiere al conocimiento no ya del carácter ilícito de la información, sino al conocimiento

nacional de criterios de atribución de responsabilidad por alojamiento de datos ilícitos en aquellos casos en que el intermediario, conociendo la ilicitud, no actúe con diligencia y prontitud para la retirada de los datos o para hacer imposible el acceso a ellos. El precepto concluye permitiendo además a las autoridades administrativas o Tribunales de los Estados miembros tomar medidas para poner fin a una infracción o fijar procedimientos o protocolos de actuación para la retirada de información lesiva, lo que implica, de suyo, que el legislador nacional no tendrá la necesidad de esperar a que la autoridad administrativa o judicial informe al *Provider* de la ilicitud de los datos, pudiendo en consecuencia éste quedar informado a través de personas privadas, en coherencia con el contenido del artículo 15 DCE que se examina a continuación.[40]

4. La cláusula de cierre del artículo 15 de la Directiva

El artículo 15 DCE finaliza las previsiones en materia de responsabilidad eximiendo con carácter general a los intermediarios, ya sean éstos meros transmisores de información, prestadores de servicio de alojamiento, de simple acceso a red o nodos de transmisión con capacidad de reproducción en memoria caché, de la obligación de supervisión de los contenidos *o* de los hechos o circunstancias que indiquen una posible actividad ilegal. La exención general de búsqueda de contenidos viene en cambio compensada con la habilitación a los Estados miembros para la imposición de genéricos deberes a los intermediarios, algunos de ellos abiertamente reñidos con la lógica hasta ahora imperante en Internet y cuyo establecimiento podría llegar a provocar huidas hacia paraísos informáticos situados extramuros del Estado que las establezca o, por qué no, del propio continente[41]. Es el caso de la posible obligación de comunicar a las autoridades la identidad de los destinatarios del servicio, reservada sólo para quienes presten el servicio de alojamiento, lo que significa un control de la identidad del usuario –libertad en este punto para la determinación de los niveles de rigurosidad, *v. gr.*, a través de firma electrónica- y el fin del anonimato en la comunicación.

IV. CRITERIOS DE ATRIBUCIÓN DE RESPONSABILIDAD JURÍDICO PENAL POR CONTENIDOS AJENOS

de hechos o circunstancias que revelen tal extremo –es decir, ya no es un conocimiento efectivo de la ilicitud, sino tan sólo de los hechos o circunstancias que puedan revelar la misma. Por ello, parece que se mantendría incólume la posibilidad de depurar responsabilidad civil derivada del delito, directa o subsidiaria, cuando no el proveedor del servicio de *hosting* no haya adquirido conocimiento efectivo de la ilicitud de los datos –esencial para la afirmación de cualquier título de autoría o participación en delitos de la parte especial, salvo los casos de imprudencia- pero sí de hechos o circunstancias que pudieran dar cuenta de ello (supuestos próximos, pues, a la culpa *in vigilando* o *in eligendo*). Lo expuesto, además, parece confirmarse con lo dispuesto en el artículo 15.1 DCE, donde de nuevo vuelve a referirse a búsqueda de contenidos ilícitos o de hechos y circunstancias que indiquen actividades ilícitas.

[40] Cfr., sin embargo, las dudas planteadas por **RICCIO, G. Mª,** *Anonimato*, *op. cit.*, pp. 317 y s.

[41] **RICCIO, G. Mª,** *Anonimato*, *op. cit.*, p. 318, quien apunta el riesgo al que, desde la lógica del artículo 15.2 DCE, se estaría sometiendo a la libre competencia.

Las disposiciones contenidas en la Directiva del Comercio electrónico no fundamentan supuestos de responsabilidad de los prestadores e intermediarios. Por el contrario, según hemos tenido ocasión de comprobar, precisamente la Directiva responde en este punto a su función, marcando los límites negativos, traspasados los cuales los Estados podrán establecer prescripciones positivas de responsabilidad a los operadores. Esta función directriz hace más compleja, en tanto no sea traspuesta al Derecho español, la determinación de sus repercusiones sobre el ámbito penal, que sin duda deberían quedar disipadas con la entrada en vigor de lo que aún figura como *Anteproyecto de Ley de la Sociedad de la Información*, preparado por el Ministerio de Ciencia y Tecnología[42]. Efectuadas estas consideraciones a modo de prevención, procede el análisis de los mecanismos de atribución de responsabilidad jurídico penal a los intermediarios.

1. Sobre la aplicación del artículo 30 CP

En el contexto tecnológico en que la actividad de los actores de Internet se desenvuelve, y con carácter previo a la promulgación de la Directiva del Comercio Electrónico, algunos países de nuestro entorno han tratado de extender el régimen jurídico de la prensa escrita o, incluso, el de otro tipo de medios de comunicación (empleando aquí convencionalmente el término) a la actividad desarrollada en Internet, experimento ampliamente rechazado por la doctrina[43], y la jurisprudencia[44]y que, tampoco es acogido en la Directiva. Una apuesta similar en nuestro país, arroja un resultado igualmente rechazable, por razones en abstracto semejantes, y sólo diferentes en relación a la terminología empleada en la normativa sectorial de telecomunicaciones. La Ley 14/1966, de 18 de marzo, de Prensa e Imprenta, ampliamente derogada tras la entrada en vigor de la Constitución regula básicamente, según se desprende de lo dispuesto a lo largo del Capítulo II, la actividad de difusión a través de impresos, entendiendo por tal "toda reproducción gráfica destinada, o que pueda destinarse, a ser difundida". La amplitud de esta definición viene luego acotada por la clasificación de los impresos en publicaciones unitarias y periódicas, comprendiendo las primeras "los libros, folletos, hojas sueltas, carteles y otros impresos análogos" en tanto los segundos estarían integrados por "seminarios y aquellas otras que, en general aparecen en cualesquiera períodos de tiempo determinado". La prensa escrita, pues, difiere de la comunicación establecida en

[42] De ahí que no pueda afirmarse con rotundidad que lo dispuesto por ejemplo en el artículo 12 DCE comprenda en sentido estricto la responsabilidad penal, pues precisamente lo que debe averiguarse es el alcance de la exención y posteriormente proyectar los instrumentos dogmáticos de la disciplina penal en su integración. Cfr., sin embargo, **GARROTE FERNÁNDEZ-DÍEZ, I.,** *La responsabilidad civil, op. cit.*, p. 43.

[43] Por todos, **ZENCOVICH, Z.,** *La pretesa estensione, op. cit., passim.*; **RICCIO, G. M.,** *Anonimato, op. cit.*, p. 321 y bibliografía citada en nota 21.

[44]Así sucede en el caso *Cubby Inc. V. Compuserve*, recogido por **MAGNI/SPOLIDORO,** *La responsabilità degli operatori inInternet: Profili interni e internazionali*, en Il Diritto dell'informazione e dell'informatica, nº 1, 1997, p. 75, en el que, frente a una presunta difamación efectuada por un tercero a través de un Grupo de noticias alojado en un servidor, el Tribunal entendió que la equivalencia del *host* no se hallaba tanto en la figura del editor, encargado de la supervisión de todas y cada una de las informaciones publicadas, cuanto la de un vendedor de libros, a quien sería absurdo reclamar un deber de control de los contenidos que vende.

