

ASPECTOS LEGALES A CONSIDERARSE EN UN *DUE DILIGENCE* INFORMÁTICO

por Juan Carlos Riofrío Martínez-Villalba

“Aspectos legales a considerarse en un due diligence informático”, en *Leggio*, N° 222, octubre de 2003.

Los buenos artistas suelen pecar justamente de eso, de ser solamente «*artistas*», sin pizca de *comerciantes* para vender sus obras, ni gota de *abogados* para proteger sus derechos.

Para sorpresa de ellos, Internet ya no es aquel paraíso legal donde cada uno hacía lo que quería, sin que nadie pudiese protestar. Hoy, casos como los de *Compuserve*, *Napster*, *E-bay*, *Shetland News*... nos han demostrado todo lo contrario: que las personas también son civil y penalmente responsables en su vida *on-line*. Esto repercute directamente en la actuación de los diseñadores de páginas *web*, quienes deben –por obligación profesional– tener un mínimo de mentalidad jurídica.

Aquí detallamos algunos puntos clave que deben considerarse dentro de un *due diligence* informático, preferentemente antes de subir la página a la *Web*.

1. Determine los derechos de su cliente. Luego protéjalos.

En breve síntesis, el diseñador de una página web, el que elabora un programa de software, quien produce un componente de hardware, tiene diversos derechos sobre los programas de ordenador elaborados, sobre las fotos que haya tomado, sobre las imágenes que dibuje, sobre el texto que redacte, sobre la disposición de los elementos en la página, sobre las utilidades que haya inventado, y, en general, sobre toda creación que quede plasmada en su página *Web*.

Sobre todos estos campos la persona tiene, al menos, un derecho de autor, cuando no uno de patente. Esto de las patentes es muy cuestionado. En algunos lugares se han patentado los *carros de compra*, la *subasta electrónica*, la *tecnología push*, la *publicidad con compensación al destinatario*... Por lo pronto, solo es posible patentar inventos de software en parte del mundo anglosajón, aunque la Comunidad Europea lo está considerando seriamente.

Generalmente lo único que tiene el implicado es un derecho de autor (o una especie de derecho de autor mixtificado, según la legislación de cada país), y lo tiene desde el mismo momento de la creación. No obstante, para hacerlo eficazmente exigible frente a terceros, deberá poder probarse su autoría «*previa*» (previa a la copia). Con lo cual, también habrá de verificarse la posibilidad de realizar tal prueba; en su defecto, tenemos una primera conclusión de nuestro *due diligence*.

Para el efecto las obras se suelen registrar en algún instituto de Propiedad Intelectual (nacional o internacional), o ante un notario tradicional, o ante el *Escrow* (una especie de cybernotario). La eficacia de tal registro, según se haga en uno u otro notario, no siempre será la misma en todos los países. En esto conviene asegurar la formalidad máxima.

Es importante anotar que la prueba también puede realizarse acudiendo al auxilio de técnicas de estenografía, como los *watermarks* en las imágenes, o añadiendo líneas *rem* y otras inservibles a los programas, para marcarlos como se marcan las vacas. Así, en un juicio será más fácil probar la autoría original de la obra copiada.

Es muy recomendable revisar si las páginas *Web*, los archivos y productos incluyen letreros de *Copyrights* o su signo “©”, así como también ver si constan dentro de las páginas *web* leyendas que especifiquen que «*todos los derechos están reservados*».

2. Revisión de licencias.

Así como el cliente tiene derecho sobre sus obras, los demás también tienen derechos sobre las de ellos. Si en la página *web* se utilizan aplicaciones, imágenes, sonidos, programas, etc. que no pertenecen a su cliente, seguramente tendrá que pagar por su uso, salvo, claro está, que sea una versión *freeware*. Un buen *due diligence* informático habrá de revisar estos aspectos.

En concreto, deberá revisarse a fondo el contrato de *freeware*. Los dueños de esos productos suelen establecer que el programa, aplicación, etc. no se podrá utilizar para fines comerciales sin el pago de la regalía correspondiente.

Mayor cuidado habrá que tener cuando se utilizan aplicaciones patentadas.

Por otro lado, la inclusión de logotipos de marcas como *Mastercard*, *Visa*, etc. debe estar autorizada por dichas entidades. Existen penas de prisión y multas significativas por la utilización no autorizada de marcas.

