RIESGO, DAÑO Y RESPONSABILIDAD JURÍDICA EN LA ERA DIGITAL

*Daniel Peña Valenzuela**

INTRODUCCIÓN

El concepto de sociedad de la información es objeto de diversos enfoques, entre los cuales está el jurídico. El derecho y la tecnología pertenecen a dominios distintos, su interacción no es simple, ambos son determinantes en la sociedad postmoderna. Sin embargo, los avances tecnológicos requieren de él en la medida que éste cumpla con su función de regular las relaciones privadas e incluso las relaciones entre el Estado y los particulares cuando se usan tecnologías de la información.

Las nociones de riesgo y responsabilidad –esencialmente jurídicas– son el resultado de deberes generales y particulares de cuidado, de observancia de reglas sociales y jurídicas. Como fundamento de las obligaciones, el deudor, en sentido amplio, debe responder por haber incurrido en una determinada conducta, prevista por el ordenamiento con consecuencias que son de sanción adversa.[1]

El ciberespacio es un territorio virtual creado por la existencia de la red global –internet– y sus varios millones de usuarios y navegantes, que la utilizan para el intercambio social, cultural y comercial. El ciberespacio aparece como consecuencia de la convergencia de

---

* Abogado de la Universidad Externado de Colombia. DESS (Grenoble) y LLM (Londres). Profesor Investigador de la misma universidad en el área de comercio electrónico y nuevas tecnologías. Socio de Cavelier Abogados. La presente ponencia refleja la opinión personal del autor.

1 HINESTROSA, FERNANDO (1983) "La responsabilidad Civil " en *Escritos Varios*, Universidad Externado de Colombia, Bogotá.

las telecomunicaciones e informática.[2] Es un efecto de que la red global sea utilizada como medio de comunicación. Ahora predomina la movilidad como valor social y por ende, la deslocalización de redes y usuarios. El contrato y el hecho punible en el ciberespacio también abarcan diversos territorios en sus consecuencias y efectos.

Los sujetos mismos de las relaciones jurídicas se están "virtualizando", los *avatars* son creados a imagen y semejanza de los usuarios de las comunidades virtuales, como por ejemplo *Second life.* Estos sujetos tienen identidad digital propia aunque derivada del intelecto de los usuarios-creadores.

La regulación del ciberespacio fue mirada inicialmente con recelo: Internet constituía un territorio ajeno a los gobiernos, en el cual la libertad –algunos la interpretaron como libertinaje– y la innovación eran sus fuerzas impulsoras. El comercio y los gobiernos paulatinamente han propiciado la regulación del espacio virtual[3]. Ambos requerían seguridad y certeza. Se necesitaba regulación legal tradicional con normas y leyes, pero también cuasi-reglas como, por ejemplo, la configuración de la arquitectura de la red para reestablecer el control "perdido" inicialmente.[4] Ejemplo de esto último es la configuración de los programas de ordenador que puede propiciar mayor o menor control, y puede facilitar la protección de la intimidad, al permitir al usuario aceptar o no recibir, por ejemplo *cookies o spyware.*[5] La publicidad directa e interactiva –tan usual hoy en día en internet– requiere, para obtener su máximo potencial, del conocimiento respecto de hábitos y costumbres de los usuarios. Cada vez la informática produce herramientas más poderosas para lograr tal fin.

De un territorio virtual caracterizado por la irresponsabilidad, caos y anarquía, la regulación legal de internet ha construido nuevas categorías, ha resuelto nuevos problemas y en muchos casos ha reinterpretado nociones jurídicas tradicionales para adaptarlas a las necesidades de la sociedad de información y para mitigar los riesgos propios del vértigo que la caracteriza. Esta tarea aún está comenzando, cada día con cada modelo de negocios que surge en el ciberespacio se crean nuevos retos.

La determinación del grado de responsabilidad de los diferentes agentes económicos que participan en la red, sea por interpretación de los jueces o por decisión legislativa, es la única garantía jurídica de certeza para los propios participantes en la red, permite la adecuada distribución de las cargas probatorias en caso de conflicto y hace posible que las inversiones tengan unos costos de transacción acordes y proporcionales según

---

2 Torres Nieto, Alvaro (1999) "Telecomunicaciones y telemática. De las señales de humo a internet", Escuela Colombiana de Ingeniería, Bogotá

3 Lessig Lawrence (1999) "Code and other laws of the Cyberspace", Basic Books, Nueva York

4 Ibídem

5 Archivos electrónicos que se instalan en el disco duro de un navegante que ha visitado un sitio de internet y que permiten posteriormente rastrear las visitas a otros sitios.

la actividad y el riesgo. La distribución de riesgos en los contratos por medios electrónicos va a depender en gran medida de la consolidación de esquemas de seguridad tecnológica que aseguren la confianza de usuarios y empresas.