Internet, ya en la definición misma de su objeto, que se limita a la versión impresa de las comunicaciones difundidas en el medio y que, además, debe responder, según se desprende del artículo 9 de la citada Ley de prensa a unos requisitos formales en función de la periodicidad de la publicación, nuevamente circunscrita a la versión en papel de aquella. De ello pueden extraerse ya algunas consecuencias, no por obvias innecesarias: por un lado, de las posibles analogías entre el sistema Internet y la prensa, no cabe diferir *in totum* el régimen de responsabilidad (y, específicamente el penal) previsto para ésta sobre aquella; por otro, la comunicación vía Internet, según el modelo analizado, no responde en sentido estricto a la idea de difusión, no al menos en algunos de los servicios a través de los cuales pueden ser realizadas determinadas acciones de carácter delictivo, por lo que la proyección del régimen de la prensa escrita a la anomia reinante en Internet, dejaría huérfano de tutela un amplio abanico de conductas –de gran importancia- realizadas a través de la Red. Allí donde la difusión es la función principal desempeñada o que es capaz de desempeñar el servicio concreto de que se trate, la sumisión de Internet a la legislación de prensa, al menos jurídico penalmente – y por relación tampoco civilmente-, no es satisfactoria, incluso aunque se pretenda la equiparación no ya desde el concepto de difusión o las analogías entre Internet y la prensa, sino desde la idea de *medio mecánico de difusión*.

En efecto, el régimen diseñado en el Capítulo X de la Ley, remite la depuración de responsabilidades penales a lo dispuesto en el artículo 15 CP/1973, que se corresponde, en lo fundamental con el artículo 30 del CP 1995. De nuevo las dificultades estructurales para armonizar los diversos sistemas de difusión bajo una única norma es harto complejo, pues presupuesto básico para la aplicación de dicho precepto es la realización de delitos o faltas "utilizando medios o soportes de difusión mecánicos". Frente a la opinión generalmente aceptada de que el empleo de la expresión "medio de difusión mecánico" permite la incorporación de cualquier sistema distinto de la pura comunicación oral intersubjetiva no auxiliada de soporte alguno incluyendo toda innovación técnica que permita la difusión, incluso más allá de la prensa escrita, radio y televisión[45], cabe efectuar algunas precisiones[46].

En primer lugar, algunos servicios de la sociedad de la información, como la transmisión punto a punto, aunque multifrecuente, son excluidas legalmente desde su régimen jurídico sectorial del concepto de difusión, lo que hace innecesaria la conceptualización del medio técnico como mecánico, puesto que en todo caso no lo será de difusión, aunque la información, en sentido amplio sea difundida a través de dicho medio.

En segundo término, el concepto *medio mecánico* desde la interpretación gramatical viene referido a estructuras complejas energéticamente alimentadas, a un conjunto de estructuras interdependientes que funcionan en sí mismas. Internet, en cambio, no

[45] **QUINTERO OLIVARES, G.,** *Manual de Derecho Penal. Parte General*, con la colaboración de Morales Prats y Prats Canut, Aranzadi, 1999, p. 644.

[46] *Vid.*, crítico con la proyección a Internet, del régimen de responsabilidad en cascada diseñado para la prensa y la radiodifusión en algunos países, **MONTERO, E.,** *La responsabilité des prestataires intermédiaires de l'Internet*, en Revue Ubiquite, nº 5, 2000, pp. 102 y s.

funciona en sí misma sino que permite el tráfico de información en un modo específico, precisamente el consignado en el gráfico. Es un medio técnico, no mecánico. Desde un punto de vista hermenéutico basado en la historia del precepto es evidente que el mismo fue creado para garantizar la depuración de responsabilidad en los nuevos medios de difusión de noticias basados en la mecánica[47] -comprometiendo al mínimo la libertad de expresión[48]-, no en la técnica, tales como la prensa, que requiere un complejo sistema mecánico de creación de planchas, inyección de tinta, secado, etc., para la posterior difusión de la información. Por este motivo, la sistemática del precepto hace referencia a los modos de gestión conocida de la prensa escrita, ni siquiera adaptable a la realidad de la radio y televisión, mucho menos a la realidad de Internet. En efecto, la actividad de un diario es limitada, en cuanto la información en él contenida, si es que se quiere ser fiel al concepto de publicación periódica, ocupa un espacio físico, de modo que la información de la que puede hacerse responsable al Director ha de ser necesariamente limitada, lo suficiente para hacerle desempeñar el rol de Director; máxime, cuando la nomenclatura del artículo 30 CP no puede ser formalmente entendida sino referida al desempeño de roles específicos. Contrariamente, la información capaz de ser difundida en Internet, por ilimitada, impide el desempeño de un rol propiamente parangonable al de Director de una publicación, salvo en los casos en que la actividad desempeñada a través de dicho medio coincida exactamente con el sistema de publicaciones periódicas. Pero la subsunción en el concepto medio mecánico de difusión por dicho motivo, ignorando los anteriormente apuntados confundiría la *pars pro toto*, pues la publicación periódica no es característica esencial de la red. Cabe añadir, además, que el régimen excepcional de responsabilidad del artículo 30 CP, no se ajusta a la dinámica de Internet, donde existen operadores difícilmente encuadrables en dicho precepto, ajenos por tanto a las reglas de subsidiariedad y exclusión que en él se promocionan y, viceversa, sujetos sometidos al alcance del artículo 30 CP y que son desconocidos en el ciberespacio. Entre los primeros cabría señalar a los usuarios que, sin ser autores de las imágenes que hospedan bajo la técnica del *linking* en sus páginas web, conocen el contenido ilícito que se esconde en los enlaces de remisión, sin que se les pueda considerar directores de publicación (la página web, propiamente no lo es) o del programa (relativo al momento y rol desempeñado por un espacio específico), lo que tampoco es válido para el servicio web de Internet. Entre los segundos, cabe adelantar los extraordinarios problemas de identificación entre los operarios de Internet de directores de empresas grabadoras, emisoras o impresoras, necesidades por definición inexistentes en aquél medio.

Por último, la posible identificación entre los prestadores de servicios y algunas de las categorías clásicas de la difusión mediante prensa escrita u otros soportes *mecánicos* se desvanece a la luz de los principios de exclusión de responsabilidad

---

[47] *Vid.*, con carácter general, **QUINTERO OLIVARES,** *Comentario al artículo 30 CP*, en **VVAA**, Comentarios al Nuevo Código Penal, Gonzalo Quintero Olivares (dir.) José Manuel Valle Muñiz (coord.), p.313, en las que aclara la distinción entre necesidad de garantizar la responsabilidad jurídico penal por los contenidos ilícitos difundidos mediante medios mecánicos y la necesidad de aumentar dicha represión, tal y como en alguna ocasión había sido apuntado.

