Internet: Responsabilidades Legales

JAVIER RIBAS ALEJANDRO

Abogado especialista en Derecho Informático. Asesor Jurídico de SEDISI y BSA.

INTRODUCCION

El ciberespacio es un mundo virtual en el que los defectos, miserias y malos hábitos del ser humano se reproducen con la misma fidelidad que las virtudes. El efecto de aldea global generado por el entramado de redes y la proliferación de nodos en todo el planeta ayuda a la difusión inmediata de los mensajes y permite el acceso a cualquier información introducida en la red. A las reconocidas ventajas que ello supone se unen las distorsiones y los malos usos que pueden tener lugar en el sistema y que confirman una vez más que el mal no está en el medio utilizado sino en la persona que lo utiliza.

Actualmente se está produciendo un intenso debate respecto a la necesidad de prevenir y sancionar estos malos usos en la red de redes Internet y el objetivo de este artículo es localizar las distorsiones más habituales que se producen y resumir los argumentos que se han dado a favor de una legislación que regule el uso de la red y los criterios contrarios a esa regulación.

1. ARGUMENTOS A FAVOR DE LA REGULACIÓN

Los partidarios de la regulación se apoyan en la tesis de que las redes de telecomunicaciones como Internet han generado un submundo en el que los delitos son difíciles de perseguir debido a la propia naturaleza del entorno y a la

falta de tipificación de las modalidades de comisión y de los medios empleados. Entre los delitos, infracciones administrativas y malos usos que se pueden llevar a cabo en la llamada infraestructura de la información, destacan, sin ánimo de clasificarlos, los siguientes:

1.1 Delitos tradicionalmente denominados informáticos

A pesar de que el concepto de delito informático engloba tanto los delitos cometidos contra el sistema como los delitos cometidos mediante el uso de sistemas informáticos, cuando hablamos del ciberespacio como un mundo virtual distinto a la "vida real", me refiero al delito informático como aquél que está íntimamente ligado a la informática o a los bienes jurídicos que históricamente se han relacionado con las tecnologías de la información: datos, programas, documentos electrónicos, dinero electrónico, información, etc..

Incluyo también dentro de este apartado los actos que sólo constituirían una infracción administrativa o la vulneración de un derecho no tutelado por la jurisdicción penal, pero que en algunos países pueden llegar a ser delito.

Dentro de este tipo de delitos o infracciones podríamos destacar:

Acceso no autorizado: La corriente reguladora sostiene que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático no disponen en algunos países de preceptos que permitan su persecución.

Infracción de los derechos de autor: La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial. No existe una opinión uniforme sobre la responsabilidad del propietario de un servicio on-line o de un sysop respecto a las copias ilegales introducidas en el sistema. Mientras un tribunal condenó a un sysop porque en su BBS había imágenes scaneadas de la revista Playboy, en el caso LaMacchia, el administrador del sistema fue hallado no responsable de las copias de programas que albergaba su BBS. El recurso de los propietarios de sistemas on-line y BBS ha sido incluir una advertencia o una cláusula contractual que los exonera de responsabilidad frente a

un "upload" de un programa o fichero que infrinja los derechos de autor de terceros.

Infracción del copyright de bases de datos: No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan "downloads" de los ficheros contenidos en el sistema, pero prohibe el replicado de la base de datos o la copia masiva de información.

Interceptación de e-mail: En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

Estafas electrónicas: La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

Transferencias de fondos: Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático. A pesar de que en algunas legislaciones y en sentencias aisladas se ha asimilado el uso de passwords y tarjetas electrónicas falsificadas al empleo de llaves falsas, calificando dicha conducta como robo, existe todavía una falta de uniformidad en la materia.

1.2 Delitos convencionales

Al hablar de delitos convencionales me refiero a todos aquellos que tradicionalmente se han venido dando en la "vida real" sin el empleo de medios informáticos y que con la irrupción de las autopistas de la información se han reproducido también en el ciberespacio. También en este caso incluyo en este apartado actos que no son propiamente delitos sino infracciones administrativas o ilícitos civiles. No obstante, teniendo en cuenta el carácter global de Internet, alguna de las conductas reseñadas pueden constituir un delito en unos países y en otros no.

Espionaje: Se ha dado casos de acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera. Entre los casos más famosos podemos citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles. Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales.

Espionaje industrial: También se han dado casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y know how estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada.

