La Sociedad Digital: Riesgos y Oportunidades

JAVIER RIBAS ALEJANDRO

Abogado Microsoft y SEDISI

El desafío que suponen las nuevas tecnologías nos obliga a observarlas desde una doble óptica. Si bien el temor inicial que suscita lo desconocido ha hecho proliferar una serie de tabúes que han encontrado en Internet el lado más morboso, la posibilidad de compartir, en tiempo real, cualquier faceta del saber humano, abre un mundo de oportunidades que, hasta hace poco tiempo, era inimaginable.

La imagen que ofrece Internet, asociada siempre a un espacio en el que resulta difícil aplicar la Ley, contrasta con la situación que se da en la realidad, tras el estudio de las normas de ámbito nacional e internacional y a partir de las experiencias procesales y la jurisprudencia existente hasta el momento.

A pesar de la novedad aparente de estas cuestiones, la materia a analizar es tan amplia, que nos obliga a limitar el objeto del debate a los siguientes puntos:

- Comercio electrónico
- Delitos en Internet
- Medios de control y prevención
- Responsabilidad del proveedor de contenidos
- Conflictos jurisdiccionales
- Problemática específica de los derechos de autor

1. Comercio electrónico

La revolución del comercio electrónico está llegando a nuestro país, y se espera que el próximo año sea el periodo de mayor crecimiento de esta modalidad, gracias a la consolidación de los nuevos protocolos que garantizarán la seguridad de las transacciones y al incremento de usuarios de la red.

El hecho de que el comercio electrónico en Internet vaya dirigido prioritariamente al consumo, y en especial, a la compra compulsiva, obliga a tener en cuenta los aspectos jurídicos de la transacción, tanto en la fase de preparación de la oferta, como en la de aceptación.

Las razones que impulsan a un usuario a permanecer en un web no son únicamente la utilidad y el interés de sus contenidos, sino también el atractivo de sus gráficos y el nivel de sorpresa que suscita cada sección. Ello conlleva un esfuerzo creativo que debe ser convenientemente protegido mediante las medidas habituales del Derecho de Autor y de la Propiedad Industrial. En este ámbito no se detectan lagunas legislativas, ya que recientes actuaciones en este ámbito han actualizado la normativa existente :

- Texto Refundido de la Ley de Propiedad Intelectual de 1996.
- Protocolo por el que se modifica el Convenio de Berna en materia de redes.
- Directiva sobre protección de bases de datos

Por otra parte, debe cuidarse el contenido del contrato on line, la adecuación de sus cláusulas a las especiales características de la contratación electrónica, y la forma en que se efectúa la transacción, con el fin de demostrar que el usuario ha prestado su consentimiento a las condiciones de la oferta.

La concurrencia de oferta y aceptación, pago y entrega, puede producirse en tiempo real o de forma diferida. El software, por ejemplo, que constituye el producto más vendido a través de Internet, puede ser transferido mediante ambas modalidades. A través de una transacción en tiempo real, el usuario efectúa un "download" del programa tras cumplimentar el formulario de pedido en un entorno seguro. En el caso de la transacción diferida, recibirá el producto o servicio a través de medios convencionales.

No obstante, no todas las transacciones podrán basarse exclusivamente en medios electrónicos: algunas operaciones bancarias, los negocios que deban formalizarse en documento público y la contratación de seguros de vida o altas en mutuas, que contengan datos relativos a la salud, exigirán la firma analógica original del usuario.

Otro problema relativo al comercio electrónico a través de Internet estriba en la aplicación de la normativa sobre venta a distancia, en especial, la reciente Directiva europea sobre la materia, que aporta las siguientes consecuencias :

- Plazo de siete días para la devolución de una compra realizada a distancia.
- Plazo de entrega de treinta días.
- Posibilidad del titular de una tarjeta de crédito de repudiar las transacciones en las que no ha habido una presencia física de la tarjeta.
- Necesidad de inscripción en el Registro de Empresas de Venta a Distancia.

