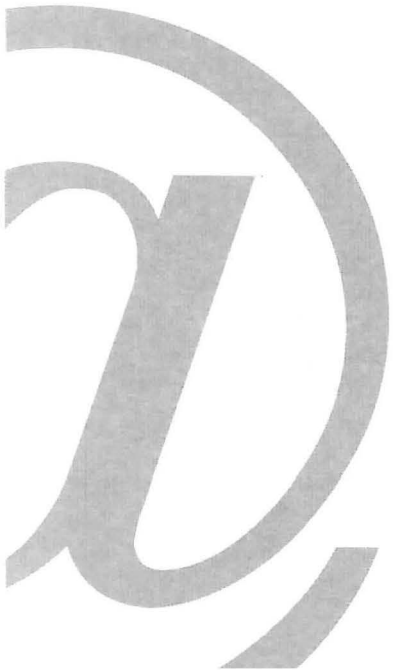

Internet: Perpectivas de Futuro

Amalia Cuena Boy

INTERNET: PERSPECTIVAS DE FUTURO

Mesa redonda celebrada en Cáceres, en las jornadas de Derecho e Internet el 24 de noviembre de 2000.

No cabe duda de que Internet es el fenómeno estelar de las nuevas tecnologías, que contribuye decisivamente a la eliminación de fronteras culturales, geográficas y políticas. Esta internacionalización de las comunicaciones y globalización de la información que supone la red, produce sus efectos en numerosos ámbitos de nuestra vida, en nuestro ocio, trabajo, consumo... y también en el derecho, ámbito al que me voy a referir especialmente, dada mi condición de jurista; todo ello sin ánimo de dar soluciones definitivas, y si solo de poner en esta mesa una serie de puntos que nos inviten a todos al debate y a la reflexión.

Por lo que se refiriere a la relación entre Derecho Penal e Internet, se manifiesta esta influencia en dos fenómenos:

1. Que a través de la red es posible cometer, y se están cometiendo, hechos delictivos.
2. Que con frecuencia se comenten delitos que podríamos denominar transfronterizos, es decir, delitos cuya persecución escapa del tradicional principio de territorialidad de la ley penal. De ello deriva otra importante consecuencia: la aparición de paraísos informáticos, esto es, lugares en los que por falta de legislación adecuada sea posible cometer hechos delictivos con absoluta impunidad.

Por todo ello creo, que desde el punto de vista del jurista, el gran reto estriba en la promulgación de normas que permitan paliar los efectos de una tecnología que carece de límites temporales y espaciales.

Esta relación entre desarrollo tecnológico, sociedad y derecho, que permite que a través de la red se cometan ataques contra bienes jurídicos penalmente tutelados, conlleva una problemática añadida, por el efecto multiplicador que

tiene la red, dado su carácter global o internacional, sobre estos ataques, revelándose como un medio idóneo para delinquir en cinco ámbitos:

1. Intimidad, honor y propia imagen, sobre todo por la potencialidad agresiva de la informática en relación con el tratamiento automatizado de datos de carácter personal (tema al que atienden las denominadas leyes de protección de datos); y mediante la posible difusión de ideas o noticias calumniosas o vejatorias.
2. .Propiedad intelectual, no solo a través de la piratería de software, sino mediante la distribución ilícita de todo tipo de obras; pensemos en el famoso formato digital de música, el mp3, que dio lugar a una demanda de las grandes discográficas contra el gigante de los mp3, el Napster, un programa que permite la descarga gratuita de este tipo de archivos.
3. Delitos contra la libertad sexual, al ser un medio idóneo para la difusión de pornografía infantil, actos sexuales violentos o forzados, prostitución...
4. Delitos contra la Hacienda Pública, pues numerosas paginas web permiten la realización de transacciones comerciales eludiendo el pago de impuestos, fundamentalmente el IVA, mediante la no identificación del lugar físico en que se realizan, a lo que se añade el hecho de que numerosas empresas desarrollan sus actividades en la red careciendo de cobertura física y teniendo un soporte meramente informático.
5. Seguridad del Estado y Orden Público, a través de la difusión de ideas racistas o terroristas, espionaje electrónico...