I. INTERNET: ESTRUCTURA INFORMÁTICA Y FUENTE DE RIESGOS

El comercio electrónico aparece como una aplicación en internet, que se ha convertido por la fuerza de las circunstancias y por el crecimiento económico. Existe por la *world wide web*, porción comercial de la red global conformada por millones de páginas de internet, comunidades, blogs, portales, motores de búsqueda y sitios de internet. Una página de internet es un mensaje de datos almacenado en un servidor: los usuarios al utilizar un programa de computador –navegador– solicitan la transferencia de unos datos ubicados en un lugar determinado (página internet) ubicado en un lugar definido por una dirección protocolo internet (IP). La "definición" del lugar donde se origina o se recibe un mensaje de datos depende en muchos casos de la decisión del legislador que puede establecer presunciones al respecto con el fin de disminuir la "indeterminación" propia de los flujos de información digital. [6]

La estructura de internet es compleja, compuesta de elementos *materiales* como servidores, computadores o aparatos terminales y redes de telecomunicaciones; e *inmateriales* como protocolos, direcciones virtuales, programas de ordenador, contenidos y datos que circulan constantemente.[7]

Esta estructura informática compleja no es otra cosa que un valor agregado[8] intangible creado en relación con las redes de telecomunicaciones tradicionales que permitían solamente la transferencia de mensajes de voz. Internet permite, básicamente, la transmisión de mensajes de datos o cualquier forma de información digital entre computadores personales, servidores y *hardware*.

La transmisión de datos entre usuarios directamente (*peer to peer*), es decir, sin utilizar las páginas de internet ha redescubierto una característica del internet original y ha propiciado la noción de comunidades virtuales no necesariamente con actividades o fines comerciales.[9]

---

6 Artículos 20, 21, 23 y 24 de la ley 527 de 1999

7 BERNERS LEE TIM (1999) Weaving the web the original Design and ultimate destiny of the world wide web by its inventor, Harper, San Francisco

8 Decreto 1794 de julio 15 de 1991

9 Para más detalles sobre la estructura de internet ver PEÑA VALENZUELA, DANIEL (2001) "Aspectos legales de internet y del comercio electrónico." Dupré Editores, Bogotá

Debido a la configuración actual de la red, en todo caso, el almacenamiento o *hosting* de los sitios ha creado un negocio específico, la provisión de servicios de arrendamiento de espacio en servidores para acoger las páginas. Los proveedores de servicios de internet (PSI) son empresas, en muchos casos, íntimamente vinculadas a las empresas que prestan servicios tradicionales de telecomunicaciones que han ampliado su modelo de negocios.

La participación de los PSI en la red internet no se limita a la provisión de los servicios de almacenamiento de las páginas, el acceso de los usuarios también requiere una conexión la red que usualmente se realiza a través de la configuración de un computador que interactúe con la red global. Nuevas tecnologías han permitido la conexión inalámbrica y las redes digitales de comunicación. La utilización de cables de fibra óptica para las telecomunicaciones ha permitido mejores conexiones y la utilización de un mayor ancho de banda.

Las *comunidades virtuales o redes sociales* constituyen un adelanto en la integración entre usuarios de la red global. Con la utilización de una página de internet se reúnen e interactúan múltiples usuarios –a veces millones– que comparten el objeto de la red por ejemplo, compartir música, o videos. [10]

Esos sujetos, nuevos en su mayoría, son los extremos de relaciones jurídicas que enmarcan riesgos tecnológicos en la medida de que el ciberespacio es un espacio virtual creado por avances tecnológicos en la informática, en las telecomunicaciones y en los modelos de negocios.

II. COMERCIO ELECTRÓNICO: LA DINÁMICA DEL E-BUSINESS

La actividad comercial ha dominado el desarrollo de internet en los últimos tiempos. La red global es a la vez medio de comunicación y plataforma de negocios. Las empresas *puntocom*, especialmente diseñadas para la red con revolucionarios modelos de negocios fracasaron por razones diversas. El menosprecio de las reglas económicas tradicionales, la sobreestimación de un consumo virtual y la especulación de los mercados llevaron al fracaso a la primera fase de empresas dedicadas al negocio electrónico.