Aunque estas normas son de enorme utilidad para proteger los derechos de los consumidores y usuarios en Internet, dejan a la empresa suministradora en una situación precaria que sólo será subsanada con la aplicación de los sistemas de firma digital y certificación.

Finalmente, en la Orden del Ministerio de Economía y Hacienda de 22 de marzo de 1996 se dictan las normas de aplicación del sistema de facturación telemática que ya había sido previsto en el artículo 88 de la Ley del Impuesto sobre el Valor Añadido y en el artículo 9 bis del Real Decreto 2402/1985.

La referida Orden define la factura electrónica como un conjunto de registros lógicos, almacenados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos, que documentan las operaciones empresariales o profesionales, con los requisitos exigidos para las facturas convencionales.

Los interesados en promover la implantación de un sistema de intercambio de facturación por medios telemáticos deberán solicitarlo al Departamento de Inspección Financiera y Tributaria de la Agencia Estatal de Administración Tributaria, que resolverá de forma expresa en el plazo de seis meses.

Los empresarios o profesionales que deseen operar como usuarios de un sistema de intercambio de facturación por medios telemáticos deberán solicitarlo al mismo organismo, que resolverá en el plazo de un mes. En este caso, el silencio administrativo se interpretará de forma positiva.

Los usuarios que utilicen el sistema de facturación telemática estarán obligados a conservar en soporte magnético u óptico y en el mismo orden de transmisión o recepción, e íntegramente, los ficheros de facturas transmitidos y recibidos. Asimismo deberán adoptar las medidas de seguridad necesarias para su conservación, y guardar un listado secuencial de las operaciones diarias efectuadas.

Los riesgos generados por el comercio electrónico se inician en el momento en que la empresa decide tener presencia en la red a través del correspondiente establecimiento de una tienda virtual. El dominio que va a identificar a la compañía en Internet puede haber sido reservado de mala fe por un especulador que solicitará una importante suma de dinero para formalizar su transferencia.

Los pedidos recibidos a través de un formulario electrónico pueden contener datos falsos, generados con programas que simulan el número de una tarjeta de crédito válida.

También puede producirse la interceptación de una transacción con el fin de alterar su contenido o acceder a las claves de las partes que participan en la misma.

Por todo ello, antes de poner en marcha un proyecto de comercio electrónico en Internet, es conveniente que se compruebe el cumplimiento, entre otros, de los siguientes requisitos:

- Protección mediante Propiedad Intelectual e Industrial del diseño gráfico del web, así como de sus contenidos (texto, gráficos, iconos, fotografías, animaciones, etc.) y código fuente (HTML, JAVA, VRML, CGI, etc.)
- Protección del dominio en Internet
- Establecimiento de los medios de prueba que permitan demostrar la aceptación del usuario
- Sistemas de certificación que garanticen la confidencialidad, autenticidad, integridad y no repudiación de la transacción

- Adecuación de los formularios de recogida de datos personales a la LORTAD
- Adecuación del contrato de adhesión a la Orden de 22/3/96 sobre facturación telemática
- Cumplimiento de los requisitos legales de la venta a distancia
- Medios de prevención de delitos informáticos
- Cláusula de arbitraje
- Seguro de responsabilidad civil específico

2. Delitos en Internet

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 Internet, lo cual obliga a localizar las distorsiones más habituales que se producen y a analizar 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.

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.

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.

Por el momento, y a falta de una legislación específica, en Internet existen unos códigos de ética (netiquette) 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 convenios internacionales y órganos supraestatales encargados de aplicarlos, pueden hacer que esas pautas se relajen.