[48] **VIVES ANTÓN, T-S.,** en *Comentario al artículo 30 CP*, en **VVAA,** *Comentarios al Código Penal de 1995,(I)* Tomas S. Vives Antón (coordinador), p. 289.

establecidos en la Directiva del Comercio electrónico, antagónicos a los que tradicionalmente fundamentan la responsabilidad en el seno de la prensa escrita. Debe partirse en todo caso, tal y como establece la Directiva en el artículo 15, de la ausencia de deberes de vigilancia y supervisión de los datos alojados en el servidor, de todo punto razonable en cuanto la capacidad lógica de un servidor de mediano alcance permite, con la tecnología actual, el hospedaje de miles de páginas bajo cualquiera de los protocolos convencionales -que se multiplica debido a la técnica del *linking* desde páginas hospedadas en otros servidores, lo que sin duda prácticamente imposibilita el control real o eficaz[49]. A mayor abundamiento, la búsqueda activa de contenidos ilícitos o la supervisión general de los datos hospedados en el *host* encontraría serias dificultades ético sociales, pues a la luz de los diversos modos de filtrado de contenidos que pueden efectuarse en un sistema de red, significaría un control de la actividad de terceros y una valoración sobre el carácter lícito o ilícito del mismo; el riesgo es en este punto evidente. Si se tiene en cuenta el paralelismo de Internet con los sistemas de difusión de prensa y televisión, la actividad de inspección del *Provider* habría significado abiertamente el establecimiento de un sistema de censura difícilmente compatible con el entorno[50]: en tanto la responsabilidad del director de un medio de comunicación escrito puede escalonarse por los contenidos de terceros editados en su plataforma, la depuración de responsabilidad del *Provider* no admite la comparación: así, aquella actividad que más fácilmente podría asimilarse a la desempeñada, por ejemplo, por el Director de la empresa editora, es decir, la del prestador del servicio de almacenaje de datos, queda exenta de responsabilidad siempre que éste desconozca la ilicitud de la actividad o actúe con prontitud una vez advertido de ello, eximiéndole en cualquier caso de la necesidad de supervisión de contenidos[51]. O, de modo idéntico, en cuanto la Directiva exime de una obligación general de supervisión y/o búsqueda activa de contenidos al prestados de servicios cuando éstos consistan en el almacenamiento de datos, está situando en esferas distintas a operadores que analógicamente serían asimilables, como el Director de la publicación y el proveedor del servicio de almacenamiento[52].

1. Responsabilidad por comisión activa a título de autoría o participación

[49] *Vide supra* nota 25.

[50] Cfr. **SEMINARA, S.,** *La pirateria su Internet e il Diritto Penale*, Rivista Trimestrale di Diritto Penale dell'economia, nº 1-2, 1997, p. 99. El autor pone de manifiesto cómo la técnica del filtrado, además, sería aplicable sólo al texto escrito y no a las imágenes o al sonido; dejando de lado que entre la publicación de la obra citada y la elaboración de esta cita son ya múltiples los programas capaces de efectuar filtrado de imágenes y reconocer aquellas que contienen elementos pornográficos y aun distinguir si éstos pueden ser clasificados como pornografía infantil, al margen de dicha eventualidad, no le falta razón al autor al advertir del riesgo de criminalización de textos perfectamente lícitos en cuyo contexto las palabras clave cribadas carecen del sentido ilícito que trata de prevenirse; en el mismo sentido, también **SIEBER, U.,** *Strafrechtliche Verantwortlichkeit,I, op. cit.*, p. 19.

[51] Cfr., los interrogantes en esta dirección planteados por **MONTERO, E.,** *La responsabilité, op. cit.*, p. 102.

[52] A soluciones similares se ha llegado desde el ámbito jurídico civil. Sobre las relaciones entre la Directiva y la Ley de prensa e Imprenta, a los efectos de determinar el alcance de ésta sobre los Prestadores de Servicios *on-line*, recientemente, **GARROTE FERNÁNDEZ-DÍEZ, I.,** *La responsabilidad civil, op. cit.*, pp. 62 y ss.

Partiendo de lo establecido anteriormente, la (co)responsabilidad de los intermediarios de la Sociedad de la Información podrá ser depurada mediante las respectivas figuras de la parte especial, imputadas a título comisivo, lo que será posible en aquellos casos en que el Proveedor desarrolle un verdadero hacer positivo, más allá de la simple facilitación de un servicio, es decir, tomando parte directa en la ejecución del hecho mediante la creación de contenidos propios o la selección de los ajenos que serán difundidos; ello sucederá en los servicios de *webcasting* o, de modo algo menos evidente, con las listas de distribución, en los casos en que el proveedor desarrolle el doble rol de proveedor de contenidos y difusor de los mismos, es decir, allí donde el intermediario no sólo presta el servicio de difusión sino que asume la producción propia de los contenidos[53]. Se trata, en definitiva, de intervenciones positivas en la delimitación de los contenidos que formarán parte del paquete de información del servicio de multidifusión y/o polidistribución mediante listas. Ciertamente, la acción desarrollada por el proveedor será, en la mayoría de los casos, producto de la infracción del deber de cuidado en la tarea de selección de contenidos, lo que limita la punición a través de la cláusula de comisión imprudente, pero también el alcance de eventuales tipos imprudentes, dada la ausencia de deber de control de contenidos[54]. Verificada su expresa tipificación será preciso, además, recurrir a las estructuras de imputación en cumplimiento de la interdicción de regreso (*Regressverbot*).

La imputación del hecho al Proveedor del servicio a título de participación tampoco está exenta de problemas. Desde luego, si el mismo no tiene conocimiento del contenido o, aún teniéndolo carece de medios técnicos para su supresión del servidor[55], difícilmente podrá convenirse en una responsabilidad como cómplice o partícipe necesario, pues el hecho principal dependerá íntegramente de un tercero, sin que su aportación pueda ser reprochada al ajustarse al ejercicio de una función determinada. Distinto es el caso en que el proveedor del servicio decide no retirar la información o bloquear el acceso a la misma, pudiendo hacerlo sin dificultad. En tal hipótesis los interrogantes se abren en un doble ámbito.

Por una parte, en relación con el posible agotamiento del delito, de modo que la participación del intermediario se limitaría a enervar o amortiguar los efectos del

---

[53] De acuerdo en este punto, pues, con lo ya sostenido por **PICOTTI, L., .,** *La responsabilita'penale dei Service-Providers in Italia*, en Diritto Penale e Processo, nº 4, 1999, p. 502. El autor extiende la responsabilidad a título de coautor o incluso autor comisivo al *hosting* que, además, modera personalmente los grupos de noticias supuesto que será analizado sin embargo, en este trabajo, desde la perspectiva de la omisión.

[54] La exención del deber general de control o supervisión de la información alojada o que simplemente se trasmite a modo de nodo de comunicación dificultaría en extremo la punición de conductas en las que se tiene conocimiento doloso eventual de la ilicitud de los datos, pues ciertamente en tal caso volvería por la puerta lo que sale por la ventana. Cfr., sobre ello, **ENGEL/FLECHSIG/MAENNEL/TETTENHORN**, *Neue gestzliche Rahmenbediegungen für Multimedia. Die Regelungen des IuKDG und des MdStV, 1998*, pp. 17 y s.