3. Cuidado con los «hipervínculos» y con los «frames».

Si se vincula una página, deberá siempre dejarse en claro que esa página no pertenece al *vinculador*, sino de otra persona. Han existido periódicos *on-line*, que mediante «frames» e «hipervínculos» se han aprovechado de las noticias levantadas esforzadamente por otros periódicos, y las incluyen dentro del suyo, creando una cierta confusión acerca de cuál es su autor. Ello es claramente una violación a los derechos de autor.

Alguna jurisprudencia comparada ha condenado el uso de «hipervínculos profundos», que son aquellos que remiten a las páginas interiores de algún sitio. El criterio seguido es que los dueños de un sitio tienen derecho a exhibir la publicidad constante en su página principal a todos los que visiten su sitio. Luego, si alguien se vincula directamente con una página secundaria, no vería la publicidad, y le ocasionarían un perjuicio.

Para evitar problemas, habremos de recomendar a nuestros clientes que suscriban convenios de vinculación.

4. Escoja «domain names» a prueba de demandas.

Sobrada memoria tenemos de los especuladores que se apropian de los «domain names» para vendérselos luego al dueño de la marca. Quizá esto se permitió antes, cuando imperaba a raja tabla la política del «*first come, first served*». Hoy en día ya no se puede registrar un nombre si existe mala fe, o si, perjudica a una marca registrada en el país, o a una marca extranjera notoriamente conocida o de alto renombre. Tampoco se suele permitir el registro de nombres de personalidades, aunque ciertamente han aparecido detractores de esta política, como en el famoso caso de *Madonna*.

Conviene para el efecto revisar si el DNS de nuestro cliente cumple con la *Normativa Reguladora de Resolución de Conflictos de Nombres de Dominio* de la ICANN.

En general, los especuladores de «*domain names*» no reparan en que, a más de las responsabilidades civiles que su conducta acarrea, también existen las penales.

Antes de escoger un «*domain name*» aconsejamos que, a fin de evitar una eventual demanda, se visiten lugares como *WHOIS* y los localizadores de marcas y nombres comerciales de la Comunidad Europea, donde constan las marcas y registros más significativos en el ámbito mundial.

5. ¡Ojo! No todo «*contrato click*» es válido.

Los «*contratos click*» son aquellos que se suscriben aplastando el botón de aceptación. Pero para que la aceptación surta plenos efectos jurídicos (es decir, que el contrato sea válido) se habrá de cumplir con ciertas exigencias legales.

Por ejemplo, ciertos países exigen que los contratos sean redactados con una letra no menor a 10 puntos; las cláusulas del contrato no serán exigibles al consumidor. Si en el texto constan «*hipervínculos*» que remiten a otras páginas, donde aparecen nuevas condiciones del contrato, generalmente se ha dispuesto en el derecho comparado que es necesario que esas páginas remitidas sean conocidas por el aceptante. Por lo tanto, será conveniente incluir una leyenda al lado del botón de aceptación que diga; «*Conozco y acepto lo contenido en los 9 hipervínculos constantes en esta página*», o, mejor aún, evitar el uso de *links* en los contratos electrónicos.

Para fines probatorios, sugerimos recomendar a los clientes que notaricen las páginas *web* donde se muestren los contratos. Así podrán demostrar al juez cuáles eran las condiciones a las que el consumidor se obligó. De otra forma, en el juicio él podrá aducir que las condiciones que actualmente constan en la *web* no eran las que aparecieron el día en que compró el producto.

El tema de los contratos electrónicos *on-line* además tiene muchos aspectos de derecho internacional privado que deben analizarse en un *due diligence* informático, como lo son el derecho de la publicidad y los derechos del consumidor, entre otros.

6. Evite la desinformación.

Todo ser humano, por el hecho de serlo, tiene derecho a la información. Pero no siempre los medios informan al hombre; algunas veces lo desforman. Así, un niño desinformado es un niño mal formado. Por eso el legislador ha procurado limitar la difusión de contenidos que desinforman: pornografía, atentados contra la privacidad, contra la dignidad de las personas, terrorismo, propaganda de delitos, violencia, racismo, discriminaciones, etc.

Internet es un medio de comunicación abierto al público: en general, todo el que ingresa puede ingresar a cualquier sitio. Un contenido publicado en un servidor ecuatoriano puede verse en Holanda, y viceversa. ¿Bajo qué ley nos cobijamos? ¿Bajo la ecuatoriana? ¿O, quizá, la holandesa? Es cuestión difícil su respuesta, incluso para los expertos. Como ejemplo paradigmático, en Francia se condenó a un ciudadano alemán por exhibir material neonazi en su Estado; en Francia eso constituía una infracción, mientras que en Alemania no.