La euforia de los primeros tiempos de la revolución digital ha sido reemplazada por una visión nueva de las empresas tradicionales que han encontrado en internet un novedoso medio de distribución y mercadeo de productos y servicios. Internet ha dejado de ser "revolucionario" y se ha convertido en una herramienta para mejorar el servicio al

---

10 Peña Valenzuela, Daniel (2004) "Comunidades Virtuales: Nuevo paradigma de la contratación internacional" en Derecho de los Negocios Alcances Tomo II, Universidad Externado de Colombia, Bogotá

cliente y para lograr mayor interactividad en la relación entre empresas y consumidores. Las empresas, cada día de manera más creciente, consolidan su cadena de suministro y distribución integrándose de manera horizontal y vertical con otras empresas, utilizando los medios electrónicos para tal fin.

El "negocio electrónico" ha impactado muchas actividades de tal manera que estamos en los albores de la sociedad de la información en la cual el conocimiento, la propiedad intelectual y la creación serían los pilares de la nueva riqueza y el bienestar. Es lugar común afirmar que la competitividad de las naciones estaría basada en la educación y la cultura y no necesariamente en las materias primas.

La regulación legal del negocio electrónico ha sido impulsada desde diversos frentes internacionales. Tratados y Convenciones internacionales se han revisado, los bloques económicos han creado regulación a la medida, las organizaciones internacionales[11] han discutido toda clase de proyectos en la materia de su incumbencia. Los proyectos de regulación internacional abarcan temas como impuestos, firmas digitales, valor jurídico de los documentos electrónicos, nombres de dominio, estándares técnicos, entre otros.

El tema de responsabilidad de los diversos agentes que participan en la red, como el de la jurisdicción y ley aplicable a los actos en el ciberespacio, es difícil de unificar en cuanto a conceptos y aplicación práctica, si no imposible, partiendo del supuesto de que existen dos sistemas de responsabilidad: el de *common law*, basado en precedentes jurisprudenciales y en el concepto de *tort y* el romano-germánico, estructurado en el daño y la obligación de resarcimiento.

III. ELEMENTOS DE LA RESPONSABILIDAD TRADICIONAL

La noción de responsabilidad está vinculada a la obligación. Esta es el vínculo o relación jurídica entre dos personas determinadas mediante la cual un sujeto espera una colaboración, cooperación, deber de conducta o prestación del deudor.[12]

En caso que el deudor incumpla tal expectativa tutelada por el derecho es responsable y al subsistir la deuda se puede hacer efectiva incluso de manera forzada con la satisfacción *in natura* o mediante la compensación pecuniaria y la respectiva indemnización, si a esa hubiere lugar.

---

11 OECD, UNCTAD, OMPI, ONU y OMC entre otras

12 Prólogo de Fernando Hinestrosa al libro de Henao Juan Carlos (1998) El daño, Universidad Externado de Colombia, Bogotá

La responsabilidad puede emanar de la existencia de una relación jurídica previa entre las partes, es decir, por existir un deber concreto o por la violación de un interés legítimo o un derecho en un encuentro social ocasional. Estas nociones abarcan los conceptos más tradicionales y más difundidos de responsabilidad contractual y extra-contractual.[13] La responsabilidad es el resultado de la existencia de riesgos sin solución.

Los tres elementos fundamentales para que exista responsabilidad son el daño, la imputación de éste a un autor especifico de la conducta mediando una relación de causalidad y el juicio de valor que define la conducta, como sería la culpabilidad o el desempeño de una actividad peligrosa o la existencia de un riesgo.

El daño es el factor o elemento fundamental de la responsabilidad; luego se deberá indagar quien lo causó, es decir, a quien se le imputa el mismo, y como complemento de la noción se deben analizar las circunstancias en las cuales se causó el daño. La responsabilidad no es nada diferente del hecho de que alguien está obligado a resarcir un daño.[14]

El daño puede comprender: (1) la afectación al interés patrimonial –lucro cesante y daño emergente– y (2) Extra patrimonial: el daño moral a la proyección social de la persona y a su integridad afectiva y el daño biológico. El daño debe ser cierto y directo. Se debe indemnizar "el daño causado, todo el daño causado y nada más que el daño", bajo el apotegma citado por los tratadistas de las obligaciones.