[55] Especialmente, en los casos de mera provisión de acceso, sin perjuicio de lo que se dirá más adelante (cfr. *Infra* nota 31, en relación con los progresos técnicos que permitirían la supresiónde contenidos por el proveedor de acceso).

hecho antijurídico[56]. Frente a la opinión de que el hecho principal se encontrará por lo general consumado dada la clase de acciones típicamente relevantes que concurrirán a la subsunción del hecho (difusión, comunicación, reproducción), caben dos frentes argumentales que favorecerían la incriminación como cooperador necesario o cómplice. De un lado, si el proveedor conoce el contenido antes de permitir el acceso al mismo, su aportación al hecho podrá ser calificada de cooperación necesaria atendida la doctrina de los bienes escasos o incluso del dominio del hecho[57]. Si, por el contrario, no tuvo dicha posibilidad, pero adquiere conocimiento con posterioridad a su difusión, deberán diferenciarse varias hipótesis. Si el delito es permanente en cuanto a su consumación, el proveedor podrá responder a título de participación, toda vez que el hecho permite la intervención de terceros en cualquier momento, previo al agotamiento del delito. Si el hecho es de consumación instantánea, no responderá de los hechos producidos con anterioridad a su conocimiento. En cambio, el mantenimiento del contenido ilícito (piénsese en un delito contra la propiedad intelectual, por ejemplo por reproducción del código fuente de un software o comunicación pública del mismo), permitirá la interrupción de la unidad de hecho –allí donde ésta esté presente- de modo que los actos posteriores, en tanto entra en juego un factor de esencialidad en el mantenimiento de la acción ilícita, fueran constitutivos de un nuevo delito en el que el *Service Provider* debe responder a título de participación.

De la reflexión anterior nace el segundo problema, en el cual se ha centrado actualmente el debate jurídico penal europeo. Admitida la posibilidad de participar en el hecho ajeno mediante el mantenimiento de la prestación, es preciso determinar el modo activo u omisivo en que la misma se manifiesta. Y la cuestión no es baladí. Si la legislación extrapenal no alcanza deberes de actuar del intermediario; si la Directiva de la Sociedad de la Información no determina los supuestos en que los prestadores serán responsables sino aquellos en los que de ningún modo podrán serlo; y si las excepciones a las exenciones aún no han sido traspuestas al Derecho positivo en la legislación de los Estados miembros como situaciones en las que será exigible la responsabilidad; si todo ello es así, la imputación a título omisivo será compleja allí donde existan cláusulas de incriminación del delito omisivo como las del Derecho italiano, alemán o español. Desde estas premisas, se ha entendido que el mantenimiento del servicio cuando el intermediario conoce la ilicitud de los contenidos alojados en el Servidor constituye una contribución objetiva al hecho ajeno en la que no caben excepciones a las reglas generales de participación activa[58]. La automatización del servicio no sería entonces un obstáculo para la verificación de

---

[56] Apuntado ya por **SEMINARA, S.,** *La responabilità penale, op. cit.*, p. 764; también, **FORNASARI, G.,** *Il ruolo della esigibilità, op. cit.*, p. 5, aunque de todos modos la cuestión se plantea igualmente desde la participación omisiva.

[57] En este sentido, el ejemplo recogido por **PICOTTI,** *Fondamento e limii, op. cit.*, p. 385, en el que el Tribunal Federal Suizo confirmó la condena por participación necesaria activa del proveedor de un servicio telefónico de contenido erótico, previamente advertido por la Administración de Justicia suiza para que impidiera el acceso a los menores a dicho servicio, aun cuando para ello hubiera de suspender la actividad del mismo. De todos modos, sobre el presupuesto de la exigibilidad, cfr. *Infra*. Un comentario a dicha resolución en **WIDMER, U./BÄHLER, K.,** *Strafrechtliche und aktienrechtliche Haftung von Internet Providern*, en Computer und Recht, 1996, pp. 178 y ss.

[58] **PICOTTI, L.,** *La responsabilita'penale, op. cit.*, p. 501.

una conducta de cooperación necesaria activa, en la que de todos modos concurren acciones positivas enderezadas al mantenimiento, aun automatizado, de dicho servicio y que actúan a modo de concausa o *conditio sine qua non* del resultado típico[59]. Frente a ello, se ha opuesto la desconexión en términos de imputación objetiva entre la conducta del intermediario y el resultado típico derivado en todo caso de la conducta del autor, riesgo en consecuencia sólo jurídicamente imputable desde estructuras omisivas[60]; o la exigencia de un *dolo particularmente intenso del intermediario*.[61]

3. La responsabilidad a título de comisión por omisión.

La actuación del Proveedor, sin embargo, no siempre podrá ser reconducida al ámbito del actuar positivo, al menos desde el punto de vista de la relevancia penal de su acción (con estructura causal). Ello sucederá con especial claridad en la pura facilitación de acceso a red, alojamiento de páginas ajenas, así como en la gestión de grupos de noticias no moderados y el correo electrónico y, de modo distinto, según se analizará más adelante, en los grupos moderados por el intermediario, la información cursada mediante listas de distribución y webcasting.

En la prestación de los servicios expuestos en primer lugar, los juicios de imputación del resultado respecto a la acción del autor de la información o los datos y del intermediario se sitúan en planos diversos, carentes de conexión jurídica, de nuevo salvo infracción de la prohibición de regreso, imputando *ad infinitum* a través de estructuras causales o de equivalencia de las condiciones. Pues, en sí mismo considerado, el hecho de proveer la infraestructura técnica o el alojamiento de contenidos carece de relevancia jurídica, reafirmada por los criterios expuestos en la Directiva del Comercio electrónico; de manera que la búsqueda de criterios de imputación únicamente podría discurrir en el seno de la omisión de específicos deberes de control sobre cuya existencia y en su caso alcance profundizaremos en las páginas subsiguientes. La cuestión es algo diversa en el segundo grupo de supuestos, dado que en ellos convergen formas activas (supervisión y control, por ejemplo) con su anverso (ausencia de control o supervisión cuando previamente se han tomado decisiones positivas en cuanto, por ejemplo, a los contenidos seleccionados). En tal caso, el concepto de omisión del que se parta, el criterio de equivalencia con la *causación activa del resultado* que se maneje, y el sentido y alcance de las posiciones de garantía descritas en el artículo 11 CP serán fundamentales para la fijación de las bases sobre las que fundamentar la posible co-responsabilidad del intermediario en cada una de las modalidades delictivas que abarca Internet.

---

[59] *Ibidem*, pp. 501-502.

[60] Particularmente en este sentido, **SIEBER, U.,** *Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (II)*, en http://www.jura.uni-wuerzburg.de/lst/sieber., pp. 7-8. Sobre ello, cfr. *Infra*.