Nuestro Código Penal contempla específicamente delitos que pueden ser cometidos a través de Internet , y que se relacionan a continuación :

Artículo 197 - Interceptación de correo electrónico
Artículo 197.2 - Cesión de datos reservados de carácter personal
Artículo 248 - Estafas electrónicas
Artículo 264.2 - Daños informáticos
Artículo 270 - Delitos contra la propiedad intelectual
Artículo 186 - Difusión y exhibición de material pornográfico a menores
Artículo 189 - Pornografía infantil
Artículo 211 - Difusión de mensajes injuriosos o calumniosos
Artículo 282 - Publicidad engañosa
Artículo 278 - Revelación de secretos
Artículo 390 - Falsedad documental
Artículo 256 - Uso de terminales de comunicación sin autorización

3. Responsabilidad del proveedor de contenidos

Existen diversas posturas sobre la atribución de responsabilidad por los contenidos introducidos en Internet o en una obra multimedia. Es conocida la existencia de una corriente que establece una comparación entre los proveedores de acceso o albergue y los editores, en el sentido de que ambos proporcionan el soporte material que permite a los autores la divulgación de los contenidos generados.

Según esta tesis, los PSI, deben responsabilizarse de los contenidos que publican, al igual que los editores lo hacen con sus obras.

Por ejemplo, Austria, Alemania, Francia, Reino Unido y España han regulado o están regulando los delitos de injurias y calumnias en el sentido de establecer la responsabilidad civil solidaria del propietario del medio de difusión utilizado para divulgar el mensaje injurioso o calumnioso. En España, este tipo penal está descrito en el artículo 212 del Código Penal.

Por el contrario, la segunda corriente asimila los PSI a los propietarios de librerías, de manera que se reconoce la imposibilidad de controlar el enorme volumen de información dinámica o estática que los usuarios introducen en el servidor.

Respecto a la imposibilidad de control de los contenidos de un servidor, cabe distinguir entre foros abiertos y foros cerrados. Sin tener en cuenta las dificultades técnicas de monitorizar todos los foros abiertos que haya en un servidor, podemos decir que no existen obstáculos jurídicos para observar, bloquear, e incluso eliminar los contenidos ilícitos localizados en un entorno WWW, FTP, News, etc. Por el contrario, la monitorización del correo electrónico y de las conversaciones privadas mantenidas en los foros cerrados del servidor podría constituir, en sí misma, un delito de interceptación de las telecomunicaciones, previsto en el artículo 197 del Código Penal español.

Por ello, cabe concluir que la responsabilidad del PSI sólo debería apreciarse cuando se demuestre un conocimiento directo de la existencia de los contenidos ilícitos, sin que se haya producido posteriormente un bloqueo de dicha información.

4. Medios de control y prevención

Los suministradores de acceso a Internet y los suministradores de servicios de ordenador central desempeñan un papel decisivo para dar acceso a los usuarios a los contenidos de Internet. Sin embargo, no se ha de olvidar que la responsabilidad primordial de los contenidos recae sobre los autores y los suministradores de contenidos. Por ello es imprescindible señalar con exactitud la cadena de responsabilidades con el fin de situar la responsabilidad de los contenidos ilícitos en sus creadores.

Algunos países han introducido una legislación muy amplia para bloquear todo acceso directo a Internet a través de los suministradores de acceso mediante la introducción de la exigencia de servidores "proxy" análogos a los que utilizan las grandes organizaciones por razones de seguridad, junto con "listas negras" centralizadas. Un régimen tan restrictivo es impensable en Europa, ya que atentaría gravemente contra la libertad individual y sus tradiciones políticas.

La norma PICS (Platform for Internet Content Selection, plataforma de selección de contenidos de Internet), que lanzó oficialmente el World Wide Web Consortium en mayo de 1996, constituye un intento de establecimiento de una

norma mundial para toda la industria. PICS, que ofrece un "control del acceso a Internet sin censura", está apoyada por una amplia coalición de fabricantes de material y programas informáticos, suministradores de acceso, servicios comerciales en línea, editores y suministradores de contenido. Actualmente se incluye como característica normal de la última generación de navegadores (browsers) de Internet, como Microsoft Explorer 3.0 y Netscape 3.0, y también cuenta con el apoyo de una serie de conjuntos de programas de filtrado.