Además, y en todo caso, el carácter internacional de estas conductas complica y dificulta, más que su descubrimiento, su castigo, siendo difícil averiguar la identidad del delincuente, y lo que es peor, su conexión con el delito, y plantea problemas de jurisdicción competente, pues así como el Estado tiene un espacio físico delimitado por sus fronteras exteriores, Internet es un medio en el que el concepto de frontera no existe.

De este modo el tradicional principio de territorialidad de la ley, del poder penal estatal, quiebra a medida que la criminalidad va adquiriendo un componente global o internacional, al afectar a toda la comunidad internacional, y obliga a modificar la forma de afrontar la persecución penal de estos delitos por parte de los Estados.

La mayoría de los códigos penales y procesales nacionales, aceptan la existencia de delitos contra el derecho de gentes, perseguibles en cualquier país, como sucede en el nuestro con lo dispuesto en el articulo 23. 4º de la Ley Orgánica del Poder Judicial de 1985, que amplia, en su ultimo párrafo esta posiblidad a *cualquier otro* (delito) *que según los Tratados o Convenios Internacionales, deba ser perseguido en España*, lo que supone, en esta materia, dejar abierta una importante vía a la cooperación internacional.

No obstante, el problema de la jurisdicción y competencia se plantea de forma diversa en cada país. En el ámbito europeo, en general, la jurisdicción y competencia se determina por el lugar de causación del resultado; el caso *Mecklermedia*

lo ilustra: una empresa americana anunció en una página web un congreso denominado *Internet World*; otra empresa alemana organizó un congreso del mismo nombre, e igualmente anunció su contenido en una página web, redactada en inglés. La demanda se planteó en Gran Bretaña, y los tribunales de este país se estimaron competentes para conocer de ella, por entender, que al estar la página redactada en inglés, y no en el idioma de origen, es decir, en alemán, sus contenidos iban destinados a sus ciudadanos.

Esto es importante, pues los tribunales del país donde se producen los efectos del delito, pueden ser competentes para conocer de él, aunque haya sido cometido a través de un servidor ubicado en un país distinto.

En Alemania se sigue la teoría de la ubicuidad, de modo que el delito se entiende cometido tanto en el lugar donde se ejecuta como en el que se producen sus efectos, con las indudables ventajas que por ello, al menos desde mi punto de vista, esta doctrina conlleva.

En España, a los delitos cometidos en Internet, entiendo que les es aplicable la doctrina del Tribunal Supremo sobre los delitos a distancia, pues el lugar de ejecución, el lugar donde se ubica físicamente la máquina desde la que opera el delincuente, es, o puede ser distinto, a aquél en el que se producen los efectos de su acción.

En estos casos se enfrentan en la jurisprudencia del TS, las dos teorías de la acción y el resultado para determinar la competencia, no afirmándose la prevalencia con carácter exclusivo de una o de otra, debiendo atenderse a la condición y naturaleza del hecho delictivo de que se trate en cada caso.

En todo caso, la solución pasa por establecer una mayor cooperación jurídica internacional, mediante el establecimiento de un núcleo común de leyes.

En este sentido destacan los esfuerzos de la Unión Europea, por establecer una serie de mecanismos de cooperación.

Así, la Comunicación enviada por la Comisión al Parlamento Europeo, en octubre de 1996, distingue entre contenidos ilícitos y nocivos en Internet, sugiriendo el incremento de una mayor cooperación entre las partes con el fin de intercambiar una mayor información sobre los suministradores de contenidos delictivos, y establecer unos criterios mínimos europeos sobre contenidos delictivos. Además, para combatir la naturaleza transfronteriza de los delitos cometidos en la red, sugiere la necesidad de fomentar y establecer códigos tipo o códigos de conducta entre las asociaciones de proveedores de servicios de Internet, como medio para eliminar este tipo de contenidos.

La Recomendación del Consejo Europeo (R/95), de 11 de septiembre, aborda los problemas de las leyes procesales, derivados del uso las tecnologías de la información, insistiendo en una serie de puntos, de entre los que destaco los siguientes:

1. La necesidad de establecer medios, instrumentos y herramientas adecuadas de investigación penal a nivel internacional, al reconocer que la acción aislada de un Estado, en este ámbito, resulta ineficaz.
2. La cooperación con las fuerzas del orden público, a fin de garantizar la obtención de pruebas, de modo que a los proveedores de servicios de

Internet se les deba poder requerir la entrega de datos relativos a las comunicaciones a través de las cuales se han cometido los hechos delictivos investigados, a fin de permitir así la identificación de los usuarios de estos sistemas de comunicación.