[61] **SEMINARA, S.,** *La responsabiltà penale, op. cit.*, p. 766. Dolo particularmente intenso que en la construcción del autor es reconducible a la teoría del acuerdo previo o a un deseo expreso de facilitación del resultado típico, del que resultan exclusas de la participación jurídico penalmente relevante las aportaciones doloso eventuales.

Esta vía requiere, pues, en primer lugar, la posibilidad de que el hecho concreto pueda ser realizado, en función de la estructura típica de referencia, de modo omisivo[62]. Partiendo de este axioma, según el cual la cláusula del artículo 11 CP únicamente sería proyectable sobre delitos de resultado material en los que pueda adivinarse una secuencia espacio temporal entre acción y resultado en las modalidades comisivas, los principales tipos penales de referencia pierden capacidad de aplicación respecto a las conductas de los intermediarios[63]. Los delitos de injuria y calumnia, o la difusión de pornografía infantil son sólo algunos de los ejemplos, donde la responsabilidad del intermediario deberá buscarse ya por vías alternativas a la comisión por omisión. En los casos mencionados se trata de delitos de mera actividad en los que no puede establecerse una frontera nítida entre acción y resultado, entre la imputación de hechos y el resultado injurioso, entre la facilitación de la difusión y la difusión misma. En el primer caso la extensión del régimen jurídicopenal al intermediario será más compleja que en el segundo, puesto que aquí la elevación a categoría de autor de conductas puramente participativas o incluso de estadios previos a la consumación o al agotamiento del delito como la facilitación, favorecen la incriminación de conductas activas (no ya omisivas) ajenas a los estadios de mayor calado lesivo como la recopilación, producción o difusión misma del material. Por el contrario, la simple imputación de hechos realizada a través de la red -en cuanto conducta de consumación instantánea- impide ya la utilización de la cláusula de comisión por omisión para la atribución del hecho a los intermediarios por lo que cualquier extensión del régimen de responsabilidad podrá serlo exclusivamente a título de participación activa u omisiva en el hecho ajeno, exclusivamente en aquellos casos en que el intermediario que presta servicio de alojamiento o incluso el mero transmisor de la información cuando no actúa como tal[64], conocen la ilicitud de los datos (falsedad de la imputación o del temerario desprecio hacia la verdad con que la imputación fue realizada) y no obstante mantienen el servicio activo.

---

[62]La doctrina mayoritaria, como es sabido, se decanta por la reserva de la proyección del artículo 11 CP a los tipos de resultado. Doctrina mayoritaria de la que puede consultarse, **VIVES ANTÓN, T. S.,** *Comentario al Artículo 11 CP*, en Comentarios al Código Penal de 1995, Dir. Vives Antón, p. 85; **SILVA SÁNCHEZ, J. Mª.,** *El nuevo Código Penal: cinco cuestiones fundamentales*, 1997, pp. 74 y ss.; **MORALES PRATS, F.,** *Comentario al artículo 11 CP*, en Comentarios al nuevo Código Penal de 1995, dir. Gonzalo Quintero Olivares, coord. José Manuel Valle Muñiz, Aranzadi, Pamplona, 1996, p. 89; **MIR PUIG,** *Derecho Penal. Parte General*, 4ª ed., p. 317; últimamente, también, **REBOLLO VARGAS,** *Algunas reflexiones sobre los delitos de comisión por omisión en el Código Penal español*, en "El Nuevo Derecho Penal español. Estudios Penales en Memoria del Profesor José Manuel Valle Muñiz, 2001, p. 655. La exigencia de tipos de resultado en derecho español derivaría, según la opinión del primer autor citado, de la expresión gramatical *producción del resultado*, lo cual dificulta seriamente la ampliación de la cláusula del artículo 11 CP hasta delitos de mera actividad. La referencia menos clara del derecho alemán, permite una mayor apertura que, si no es mayoritariamente reconocida, si ha sido sostenida por autorizadas plumas. Cfr. **JAKOBS, G.,** *PG*, *op. cit.*, p. 450; **STREE, W.,** *Schönke/Schröder*[25]*,§ 13* Rdn. 161.

[63] Lo advierte ya, **SEMINARA, S.,** *La responsabilità penale*, *op. cit.*, p. 764, en relación al tratamiento de estas cuestiones desde el Derecho italiano.

[64] Es decir, en los supuestos recogidos en las letras a) y c), del artículo 12.1 de la Directiva del Comercio electrónico, pues allí donde el origen de la transmisión no está en el destinatario del servicio o el transmisor de los datos modifica la información no puede hablarse ya de mero transmisor.

Para aquellos casos en que la estructura del delito no impide la realización del hecho en comisión por omisión, y en cualquier caso para las conductas de participación vía omisiva y presupuestos el conocimiento de la actividad ilícita desarrollada a través del servicio técnico prestado y su mantenimiento doloso, resta aún por clarificar la presencia de deberes jurídicos de actuar[65] afirmados los cuales podrá efectuarse el juicio de equivalencia entre la causación activa del resultado y su no evitación. Deben nuevamente diferenciarse los diversos servicios desarrollados por los intermediarios en el seno de la sociedad de la información y, particularmente de Internet.

En relación con la mera transmisión de datos, la Directa del Comercio electrónico tan sólo refleja situaciones en las que en modo alguno podrá ventilarse la responsabilidad del proveedor así como otras tantas no abarcadas por dicha prohibición. No cabe en este caso inferir a contrario la existencia de obligaciones legales de actuar, por lo que la cláusula del artículo 11 CP se adivina en este caso de imposible aplicación a supuestos en que el mero transmisor no evite, por ejemplo, la circulación por sus redes de información lesiva de derechos de propiedad intelectual, lo que de acuerdo a la filosofía que inspira la Directiva parece acertado. Ya vimos, por lo demás, que los supuestos recogidos en las letras a), b) y c) del artículo 12.1 DCE no se refieren propiamente a la pura transmisión de datos ajenos sino que contienen supuestos de actuación a título propio, especialmente clara en la letra c) donde el presupuesto de hecho consiste en la selección o modificación de los datos por el propio intermediario, razón por la cual, la responsabilidad se ventilará vía autoría activa, en su caso.