Terrorismo: La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

Narcotráfico: Tanto el FBI como el Fiscal General de los EEUU han alertado sobre la necesidad de medidas que permitan interceptar y descifrar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles. También se ha detectado el uso de la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas. El notable avance de las técnicas de encriptación permite el envío de mensajes que, a pesar de ser interceptados, pueden resultar indescifrables para los investigadores policiales. Debe tenerse en cuenta que sólo en 1994 los jueces americanos concedieron 1.154 órdenes de vigilancia electrónica, de las cuales un importante número tuvieron resultado negativo a causa de la utilización de técnicas de encriptación avanzadas. Por ello, tanto el FBI como los fiscales americanos reclaman que todos los programas de encriptación generen puertas traseras que permitan a los investigadores acceder al contenido del mensaje.

Otros delitos: Las mismas ventajas que encuentran en Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas,

y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

1.3 Mal uso: cybertorts

Usos comerciales no éticos: Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo "mailings electrónicos" al colectivo de usuarios de un gateway, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red.

Actos parasitarios: Algunos usuarios incapaces de integrarse en grupos de discusión o foros de debate on- line, se dedican a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales, etc. Aunque la mayoría de estas conductas están previstas por los suministradores de servicios on-line, resolviendo el contrato con los reincidentes, existen algunos partidarios de que se establezcan normas para sancionar estos actos.

Obscenidades: Más adelante veremos la polémica generada por el proyecto de ley del senador Exon en EEUU respecto a una Communications Decency Act.

1.4 Efectos transfronterizos

Otro de los aspectos sobre los que se reclama una regulación es el de la competencia jurisdiccional en el caso de actos realizados en un país determinado pero que, debido a la extensión de la red, tienen sus efectos en otro país. Aunque el derecho internacional da solución a este tipo de conflictos, existen diversos criterios respecto a la determinación del lugar en el que se ha producido la infracción.

Así como en una radiodifusión vía satélite existe una conducta activa de emisión, sujeta a unas normas especiales, la introducción de una obra infractora en un host conectado a Internet. ¿debe entenderse también como un acto de difusión o comunicación pública?

La conducta activa o pasiva del presunto infractor es determinante para apreciar la existencia de la infracción y la competencia jurisdiccional. Si hacemos una comparación de las autopistas de la información con las autopistas de asfalto, deberíamos reconocer que no es lo mismo enviar camiones de reparto a todos los países y ciudades con vías de acceso, que tener una tienda abierta al lado de la autopista.

Un ejemplo de conducta pasiva sería el caso de Phil Zimmermann, investigado por exportar tecnología de doble uso a otros países. Zimmerman se limitó a introducir su programa de encriptación de clave pública PGP (Pretty Good Privacy) en hosts que se hallaban dentro del territorio de los EEUU, pero al estar estos hosts conectados a Internet, todos los países conectados a la red pudieron obtener una copia del programa. Zimmermann recibió numerosos mensajes de felicitación y agradecimiento desde países con embargo comercial y tecnológico. Este caso ha acabado siendo un exponente de la lucha entre el poder intervencionista del Estado y el derecho a la intimidad de la persona, como más adelante veremos.

Un ejemplo de conducta activa sería remitir una recopilación de imágenes pornográficas scaneadas a los mailbox de un país en que dicho tráfico estuviese prohibido.

2. ARGUMENTOS EN CONTRA DE LA REGULACION

Frente a la corriente reguladora se levantan los partidarios de que ciertas áreas queden libres del intervencionismo o proteccionismo estatal. Entre los argumentos más utilizados figuran el derecho a la intimidad y la libertad de expresión.

2.1 Derecho a la intimidad

Uno de los derechos más defendidos en los países en los que ha habido una gran implantación de los sistemas informáticos en la gestión de los datos de los ciudadanos por parte de la Administración, ha sido el derecho de la persona a que su intimidad no sea vulnerada por un abuso de estos medios. La protección de este derecho ha generado preceptos de rango constitucional en muchos países. En España, el artículo 18 CE garantiza el secreto de las comunicaciones y abre la posibilidad de que la Ley limite el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus

derechos. Del desarrollo de este precepto ha surgido hasta ahora la LORTAD como instrumento destinado a evitar que mediante el tratamiento automatizado de los datos se llegue a obtener el perfil de una persona, sus aficiones y sus hábitos. Con ello se reconoce que el uso de las tecnologías de la información permite una rapidez en la manipulación de datos que era impensable con el empleo de medios manuales o analógicos. En la discusión de la LORTAD se llegó a establecer la comparación de que los sistemas manuales equivalían a pescar con caña y los informáticos a pescar con red.