Las recomendaciones a seguir por los propietarios de un servidor conectado a Internet podrían ser las siguientes :

- Establecer las correspondientes advertencias y cláusulas de responsabilidad civil en los contratos que regulan los servicios de acceso y hosting.

- Conseguir la autorización del usuario para comprobar el cumplimiento de las normas de uso del servidor y monitorizar los contenidos introducidos en las zonas públicas y privadas del servidor (WWW, FTP, News, etc.).

- Introducir un formulario público en el servidor , para que los usuarios que conozcan la existencia de un contenido ilícito puedan comunicarlo al administrador del sistema.

- Promover el uso de sistemas de filtrado tipo PICS que permitan el bloqueo de los contenidos nocivos.

- Elaborar normas de conducta y recomendaciones para el uso de redes y adjuntarlas a los contratos que regulen las relaciones con clientes y empleados.

- Contratar un seguro de responsabilidad civil en el que expresamente se amplíe la cobertura a los siniestros asociados a los contenidos introducidos en el servidor por los usuarios.

5. Conflictos jurisdiccionales

El ámbito global de la red genera una dificultad añadida a la hora de perseguir los delitos en Internet.

Imaginemos la siguiente hipótesis: un usuario de Internet brasileño que introduce una copia no autorizada de un programa americano en un servidor en las Islas Caimán con el fin de que lo copie un italiano.

En este caso, además de determinar el lugar de comisión del delito, a los efectos de designar la legislación aplicable y la jurisdicción competente para enjuiciar el caso, deberá tenerse en cuenta que el país en el que se halla el servidor pertenece a la categoría de los llamados paraísos fiscales, ahora convertidos en paraísos informáticos, que no han ratificado los convenios internacionales de propiedad intelectual o de auxilio a la administración de justicia.

La proliferación de casinos virtuales, bancos de datos personales, remailers anónimos y centros de distribución de copias no autorizadas de software, han hecho que los servidores situados en estos países aparezcan como refugio para la comisión de todo tipo de delitos.

No obstante, la combinación de los tradicionales procedimientos jurídicos con las propias soluciones tecnológicas que ofrece la red, permiten la investigación y la persecución de los llamados delitos transfronterizos. A las medidas de bloqueo en destino utilizadas hasta ahora, se añade la posibilidad de un bloqueo en origen, consistente en la retirada del IP (Internet Protocol) por parte de la IANA, entidad encargada de concederlo.

El IP es un número que identifica al servidor y lo hace visible en la red, de manera que su retirada impide el acceso a la información contenida en dicho servidor. Dicho bloqueo puede tener lugar como resultado de una sentencia judicial o de la concesión de medidas cautelares por parte de un órgano judicial.

La IANA es una asociación con sede en Estados Unidos, lo cual hace posible la ejecución de sentencias dictadas por órganos judiciales europeos.

Recientemente se han producido en nuestro país diversos procedimientos judiciales relativos a presuntos delitos que utilizaban la red Internet como medio de comunicación. Los efectos transfronterizos de algunas de las actividades denunciadas obligan a determinar cuál debe ser la jurisdicción competente para enjuiciar los delitos que tienen origen en un país y causan sus efectos en otro.

La Ley Orgánica del Poder Judicial establece en su artículo 23 que corresponderá a la jurisdicción española el conocimiento de las causas por delitos cometidos en territorio español.

La jurisprudencia del Tribunal Supremo define como delitos a distancia aquéllos en los que la actividad se realiza en un lugar y el resultado se consigue en otro distinto. A la hora de determinar el lugar de la comisión de estos delitos, se enfrentan las teorías de la manifestación de la voluntad y la del resultado, no dominando exclusivamente ninguna de ellas, pues siempre se debe atender a la condición, naturaleza y presupuestos de las infracciones criminales a que se aplica. Por ello, si se trata de delitos continuados, debe ser competente el Juez del lugar donde radique el centro de las actividades criminales y en el que se fraguaron los distintos delitos, y se cursaron órdenes y datos para su realización.