Cuestión distinta es la que acontece en los supuestos de alojamiento de datos, quizá los más problemáticos. Al tiempo que la Directiva exime al intermediario de la obligación de supervisión, permite a los Estados la imposición de específicos deberes de actuar una vez comunicada la presencia de contenidos ilícitos en el *host* al administrador del servicio, o en aquellos casos en que el administrador los conozca por vías diversas a la comunicación de la autoridad administrativa o judicial. En concreto, se faculta a los Estados al establecimiento en las legislaciones nacionales de obligaciones de comunicación a la autoridad de los contenidos ilícitos así como de protocolos de actuación para la retirada inmediata del contenido, la suspensión del servicio o la obstaculización del acceso. Con ello se favorece la inclusión en Derecho interno de obligaciones legales que posteriormente sirvan a la fundamentación de posiciones de garantía es decir, que permitan acreditar la concurrencia de deberes jurídicos de actuar que, por omitirse son estructuralmente equivalentes a la causación activa del resultado material. Pues, si la asunción de una posición de garantía respecto a los contenidos ajenos debe encontrar un fundamento de legalidad, difícilmente podrá acudirse en este contexto a los supuestos de control de una fuente de peligro derivada de la realización de actividades de riesgo, pues ello no puede afirmarse como norma en Internet. En efecto, como ha podido establecerse por la

[65] *Vid.*, el planteamiento con detalle en **JOFER, R.,** *Strafverfolgung, op. cit.*, p. 127; **SIEBER, U.,** *Strafrechtliche (II), op. cit.*, pp. 9 y ss.

doctrina más autorizada[66], Internet no es un medio socialmente peligroso sino, contrariamente, un medio socialmente adecuado en el cual, ciertamente, el riesgo de lesión de otros bienes jurídicos existe. Pero ese no es el dato que caracteriza, como en el caso del tráfico rodado, la actividad que se desarrolla en aquél medio, por lo que no puede afirmarse que la realización de la actividad del Proveedor de servicios cuando ésta consiste en el alojamiento de contenidos ajenos o la omisión de la comunicación a las autoridades, constituya una *ocasión de riesgo para el bien jurídicamente protegido basada en la acción u omisión precedente*. La realización de actividades arriesgadas en algunas operaciones en Internet, tales como la utilización de tarjetas de crédito en entornos no seguros (sin cifrado o firma electrónica) o el envío de datos a través de instrucciones que se ejecutan mediante CGI, no convierten la estructura formal de Internet en un foco de peligro[67].

Y mientras la Directiva es traspuesta en los diversos Estados miembros, continúa apareciendo el interrogante de si los deberes que aquella autoriza a los Estados a imponer en las legislaciones nacionales pueden ser inferidos con carácter supralegal, en función de la arquitectura misma del sistema. Una conclusión de estas características pasa naturalmente por una interpretación laxa de las fuentes de deber jurídico de actuar consignadas en el artículo 11 CP, que ahora deberán considerarse como una lista ejemplificativa en la que el legislador, fundamentalmente, habría buscado un modo de entender incluida la injerencia como fuente de obligaciones de actuar sin que ello supusiera la exclusión de otras vías de asunción de la obligación de actuar a modo de barrera de contención del riesgo. Admitida dicha posibilidad, la tipificación de la Ley y el Contrato no impedirían la equiparación de la asunción fáctica del deber jurídico[68], especialmente en aquellos casos en que, como sucede

---

[66]**SIEBER, U.,** *Strafrechtliche (II), op. cit.*, p. 7; También en Juristenzeiutung (JZ), 9, 1996; **PICOTTI, L.,** *Fondamento e limiti della responsabilità penale dei* Service-Providers *in Internet*, notas 6 a 9.

[67]Recurriendo de nuevo a la obra de **SIEBER, U.,** *Strafrechtliche Verantwortlichkeit, op. cit.*, se comparte la opinión de que la fuente de peligro, cuando pretende fundamentarse una responsabilidad a título de comisión por omisión a través del requisito de la posición de garantía, debe serlo por sí misma, pero no por la intervención autónoma de un tercero. De todos modos la reflexión sirve aún como juicio de presente, pero no puede garantizarse su vigencia en el futuro. La socialización de Internet implica, de acuerdo a la filosofía subyacente en la propia Directiva del Comercio electrónico, su caracterización como medio estructural al desarrollo económico, social y humano; consecuentemente, en cuanto la utilización exponencial en términos de desarrollo social económico y humano de Internet mantenga una estrecha relación con las vulnerabilidades intrínsecas al sistema podrá llegar a hablarse de un sector de riesgo en el que la adopción de medidas de seguridad sea obligatoria (*v.gr.*, la utilización de sistemas de firma electrónica avanzada, como principio)

[68] Desarrolla ampliamente dicha posibilidad, **SILVA SÁNCHEZ,** *El nuevo Código Penal, op. cit.*, p. 68. El autor recurre a dos modelos posibles para solventar la paradoja que podría llegar a plantearse ante una exclusión de la órbita del artículo 11 CP de la asunción fáctica del compromiso de actuar. Por una parte, la consideración de las letras a) y b) del artículo 11 CP como una lista de carácter ejemplificativo, situación de la que se parte en el texto; de no aceptarse dicha premisa, equiparando la asunción fáctica a los casos de incremento del riesgo por la acción u omisión dolosa precedente. En ambos casos, podría llegar a fundamentarse la responsabilidad del prestador del servicio de alojamiento cuando tiene conocimiento de la ilicitud de los datos contenidos en su Servidor y no impide en los términos que más abajo se explicitarán, la conexión a los mismos o no procede a su inutilización, especialmente si se tienen en cuenta las consideraciones efectuadas en la mota precedente.

ahora, la distribución de roles en el funcionamiento ordinario de Internet lleva aparejada la confianza en que cada operador cumplirá con las funciones que le son inherentes. Desde esta perspectiva, y descartado el deber de supervisión o búsqueda activa de contenidos ilícitos, restaría por analizar la concreción de la obligación fáctica asumida por el intermediario cuya misión consiste en el alojamiento de datos, en cuyo caso deben distinguirse dos tipos de supuestos.

a) Conductas que impliquen una actividad de control expresamente asumida por el proveedor, como sucede con la moderación de grupos de noticias así como con los usuarios que utilizan el *linking*, es decir, supuestos en los que el titular de una página incluye en su contenido enlaces o links a otro tipo de servicios en los que se alojan contenidos ilícitos[69], tales como pornografía infantil o contenidos abiertamente injuriosos. Pues, tales supuestos, al igual que sucede con los contenidos sobre los que el administrador del sistema de alojamiento se atribuye una función de moderación y filtrado (por ejemplo, Grupos de Noticias), llevan aparejada la asunción de los deberes propios de dicha función y, en esa medida, acarrean la obligación de control previo de la información o los datos circulantes o alojados[70]. En el caso de la difusión de pornografía infantil, bastaría el conocimiento del contenido de lo difundido[71], para poder entender dicha conducta encuadrada en el concepto de facilitación de la difusión, especialmente a la vista de la facilidad con la que técnicamente podría desprender la información (en el caso de grupos moderados) o los links expresamente generados a páginas de pornografía infantil (en el caso de usuarios que utilizan la técnica del *linking*) lo que, en cambio, no le sería exigible al prestador de acceso, aun cuando tuviera conocimiento de que por la red cuyo acceso gestiona están siendo enviados contenidos ilícitos. En este grupo deberían también incorporarse los Grupos de Noticias no moderados alojados en servidores en los que, no obstante, el destinatario del servicio que los aloja actúa bajo la autoridad de del prestador del servicio de alojamiento en consonancia con la excepción a la exención general del artículo 14.2 DCE, puesto que en tales casos se trataría de contenidos propios de un destinatario que al actuar bajo la autoridad del servidor convierte los contenidos en directamente propios del intermediario en que se alojan los datos y

---

[69] En relación con estos últimos, el problema se planteó específicamente en Alemania donde, como ha puesto de relieve **JOFER, R.,** *Strafvervolgung im Internet*, Frankfurt, 1999, pp. 155 y ss., la Ley de Servicios telemáticos (TDG) distingue entre proveedor de acceso y servicio, sin alusión directa al concepto de usuario, lo que provocaba que, quien ofrecía en su página links a contenidos ilícitos instalados en otra ajena, pudiera llegar a beneficiarse extraordinariamente de su indefinición, y quedar exento de responsabilidad criminal al ser considerado un mero proveedor de acceso –evidentemente, de acceso al lugar en que realmente se encontraban alojados los contenidos-. La misma situación parece provocar la DCE, en cuanto el usuario parece quedar extramuros del ámbito de aplicación subjetiva de las directrices en materia de responsabilidad, al no quedar abarcados por el concepto de "prestador de un servicio dela sociedad de la información".