3. Se insiste en la necesidad de compatibilizar los sistemas probatorios de los países, a fin de reconocer la eficacia probatoria en un estado, de la prueba o evidencia electrónica recogida en otro.
4. Todo ello, se refuerza con la recomendación de que las autoridades de un país deban autorizar la búsqueda de datos en sus propios sistemas informáticos, con la finalidad de transferirlos a un tercer estado, en una investigación penal.

Todas estas consideraciones ponen de relieve la complejidad del tema, sobre todo, y además de las dificultades apuntadas, porque la delincuencia en la red es una delincuencia especializada, que en ocasiones requiere unos conocimientos técnicos en el delincuente (piénsese en una transferencia electrónica de fondos), y que por esta misma razón, reclama la existencia de unos investigadores especializados.

Por ello, no es de extrañar que en la mayoría de los países se estén creando unidades especiales de policía para la investigación de estos delitos. Alemania fue el primer país que creo una policía del ciberespacio, fundamentalmente para perseguir la violencia y pornografía ilícita en la red. En España, la propia Dirección General de la Policía y la Guardia Civil han tenido que crear un grupo dedicado en exclusiva a los delitos informáticos y, como dato curioso, destaca el que el FBI, el 90% de los delitos informáticos que investiga, tiene relación con la red.

¿Qué es lo que sucede?. Lo que sucede, a mi modo de ver, es que la red no está pensada ni desarrollada para lo que esta ocurriendo. Internet ha ido creciendo de un modo caótico y desordenado (es lo que se llama autorregulación de la red, determinada por la interactividad de los usuarios), de modo que su propio diseño no esta basado en protocolos hiperseguros, hasta el punto de que hoy en día se estima que no existe un solo proveedor de servicios de Internet en el mundo que no haya sido objeto de algún ataque por parte de un pirata informático o *hacker*.

Y, desde este punto de vista de la seguridad, o más bien, de esta inseguridad en la red, resulta especialmente inquietante el uso de la criptología por parte de los delincuentes, tanto para ocultar sus mensajes, como para ocultar sus movimientos en la red, de modo que, aunque sean detectados, no se pueda saber con exactitud en que consisten, al aparecer los archivos encriptados.

La criptología es una técnica de cifrado, destinada a ocultar el contenido de los mensajes enviados entre dos partes: emisor y receptor.

Y, esto que así dicho, en principio no debería revestir mayores problemas, se ha convertido en el punto clave de un importante debate, al estar en el punto de mira de la mayoría de los gobiernos del planeta:

-En algunos países, como en China, está completamente prohibido el uso de los mensajes cifrados.

-En otros, como en EEUU su uso está fuertemente controlado, prohibiéndose, hasta 1996, la exportación de este tipo de programas de cifrado, al considerarse legalmente equiparado por el Acta de Control de la Exportación de Armamento, a la exportación de fusiles y armamento diverso; desde esa fecha pasó a considerarse producto comercial, si bien, sujeto a licencia de dos años.

-Otros países permiten el uso en su territorio de la criptografía, si bien se exige que estos programas incluyan un *backdoor* o puerta trasera, es decir, un procedimiento que permita intervenir el contenido del mensaje cuando así se considere oportuno.

-En España, la Ley General de Telecomunicaciones, de 8 de abril de 1998, parte de la norma general del uso del cifrado, como medida de seguridad, si bien establece la obligación de los operadores de los servicios de telecomunicaciones de notificar a la Administración el uso de cualquier procedimiento de cifrado, a efectos de control según la normativa vigente, y los fabricantes que los incluyan en sus equipos, deben aportar igualmente los aparatos descodificadores a los efectos que reglamentariamente se establezcan (art. 52), lo que no deja de suponer una cierta merma de nuestra intimidad.

No obstante creo que negar a los poderes públicos la posibilidad de intervenir comunicaciones encriptadas, puede llegar a paralizar una investigación penal por un delito grave, por lo que debe admitirse su intervención, en el marco de una resolución judicial motivada, como medio para evitar la impunidad de determinados hechos delictivos.