Nuestra recomendación: obsérvese la ley del mínimo riesgo. Si sospecha que al publicar un contenido viola la ley de algún país, sugiera no publicarlo. Así, en caso de que alguien demande a su cliente, usted como abogado habrá salvado su responsabilidad.

7. Limite la responsabilidad.

En Francia y en otros estados se ha condenado a Proveedores de Servicios de Internet (PSI) por los contenidos ilícitos que hospedan o transmiten. La cuestión es harto debatida por los juristas y hasta la fecha no hay una definición tajante sobre el tema. En la Comunidad Europea, al menos existe hoy en día una Directiva que trata del asunto, pero ésta no resuelve los problemas *ad extra* de la Comunidad.

La Directriz ha establecido, en líneas generales, que quienes ejercen actividades de mero transporte de información o de alojamiento temporal, no son responsables por lo que informan, mientras no alteren los datos transmitidos y respeten las condiciones de acceso y actualización de la información. Si el PSI se dedica a dar servicios de hospedaje, no será responsable en tanto desconozca cuáles son los contenidos ilícitos que hospeda. Si los llega a conocer, debe denunciarlos.

Ciertamente se nota una cierta inclinación mundial a mitigar la responsabilidad de los PSI, mas convendrá, de todos modos, alertar sobre el tema al cliente.

Será bueno recomendar que se tenga un mínimo de diligencia –la cual es exigida por la ley– en verificar con alguna frecuencia si los contenidos que hospeda son o no

ilícitos. Si detecta alguna injuria, pornografía infantil, venta ilegal de software, etc. deberá denunciarse por escrito (o por algún medio que asegure la prueba) a las autoridades correspondientes, así como comunicárselo al interesado. Vale guardar copia de la correspondencia. Así se crearan varias pruebas de descargo.

También es conveniente que el abogado revise el contrato de servicios, e incluya – si no lo tiene– varias disposiciones limitativas de responsabilidad.

8. Para casos de delitos, asegure la creación y conservación de la prueba.

Hay muchos delitos que pueden realizarse *on-line*: robos, estafas, injurias, *spams*, propaganda del delito, pornografía infantil, etc. Si se lo han hecho a usted, ¿podrá probar quién ha sido, cuando, cómo y donde? Nosotros creemos que sí. Sí, porque sabemos que la evidencia digital que dejan estos delitos es abundante, mucho mayor a la que el común de los mortales sospecha. No existe delito perfecto, ni siquiera en el mundo virtual.

Pero la evidencia digital es volátil y resulta necesario conservarla. Por ello, cuando le informen de un delito, solicite inmediatamente a los operadores de los equipos que no los toquen, hasta realizar una *imagen* o un *backup* del sistema, o de los registros del *email*, o de la información sensible, según sea el caso.

¡Mejor aún, prepárese antes del delito para filmarlo! Existen herramientas tecnológicas y jurídicas que le permiten hacerlo.

9. Cuidado con los tributos... Internet va dejando de ser un paraíso fiscal.

Quizá a muchos les sorprenda saber que las bases de datos de los recaudadores de impuestos son gigantescas, que cruzan la información que le proporcionan todos sus administrados, y que además hoy en día se cruzan también las cuentas entre los mismos Estados. Actualmente evadir impuestos es sustancialmente más complicado que en el pasado.

Qué tributos se deben pagar, y dónde, depende mucho de cada caso. Si se exportan servicios o productos nacionales, generalmente no se causará el impuesto al valor agregado (VAT o IVA), pero se deberán declarar para efectos del pago del impuesto a la renta.

En general la doctrina considera que el «*establecimiento permanente*» para efectos del pago de los impuestos (especialmente el impuesto a la renta), es el del país donde se encuentra el servidor, o donde se realiza físicamente la mayor cantidad de operaciones.

Esto es sumamente interesante, pues de un buen *due diligence* puede resultar que el abogado recomiende a su cliente montar el «*establecimiento permanente*» en un lugar donde exista menos carga tributaria, y el cliente eventualmente querrá reestructurar todo su negocio para volverlo más competitivo.

No quiero extenderme más en este artículo destinado únicamente a enumerar los puntos más relevantes que un buen *due diligence* informático debe considerar. Sólo dejaré sentado que la lista no es taxativa: este campo tiene más bemoles de los que en mil páginas se pueden afrontar.