[70] En la tensión entre libertad responsabilidad sitúan este tipo de supuestos **FLECHSIG, N./GABEL, D.,** *Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks*, en Computer und Recht, nº 6, 1998, pp. 357 y s. Tensión que se clarifica una vez sobrepasado el umbral de la relevancia penal, lo que sucede en estos casos a través de conductas de autoría o participación, que serán determinadas en función del tipo de link establecido, el nombre que se encuentre detrás del mismo, su temática, etc. *Ibidem*, pp. 365 y s.

[71] Cfr., **WIDMER, U./BÄHLER, K.,** *Strafrechtliche, op. cit.*, p. 181.

sobre los que lógicamente no cabe negar la obligación de control, independientemente de que exista o no un compromiso del intermediario sobre su moderación (*v. gr. News* en los que el mensaje enviado corresponde a un destinatario de servicio que actúa en nombre del intermediario, a su vez proveedor del servicio de hospedaje)

b) Aquellas otras en las que el intermediario se limita a contratar el alojamiento en su servidor de determinados datos sin cláusulas que le obliguen al control de la información, como sucedería en el alojamiento de Grupos de Noticias no moderados (y, claro está, no sometidos a control del proveedor) o de ficheros recuperables vía *ftp*. La Directiva del Comercio electrónico parece adoptar en este punto una política de mínimos, a través de lo establecido en el artículo 14, en cuanto la única exigencia para el sometimiento del intermediario al régimen de responsabilidad correspondiente radica en el conocimiento efectivo de la información ilícita alojada en su servidor. Ahora bien, dicha circunstancia, cuando queda perfectamente acreditada y la continuación de la actividad delictiva depende sólo y exclusivamente del mantenimiento del servicio por quien viene prestándolo, nos situamos ante el deber general de impedir delitos y ante el problema ya reseñado al estudiar la posibilidad de imputar activamente a título de participación necesaria la continuación en el almacenaje de datos: la ausencia de conexión objetiva entre el resultado típico y la prestación (neutra) del servicio. Ahora bien, si se parte de la imposibilidad de una autoría o participación activas, la omisión del deber de comunicación a las autoridades establecido en la cláusula de cierre del artículo 15 DCE o la omisión del deber de supresión o bloqueo del contenido ilícito instaurado en el artículo 14.1 letra b) de la misma norma, podrían quedar integradas en la injerencia como fuente de equiparación entre acción y omisión; injerencia, en todo caso, derivada de la asunción fáctica de la obligación de control en estos casos, en cuanto inherente a la prestación del servicio[72]; la alternativa, posiblemente, la impunidad de un amplio abanico de conductas hasta tanto no constituyan derecho positivo las específicas obligaciones de actuar de cada uno de los intermediarios que prestan sus servicios en los procesos de transferencia de datos de la Sociedad de la Información.

A partir de aquí, el Derecho comparado ofrece datos de indudable interés. Para aquellos casos en que la estructura del delito no impide la realización del hecho en comisión por omisión, y presupuestos el conocimiento de la actividad ilícita desarrollada a través del servicio técnico prestado y su mantenimiento doloso, la aplicación de algunas de las propuestas de Derecho Comparado difieren la exigencia de responsabilidad a la verificación de que el servicio administrado por el *Provider* se encuentre técnicamente capacitado para la suspensión del servicio que aloja en sus ordenadores, como sucede con la TLD alemana, enervando el nacimiento de responsabilidad en caso contrario. La capacidad técnica, pese a no aparecer en la normativa extrapenal (en la Directiva) como criterio de limitación de la

[72] En tal caso, el conocimiento de la ilicitud penalmente relevante de los datos alojados bajo la exclusiva en la gestión y el dominio sobre la información situaría al prestador del servicio como compromisario de la contención de un riesgo conocido cuya materialización en el resultado típico sólo él está en condiciones de evitar.

responsabilidad, constituiría en todo caso un elemento estructural inherente a la modalidad comisiva por omisión, pues evidentemente la posibilidad de evitación del resultado depende de la capacidad real de actuación de quien se encuentra obligado a ello, al modo como sucede en los delitos de impago de prestaciones económicas del artículo 227 CP, donde la capacidad económica del obligado constituye *conditio sine qua non* para la realización material –y no sólo formal- del injusto; y, consecuentemente, condiciona la valoración sobre la acción omitida y la equivalencia estructural (normativa) entre las conductas activas y la omisión de la acción debida[73].

A la posibilidad de empleo de mecanismos técnicos de suspensión del servicio, como paso previo para ventilar responsabilidades penales de los intermediarios, la legislación alemana añade una cláusula de exigibilidad al prestador del servicio, de modo que la suspensión de éste al proveedor además de serle técnicamente posible debe serle así mismo jurídicamente exigible[74]. Sobre el sentido y alcance de dicha cláusula[75], se ha oscilado entre su proyección a la culpabilidad, en términos de "razonabilidad[76]" o su inclusión en la estructura misma del injusto, habida cuenta el mayor juego interpretativo que de la misma podría extraerse partiendo de los principios de proporcionalidad y ponderación de intereses[77]. Y es desde esta última perspectiva desde la que parece más razonable contemplar el requisito contenido en

[73] La verificación de este extremo, al margen ahora del derecho sustantivo deberá acreditarse mediante la realización de prueba pericial, dada la complejidad de los sistemas de anulación de contenidos. De hecho, si el caso *Compuserve* marcaba la tónica de lo que técnicamente no era posible –la anulación de contenidos por quien únicamente proveía el acceso- el asunto Yahoo.fr ha supuesto un punto de inflexión, tras el dictamen emitido por Vinton G. Cerf, según el cual la desconexión puntual por el proveedor de acceso respecto de determinados contenidos sería técnicamente viable. Claro que, si la capacidad depende de una técnica sólo al alcance de quienes poseen conocimientos especiales que trascienden al hombre medio (colocado en la situación del autor) no podría afirmarse que el intermediario ha omitido propiamente la acción a la que venía obligado, situando la mera transmisión o acceso a la red extra muros de la lógica jurídico penal.