Pese a ello, en tanto el artículo 52 del texto legal citado no sea objeto de desarrollo, la negativa del emisor o del receptor a entregar a la autoridad judicial las claves, una vez acordada una intervención judicial de los mensajes electrónicos, no constituye delito alguno. Esta negativa constituiría, efectos de prueba, un mero indicio a valorar en conjunto con el resto del material probatorio obtenido.

Lo expuesto enlaza con el problema relativo a la forma de intervención de las comunicaciones electrónicas a efectos de su validez como prueba en un proceso penal.

Aunque se trate de una tecnología diferente, de lo que no cabe duda alguna es que el régimen procesal de intervención es análogo al de las comunicaciones telefónicas tradicionales (art.579 de la LECriminal), y requiere, por tanto, de la necesaria autorización judicial, siendo de este modo nula, la interceptación meramente policial –o, desde otra perspectiva, privada, la cual además sería constitutiva del delito previsto en el art.197 del CP-, sin respetar las garantías impuestas a la limitación a este derecho fundamental tanto por el TEDH como por nuestro TC (STC 49/1999, de 5 de abril).

Por todo ello, entiendo que la declaración contenida en el artículo 18.3 de la CE, *se garantiza el secreto de las comunicaciones, y en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial,* comprende todas las comunicaciones, también las telemáticas. En este sentido, la STS de 8 de febrero de 1999, a propósito de la intervención de un teléfono móvil mediante un *scanner*, señaló que *el ámbito de protección de este medio de comunicación no tiene limitacio-*

nes derivadas de los diferentes sistemas técnicos que puedan emplearse. No sólo la primitiva telefonía sin hilos, sino también las modernas formas de interconexión por satélite o cualquier otra señal de comunicación a través de las ondas se encuentra bajo la tutela judicial.

Por tanto, un mensaje de correo electrónico, de modo análogo a un mensaje telegráfico, una vez acordada judicialmente su intervención, requiere las mismas garantías, y en especial, un control directo del juez instructor, debiendo ser éste, y no la policía, quien realice la observación directa, mediante la remisión de copias de los mensajes almacenados en el servidor.

Aunque a todo ello se añade las grandes las dificultades probatorias que en la mayoría de los supuestos se producen en estos delitos, al ser posible destruir en poco tiempo toda huella física del mismo, no se debe en ningún caso olvidar extremar las garantías legales, de modo que el acceso a un domicilio al objeto, por ej. de examinar el disco duro de un ordenador con el fin de obtener pruebas incriminatorias, deberá ir precedida de la correspondiente autorización judicial de entrada y registro, y el exámen y recogida de los archivos computerizados se deberá someter al mismo régimen procesal previsto para la interceptación de documentos y correspondencia, habida cuenta, que de ser necesario incautar un disco duro, posiblemente se encuentren almacenados en el mismo mensajes, documentos y archivos personales, que nada tengan que ver con los hechos delictivos investigados.

Desde otro punto de vista, el problema de la inseguridad, no se plantea solamente desde el punto de vista de la delincuencia, sino desde nuestra propia seguridad personal e intimidad: en Internet no existe garantía alguna respecto de la privacidad de nuestros intercambios, del tipo que sean estos, salvo que se utilicen técnicas de codificación y cifra. El rastro que dejan nuestras comunicaciones en los servidores de acceso es absoluto, hasta el punto de que nuestro correo electrónico podría ser impunemente leído. De ahí que se diga que en la sociedad global, la intimidad es un valor en baja.

Pensemos en el sistema de espionaje electrónico, conocido como ECHELON, que mantienen los aliados desde la 2ª Guerra Mundial, y que a través de una red de satélites propia y de sistemas de inteligencia artificial, puede mantener una vigilancia electrónica constante de todas las comunicaciones del planeta. En la misma línea, últimamente ha saltado a la prensa la noticia de que el FBI, ha desarrollado un sistema, denominado Carnívoro, que permite leer los documentos en la red de cualquier individuo considerado sospechoso por la Administración, teniendo capacidad para grabar comunicaciones electrónicas (Ciberpais, 23 de noviembre de 2000).