El daño es el elemento más objetivo de la responsabilidad, no cabe duda que su prueba debe estar desprovista de mayores valoraciones. La era digital sugiere que el *daño informático* reafirme lo objetivo de la noción. La culpa y la voluntad humana de dañar serían difíciles de probar en procesos informáticos complejos como los de los *web services* en los cuales el enlazamiento de la cadena de suministro de las empresas hace que la toma de decisiones sea hecha por sistemas informáticos predispuestos para ello, sin intervención humana.

Respecto del daño informático vale la pena tener en cuenta los estudios relacionados con la fase preventiva y las responsabilidades de los administradores de las compañías por el problema de Y2K o problema del año 2000, todo en el marco de una *objetivización* del daño. Esta ola de regulación legal, generó unas medidas de adecuación de los sistemas de información que pretendían minimizar la reparación en caso de la ocurrencia de los funestos hechos que nunca, por fortuna, ocurrieron[15]. Aún es impredecible lo que puede ser un desastre tecnológico, un ataque terrorista que produzca una interrupción

---

13 Ibídem

14 Henao Juan Carlos (1998) El daño, Universidad Externado de Colombia, Bogotá

15 Zagarra Mauricio Cordoba Juan Fernando (1999) Año 2000, problemas y soluciones jurídicas para la crisis informática, Legis, Bogotá.

de las comunicaciones electrónicas o una hecatombe causada por un daño tecnológico que produzca una reacción en cadena en el sector "real".

Como sustento de la noción de daño como pilar de la responsabilidad se debe tener en cuenta que el riesgo es la contingencia del daño, o sea, la posibilidad de que al obrar se produzca un daño, lo cual significa que el riesgo envuelve una noción de potencialidad referida esencialmente al daño. La teoría del riesgo tuvo como antecedente en Colombia la jurisprudencia de la Corte Suprema de Justicia en la década de los treintas y posteriormente se ha concretado, por ejemplo en convenciones y tratados internacionales sobre responsabilidad del transportador.[16]

En el caso de los sistemas de información avanzados, el manejo y administración de los mismos genera riesgos. Algunos inherentes al sistema como defectos en la programación, inadecuada interoperabilidad con otros sistemas, incompatibilidad de las aplicaciones con la plataforma del sistema operativo. Otros pueden ser externos como introducción de virus y los ataques e intromisiones de *hackers* . Es también posible que los riesgos provengan de la compatibilidad necesaria entre *hardware* y *software*, por ejemplo, la adecuación entre un programa de ordenador (controlador o manejador) y el dispositivo que se controla, por ejemplo, un dispositivo de comunicaciones.

Es posible afirmar que el riesgo de daño es inherente a los sistemas de información y que las repercusiones que puede tener un daño en un sistema de información son incalculable en una sociedad como la nuestra: global e interconectada.

En los sistemas de responsabilidad civil de inspiración romano-germánica se ha establecido la responsabilidad del guardián de las cosas como forma de responsabilidad indirecta. En Colombia, a diferencia del régimen francés y chileno, no existe una regulación legal de esa forma de responsabilidad. Sin embargo un sector de la doctrina sostiene que esta noción puede interpretarse con base en el 2343 del código civil.[17] El dilema está en determinar si un alojador de páginas, el conductor de un blog, el creador del juego virtual o el auspiciante de la comunidad virtual son guardianes de los servidores y páginas electrónicas ajenas y hasta dónde llega ese deber de control y vigilancia. Otra probabilidad es que esos sujetos sean habilitadores o permitan el uso de herramientas que permitan la infracción.

---

16 Salazar G. Juan Carlos. El transporte aereo internacional y la legislación colombiana en Revista de Derecho Privado N.º 25. Vol. XIV de la Universidad de los Andes, octubre de 2000

17 Sarmiento, Manuel Guillermo. La teoría del riesgo y la responsabilidad civil, (1986) en "Estudios de Derecho Privado, Homenaje al Externado en su Centenario", Bogotá.

IV. CAMBIOS EN LOS PARADIGMAS: EL RIESGO COMO FUNDAMENTO DE LA RESPONSABILIDAD EN LA ERA TECNOLÓGICA

A. El caso de los proveedores de servicios de internet (PSI)

Definido que el daño es el presupuesto de la responsabilidad en general, consideramos que la era de la tecnología estará marcada por la noción de riesgo reemplazando a la culpa. La culpa como expresión eminentemente personal y voluntarista no está de acuerdo con la evolución de la era digital en la cual muchas conductas tienen como fuente generatriz elementos objetivos.