[74] Evidentemente como conceptos separables, pues carecería de sentido un entendimiento de la exigibilidad, por excesivamente dilatado, que fuera más allá de lo que estrictamente posible en términos técnicos. Amén de la incongruencia que comportaría la acumulación de ambos conceptos en el mismo plano normativo. Así, **DERKSEN, R.,** *Strafrechtliche Verantwortlichkeit für internationalen Computernetzen verbreitete Daten mit strafbarem Inhalt*, NJW, 1997, p. 1885; le sigue en este punto, **JOFER, R.,** *Strafverfolgung*, *op. cit.*, p. 147.

[75] Especialmente en cuanto de la TDG alemana afecte al ámbito penal, habida cuenta del diverso significado que la exigibilidad (*Zumutbarkeit*) o su contraria (*Unzumutbarkeit*) adoptan en las diversas disciplinas jurídicas. Sobre ello, ampliamente, **SIEBER, U.,** *Strafrecht und Strafprozessrecht*, en **SIEBER/HOEREN,** Multimedia Recht, Teil 19, febrero 2000, nn. Mm. 318 y ss.

[76] Así, la Sentencia del Tribunal de Munich en el caso *Compuserve*, en el que el comportamiento razonablemente esperable del autor se manifiesta desde parámetros netamente subjetivos. Cfr. Los términos de la resolución, y la crítica, en **SIEBER, U.,** "*The Compuserve Judgment of the local Court Munich dated May 28, 1998, op. cit.*, pp. 28. y s.

[77] Particularmente, en este sentido, **FORNASARI, G.,** *Il ruolo, op. cit.*, pp. 3 y ss. El autor afirma que "Los criterios de razonabilidad y proporción llevan consigo una mayor riqueza de contenidos que la exigibilidad: pues imponen la necesidad de acudir no tanto a una particular y excepcional situación subjetiva sino también y sobre todo a una ponderación entre los bienes, el nivel de probabilidad de su violación, la dificultad y el nivel real de eficacia de la intervención impeditiva y en definitiva, la posibilidad, no remota de que la intervención misma, una vez realizada produzca indeseables efectos perjudiciales en la esfera de terceros ajenos y no responsables de compotamiento ilícito alguno".

la TDG alemana, al menos desde la lógica de la Directiva. Si el criterio de exigibilidad se analiza desde la óptica de la categoría dogmática de la culpabilidad, en términos puramente subjetivos podría obviarse la exención del artículo 15 DCE, que impide la imposición de obligaciones generales de supervisión o la parcela de impunidad prevista para los simples transmisores de información, afectando además parcelas de actuación de terceros ajenos. Por el contrario, desde la sistemática impuesta en materia de responsabilidad por la Directiva, parece razonable inferir que el carácter exigible de las medidas que debe tomar el proveedor y cuya omisión pueda derivar en la ventilación de responsabilidades de carácter jurídico penal se circunscribe a aquellos aspectos en que la salvaguarda del bien jurídico es inherente a la función misma desempeñada como controlador del tráfico de datos, en cada uno de los roles que el intermediario puede asumir en el estado actual de la técnica.

3. Locus comissi delicti

Si la responsabilidad de los Proveedores de Servicio queda enmarcada en un contexto restrictivo en nuestro país, su exigencia cuando se cumplen los requisitos de legalidad puede verse incrementada por el carácter anárquico y mundial de las redes. Internet, como se constató en líneas precedentes, responde en todos los rincones del planeta a protocolos de transmisión y recepción de datos de carácter universal, lo que facilita que el flujo de datos no sea homogéneo sino que los mismos circulen de un lado a otro del globo para atravesar distancias de apenas unos metros entre el ordenador que envía y el que recibe. La determinación del lugar de comisión del delito, juega entonces un papel fundamental en la ampliación de posibles responsabilidades del proveedor de servicios. Si el principio de territorialidad rige la determinación del lugar de comisión del hecho, éste admite excepciones en determinados supuestos. La legislación penal nacional, entonces, puede extenderse sobre conductas realizadas fundamentalmente en otros Estados, pero cuyas consecuencias (las del hecho delictivo) se extienden hasta nuestras fronteras. De modo que, lo que en el lugar en que reside el servidor es completamente lícito en términos de responsabilidad jurídico-penal, puede, en cambio, ser constitutivo de delito en alguno de los Estados por los que la información transita; Estados que, en uso de su soberanía, pueden extender la aplicación de su ley penal hasta las conductas que, aún iniciadas en otro País, dejan sentir en aquél sus efectos, siquiera parcialmente. Esta extensión de la jurisdicción, que en según que casos, puede resultar oportuna (piénsese, por ejemplo, en supuestos de distribución de pornografía infantil) podría llegar al absurdo de que el *Provider* hubiera de conocer las legislaciones civiles, administrativas, pero sobre todo penales, de la totalidad del globo[78]. Frente a ello, como algún autor ha reclamado, únicamente cabe el recurso al

[78] **SIEBER, U.,** *Legal Aspects of Computer-related Crime in the Information Society –COMCRIME-Study-*, version 1.0 of 1st January 1998, pp. 133 y s. En l doctrina italiana, **SEMINARA, S.,** *La pirateria op. cit.*, pp. 72-73, advierte, además, del indiscriminado poder que la Autoriadad judicial italiana (por ejemplo) asumiría, al declararse en tal "competente para todos los delitos cometidos en cualquier parte del mundo, via *Internet*". Pero igualmente, alerta el autor del riesgo de impunidad prácticamente absoluta que conllevaría la aplicación de la regla del *locus regit actum*, al quedar sin sancionar por la legislación nacional en la que se producen los resultados típicos los hechos producidos desde el extranjero.

Tratado Internacional[79], lo cual sitúa al problema de la responsabilidad en el mismo punto en que actualmente se encuentra el debate de la "delincuencia informática" en general: en el carácter transfronterizo y la necesidad de homogeneización no sólo de los casos en que el intermediario puede responder penalmente cuando actúa como tal, sino de los delitos específicos en los que habitualmente se verá envuelto –tal y como se ha visto, generalmente a modo de partícipe. De lo contrario, la diversidad de legislaciones penales implicadas en el tráfico jurídico internacional puede hacer en términos de error iuris imposible la depuración de responsabilidades[80] y en términos de funcionamiento práctico de la administración de Justicia, imposible el sometimiento a la justicia penal de un país al ciudadano extranjero que desde su país realiza una conducta jurídico penalmente relevante sólo en el país de destino de los datos.

[79] **SIEBER, U.,** *Legal Aspects, op. cit.,* p. 134.

[80] Piénsese en los casos en que la pornografía infantil es considerada como tal en un país determinado exclusivamente bajo la aparición de menores de edad (¿14, 15, 16, 17, 18 años?) reales, frente a aquellos en los que la tipificación de la distribución de pornografía infantil abarca los casos de pornografía técnica o pseudopronografía (también denominada pornografía virtual) y de pornografía pseudoinfantil. En este sentido, sería deseable el acuerdo a través de iniciativas como la Propuesta de Convención del Consejo de Europa, (cfr. *Supra* nota 11 y el texto de referencia), cuya dificultad radicará en la creación artificial de normas escasamente debatidas y proyectables territorialmente sobre culturas socio jurídicas radicalmente distintas.