La misma frase se ha repetido al hablar sobre el poder del Estado al investigar las transmisiones efectuadas en la infraestructura de la información, y concretamente al interceptar y leer el e-mail. En la declaración de Phill Zimmermann ante el Subcomité de Política Económica, Comercio y Medio Ambiente de la Cámara de Representantes de los EEUU, puede leerse: "En el pasado, si el Gobierno quería violar la intimidad de los ciudadanos corrientes, tenía que gastar sus recursos en interceptar, abrir al vapor y leer el correo y escuchar, grabar y transcribir las conversaciones telefónicas. Eso era como pescar con caña, de uno en uno. Por el contrario, los mensajes de e-mail son más fáciles de interceptar y se pueden scanear a gran escala, buscando palabras interesantes. Esto es como pescar con red, existiendo una diferencia orwelliana cuantitativa y cualitativa para la salud de la democracia".

Con argumentos similares se está defendiendo la idea de que si los avances tecnológicos han creado un ciberespacio en el que cualquiera puede expresarse y comunicarse sin temor a ser oído por otros, el poder del Estado no debería ampliarse hasta poder controlar este nuevo mundo.

Por de pronto, el servicio secreto norteamericano ya ha sido condenado por introducirse sin mandamiento judicial en la BBS Esteve Jackson Games y leer el e-mail en ella depositado. El servicio secreto ha tenido que pagar una indemnización de 50.000 dólares al propietario de la BBS y 1.000 dólares a cada usuario de la misma, por haber vulnerado su intimidad.

2.2 Libertad de expresión

Pocas propuestas de ley han generado tanta discusión en Internet como la Communications Decency Act. Los detractores de este proyecto sostienen que no sólo prohibiría conversaciones públicas de contenido "obsceno, lascivo, sucio o indecente" sino incluso las de ámbito privado entre dos personas, con la posibilidad de sancionar al proveedor del servicio on-line. Los usuarios de

Internet americanos se niegan a tener que hablar constantemente como si estuviesen en un entierro. La aplicación de esta ley, además de ser un importante obstáculo para la libertad de expresión, exigiría una enorme inversión en la monitorización y vigilancia del sistema y generaría constantes intromisiones en la intimidad de los ciudadanos. Durante el mes de abril y mayo de 1995, ha habido un importante movimiento para conseguir firmas de oposición a este proyecto. La dirección donde debían enviarse los mensajes era s314-petition@netcom.com.

2.3 Libertad de acceso a la información

Una corriente de usuarios de la red considera que el derecho a la información está por encima de otros derechos como la propiedad intelectual, la propiedad de los datos el secreto que se da al know how. Los partidarios de esta idea consideran que cualquier tipo de obra introducida en la red debería pertenecer al dominio público, y solicitan la inaplicabilidad de los derechos de autor y la supresión de fronteras en el ciberespacio para permitir el libre flujo de la información en todo el planeta.

3.AUTOREGULACION: CODIGOS DE CONDUCTA Y CIBERPOLICIAS

Códigos de conducta: Por el momento, y a falta de una legislación específica, en Internet existen unos códigos de ética cuyo incumplimiento está castigado con la censura popular, lo cual acaba siendo, en algunos casos, más eficaz que una norma de derecho positivo. Es posible que un usuario se marque unas pautas de conducta de acuerdo con unas leyes, pero la distancia o la ausencia de control de los órganos de vigilancia pueden hacer que esas pautas se relajen. No obstante, si sabemos que podemos ser juzgados por nuestros compañeros de la red y somos conscientes de que de nuestro comportamiento en los debates on-line y en la emisión y recepción de mensajes dependerá la opinión que tengan de nosotros y la calificación de novato, informal o persona non grata que podamos recibir, actualizaremos nuestras pautas de conducta día a día.

Ello hace que la tónica normal en Internet sea de respeto entre los usuarios de la red, siendo los demás casos la excepción.

Sistemas de seguridad informática: Las propios sistemas de control de cada host garantizan un umbral de seguridad aceptable, aunque no impiden que

los archivos que circulan por la red puedan contener algún virus. Y en muchos casos pueden ser neutralizados por un programa generador de passwords.

Ciberpolicías: Tanto NSA, FIRST Forum of Incident Response and Security Teams y CERT Computer Emergency Response Team tienen equipos de especialistas dedicados a la localización de hackers, defensa frente a sabotajes e intervención en caso de siniestros informáticos. Por otra parte, algunas policías como el FBI y Scotland Yard disponen de unidades especiales para investigar la comisión de delitos a través de la red.