Existen otras sentencias que asignan la competencia jurisdiccional al Juez del lugar donde se produjo el resultado perjudicial del delito. Pero ambas corrientes jurisprudenciales apoyan la tesis de que la jurisdicción española es competente para enjuiciar los delitos planeados y organizados en España, por ciudadanos españoles, dirigidos al público español y cuyos resultados se producen también en nuestro país, a pesar de que los medios técnicos (p.e. el servidor) utilizados para promocionar la actividad infractora se hallen situados en un país extranjero.

En materia de comercio electrónico, ARBITEC, la Asociación Española de Arbitraje Tecnológico, ofrece la posibilidad de realizar arbitrajes a través de Internet (http://www.onnet.es/arbitec).

6. La especial problemática de los derechos de autor

La protección de los derechos de autor favorece el crecimiento de la sociedad de la información, ya que contribuye a establecer la certeza de que el autor de una obra verá compensado su esfuerzo con el rendimiento económico que produzca su explotación.

Pensar que los derechos de autor son inaplicables en Internet puede poner en peligro el futuro de la propia red, ya que nadie se atreverá a publicar sus obras en un entorno donde cualquiera puede apropiarse del esfuerzo ajeno.

Un caso que puede servir de referencia es el de Kriptópolis, una sede web donde se recopila información relativa a las técnicas de cifrado (http://www.kriptopolis.com). El autor de estos contenidos siempre había considerado que el espíritu de Internet se basaba en compartir información, y por ello, nunca creó pruebas de la titularidad. Ahora debe afrontar una acusación de plagio por parte de otro usuario de Internet que se apropió de su obra, la publicó en otro web y ahora exige la clausura de Kriptópolis.

La visión romántica de un ciberespacio libre, sin derechos de autor es un espejismo. Pocos autores aceptarán que su obra pueda ser inscrita en el Registro de la Propiedad Intelectual por otros usuarios y posteriormente puedan encontrarse con una denuncia por plagio de su propio trabajo.

Pero actualmente, los mayores perjudicados por la falta de respeto de los derechos de autor en Internet son los productores de software. Si los programas de ordenador constituyen el producto más vendido de Internet, también tienen el triste privilegio de ser las obras más copiadas.

La copia se produce en todas las plataformas posibles:

-Webs Warez
-FTP Warez
-Canales de IRC Warez
-Grupos de noticias Warez ....

Pero la modalidad más extendida es la de los llamados "cracks" , que son pequeños programas que sirven la anular la protección o la limitación de tiempo de una aplicación específica.

Los cracks aparecen cuando el programa está todavía en la fase Beta y su uso ha llegado a ser tan indiscriminado que ha afectado a programas shareware de autores noveles españoles que sólo pedían 2.000 pesetas por el registro del programa.

Pero la copia no autorizada de software no se limita al ámbito de Internet. La guerra de precios en el sector de los ordenadores clónicos ha generado un submundo de profesionales informáticos dedicados a la instalación de copias ilícitas en el disco duro de los ordenadores que venden, a la copia y distribución de CD Rom e, incluso, a la falsificación de paquetes completos de las aplicaciones más conocidas.

España invierte muy poco en tecnologías de la información. El consumo de estos productos se sitúa muy por debajo de la media europea. El español consume casi en la mitad de lo que consume el europeo medio.

Pero el comportamiento actual del mercado no contribuye a la mejora de la situación, ya que las posibilidades de crecimiento se ven frustradas por el fraude continuado en software y hardware. En el primer caso porque los propios usuarios se implican en la actividad de copia no autorizada. En el segundo caso, porque las tácticas que ayudan a ofrecer precios más bajos se basan en la manipulación de procesadores y en la defraudación del Impuesto del Valor Añadido en las importaciones de material informático.

Este lastre es el que nos impide equipararnos al resto de países europeos y nos exige que tanto los suministradores como los usuarios apoyemos la aplicación de nuestras leyes, para prevenir los delitos que amenazan a la sociedad de la información.