Llegamos así a al paradoja de que un sistema que se presume plural, participativo y abierto, ofrece la posibilidad de un control gubernamental casi total de los ciudadanos, produciéndose en términos orwelianos lo que se denomina el *control del gran hermano*, que alude al directo enfrentamiento entre privacidad de las comunicaciones- derecho fundamental consagrado en el art. 18 de nuestra CE, y de la mayoría de los países democráticos- y control gubernamental, problema que se agrava en Internet, ya que los mensajes pueden permanecer en el

ciberespacio por tiempo indefinido, sin tener nosotros consciencia de ello, o de donde estará almacenada o copiada nuestra comunicación.

Esta problemática, no obstante, ha tenido eco en el seno de la Unión europea, y ha cuajado en una Directiva, la 97/66, del Parlamento Europeo y del Consejo, de 15 de diciembre, relativa al tratamiento de los datos personales y protección de nuestra intimidad, con el objetivo de armonizar las legislaciones de los estados miembros para garantizar un nivel de protección adecuado de nuestra intimidad, sobre todo en lo que respecta al tratamiento de nuestros datos personales en el sector de las telecomunicaciones.

Se exhorta al proveedor de un servicio público de telecomunicación a la adopción de las medidas necesarias para preservar la seguridad de sus comunicaciones, e incluso de avisar al usuario en el caso de que se produzca algún riesgo o ataque a esta seguridad.

En cumplimiento de esta Directiva los Estados miembros deben poner en vigor las disposiciones legales necesarias para darle cumplimiento, lo que en España ha sucedido con la Ley de Protección de Datos de 13 de diciembre de 1999.

Ahora bien, existen determinadas condiciones bajo las que los datos personales podrían ser divulgados a un tercero, como por razones de seguridad nacional, o bien para prevenir la comisión de delitos, y así, su articulo 3º, prevé que la Directiva no se aplicará a las actividades no comprendidas en el ámbito de aplicación de Derecho Comunitario, y en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa y la seguridad del Estado, y siempre que se trate de materias penales.

Pasando al tema de la respuesta legislativa a la delincuencia informática, y sobre todo a la relacionada con el uso de la red, por ser esta la materia de esta mesa, nuestro Código Penal de 1995, contiene ya numerosas referencias a los delitos informáticos y a los derivados del uso de las tecnologías, tratando de superar el desfase que existía entre la anterior legislación y el desmesurado desarrollo de las nuevas tecnologías, ante la evidencia de su uso con fines delictivos.

El problema que se planteó en esta materia fue el de su forma de punición, pues lo que realmente sucede es que la tecnología informática, ha ofrecido nuevas y sumamente complicadas posibilidades de cometer delitos de tipo tradicional en formas no tradicionales.

Por ello, y de forma, a mi criterio, totalmente adecuada, nuestro Código Penal ha optado por adecuar los tipos penales preexistentes, junto a alguno de nueva planta, a las peculiaridades derivadas del uso de la tecnología, por entender que el mero uso de un ordenador como medio para cometer un delito (por ej. una estafa electrónica) o como objeto material del delito (destrucción, robo o hurto del propio equipo) nada añade al tipo común cometido.

No obstante, este es un tema controvertido, pues no existe ni tan siquiera consenso en cuanto al propio concepto de delito informático.

Personalmente creo que el delito informático, mas que una categoría especifica de delito, engloba una pluralidad de modalidades delictivas vinculadas de algún modo con el uso de las tecnologías.

Esto es acorde, desde luego, con la definición propuesta por el Departamento de Justicia Norteamericano, según la cual, delito informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución.

Y el concepto, así entendido, como se ha dicho, abarca los delitos cometidos contra el sistema, como los cometidos mediante el uso de sistemas informáticos.

No quisiera terminar esta intervención sin indicar que en nuestro CP la delincuencia informática no constituye una categoría autónoma (no hay un título especialmente dedicado a esta materia),sino que su tratamiento aparece disperso a lo largo del articulado que compone su parte especial.

La problemática relativa a los tipos penales en concreto, es objeto de otra ponencia, que se desarrollará a lo largo de estas jornadas, por lo que con estas reflexiones, finalizo mi pequeña aportación, agradeciendo a Grupo 3000, la posibilidad que me ha brindado de estar hoy aquí con todos ustedes.