4. SITUACION ACTUAL Y PROPUESTAS LEGISLATIVAS

El Código Penal de 1995 contiene muchas referencias a los delitos informáticos y a los derivados del uso de las telecomunicaciones, entre las que podemos destacar las siguientes:

- Delitos contra la intimidad y el secreto de las comunicaciones
- Estafas electrónicas.
- Infracción de los derechos de propiedad intelectual
- Delito de daños
- Revelación de secretos contenidos en documentos o soportes informáticos.
- Falsedad en documento electrónico
- Fabricación o tenencia de útiles e instrumentos específicamente destinados a la comisión de delitos.
- Sustracción, destrucción, inutilización u ocultación de documentos electrónicos por parte de un funcionario público cuya custodia le esté encomendada por razón de su cargo.

Por otra parte, algunas leyes como por ejemplo la LORTAD, incluyen en su articulado referencias a la seguridad informática de las bases de datos.

Pero en general, los españoles estamos algo desprotegidos frente a la nueva categoría de delitos que hemos comentado en este artículo.

Proyectos de ley de EEUU: Después del atentado de Oklahoma, el gobierno norteamericano ha empezado a estudiar formas de investigación y prevención antiterrorista. Ante la sospecha de que en la organización del atentado se utilizara la red Internet para el envío de mensajes encriptados, la propuesta de

ley antiterrorista de los senadores Dole y Hatch incluyen la ampliación de las facultades del FBI en materia de vigilancia electrónica y rastreo de la red.

Otro proyecto de la Casa Blanca modifica las leyes que regulan la intimidad y la intervención de las telecomunicaciones (Privacy Act y Wiretap Act) para poder interceptar y desencriptar mensajes electrónicos enviados o recibidos por sospechosos o presuntos terroristas, con plena eficacia procesal como prueba documental incluso cuando dichas evidencias hayan sido obtenidas sin el correspondiente mandamiento judicial.

Este proyecto también prevé la asignación de una partida presupuestaria para que el Fiscal General pueda solicitar a compañías telefónicas, electrónicas y de seguridad informática el diseño de tecnologías de intervención de las telecomunicaciones.

Todo ello va acompañado de un intenso debate sobre las posibilidades de desencriptación y la posible vulneración del derecho a la intimidad, al que antes he hecho referencia.

GATT - Ronda de Uruguay: En los últimos acuerdos del GATT se hacen referencias al nuevo entorno económico y tecnológico y a la necesidad de acuerdos globales en materia de Propiedad Industrial e Intelectual, pero no se analizan a fondo ni se resuelven los problemas que se han mencionado en este artículo.

Reuniones del G7 respecto a la Global Infraestructure Information: Las conclusiones del G7 en sus últimas reuniones han supuesto un enorme esfuerzo de síntesis para resumir en unos puntos básicos las actuales necesidades en materia normativa, frente al reto de la sociedad de la información. A continuación se enumeran algunas de las conclusiones más significativas:

a) La necesidad de analizar el alcance del derecho de información frente a la seguridad de la información.
b) La conveniencia o no de seguir limitando la cobertura del copyright a la expresión, en un contexto en el que la expresión es a veces menos importante que la propia información.
c) La necesidad de modificar los conceptos tradicionales del derecho de autor.
d) La necesidad de proteger las herramientas de navegación en el nuevo contexto digital.

e) La necesidad de analizar el impacto en el derecho de autor de nuevos conceptos como "almacenamiento temporal", "browsing" y "cita digital".
f) La necesidad de que el uso de las tecnologías de la información también es importante para los países en vías de desarrollo.

Libro Verde: La Comisión Europea ha editado un Libro Verde sobre los derechos de autor y los derechos conexos en la sociedad de la información.

Entre las propuestas que contiene este texto cabe destacar:

a)La existencia de ventanillas únicas para contratar telemáticamente los derechos necesarios para crear obras multimedia, facilitando así la localización de los titulares y el pago de los royalties correspondientes a las imágenes, textos, sonidos y videos utilizados.

b)La determinación del derecho aplicable en los casos de infracciones transfronterizas a través de la infraestructura de la información.

c)La armonización del derecho de los estados miembro para proteger de manera uniforme los derechos de las obras multimedia y de las bases de datos que se hallen en la infraestructura de la información.

d)La necesidad de redefinir del concepto de reproducción por medios digitales, planteando la cuestión de si la digitalización de una obra y la copia privada deberán ser objeto de autorización por parte del titular o no.

e)La necesidad de definir el concepto de transmisión digital de una obra en el seno de la infraestructura de la información con el fin de determinar si constituye un nuevo acto que precisa autorización del autor o si, por el contrario, está integrado en otros derechos como el de cesión, distribución o comunicación pública.

f)La conveniencia o no de regular las medidas de protección, seguridad informática, passwords y encriptación.