Los PSI tienen como actividad profesional, la localización de información, el arrendamiento de espacio para que terceros coloquen sus páginas además proveen de acceso a la red a terceros. También los PSI crean espacios virtuales que como comunidades permiten el intercambio de archivos y ficheros electrónicos. La actividad de los proveedores se ha ido ensanchando en la medida en que la tecnología se hace más eficaz y dinámica. Los modelos de negocios de los proveedores también han cambiado desde los portales horizontales –meros acumuladores de información hasta los buscadores de información global en tiempo real como *google earth* o las redes sociales de creatividad conjunta como *youtube.*

Lo anterior hace evidente que la definición de su responsabilidad legal tendrá mayor o menor ámbito dependiendo de la interpretación extendida que se dé al *control* que deben tener respecto de los contenidos publicados.

La información que se coloque en sus servidores por los propietarios de las páginas o por usuarios creadores de contenidos puede violar innumerables intereses legítimos. Los propietarios de las páginas son directamente responsables de tales contenidos y de la adecuación de los mismos al régimen legal. La responsabilidad solidaria, indirecta o por contribución, complicidad o coautoría que quepa a los PSI es asunto mucho más discutido.

La reciente historia del ciberespacio que no alcanza a abarcar una década sugiere responsabilidad por delitos como injuria y calumnia, proxenetismo, pornografía, apuestas ilegales, estafas en línea; prestación de actividades reguladas sin autorización (actividades de profesiones liberales que requieren licencias especiales), prestación de servicios financieros en línea sin autorización; e infracción de propiedad intelectual o industrial[18]. Después de esta enumeración alguien podría afirmar que un PSI no tiene relación directa con actividades riesgosas.

---

18 Lipszyc, Delia (2001) Internet: la responsabilidad de los proveedores de contenidos, de servicios y

En los Estados Unidos, la jurisprudencia ha hecho responsables a los PSI por violación de derechos de autor de terceros bajo criterios de responsabilidad que abarcan la responsabilidad directa por infracción al haber realizado una reproducción no autorizada por el hecho de operar los servidores que permiten la interoperabilidad de la red (*direct infringement*).

En otros casos se ha responsabilizado indirectamente a los PSI por haber contribuido a la infracción en la medida en que han dispuesto los medios y plataformas tecnológicas necesarias para que tal infracción se consume. (*contributory infringement*)

Finalmente, otra tipología de casos demuestra la responsabilidad de los PSI por el hecho de tener el deber de supervisión y control sobre determinadas actividades que han causado daño a terceros independientemente que no se hubiera realizado ninguna actividad material directa para infringir derechos de terceros (*vicarious infringement*)[19] Esta noción anglosajona se puede asimilar a la noción romano-germánica de la responsabilidad del guardián de la cosa.

Teniendo en cuenta la incertidumbre originada en tan diversos criterios interpretativos los Estados Unidos adoptaron el *Digital Copyright Millenium Act* en diciembre de 1998, el cual establece una regulación de los intermediarios en línea, con los criterios de responsabilidad y excepciones respectivas. Estas últimas enfocadas a las actividades de los PSI en las cuales se pueden asimilar a meros transmisores de señales de telecomunicaciones o cuando solamente realizan actividades de almacenamiento temporal de archivos.[20]

Este régimen ha sido interpretado como el resultado de un compromiso entre las industrias de derechos de autor y telecomunicaciones con el fin establecer un equilibrio entre la protección del derecho de autor y el ejercicio de las actividades de los prestadores de servicios de internet.

El modelo europeo de responsabilidad de los PSI también ha tenido contradicciones. Alemania y Suecia fueron los países que inicialmente adoptaron leyes específicas sobre responsabilidad de los intermediarios en línea. La jurisprudencia de los otros países ha sido definida con base en las reglas generales de responsabilidad aplicadas a este tema. Como consecuencia de lo anterior al interior de la UE se presentaron casos contradictorios, un tribunal francés consideró que los proveedores de servicios de *hosting* eran responsables del control de los contenidos e incluso de su filtro para evitar atentados a

---

de acceso, en Revista de Derecho Privado N.º 26. Vol. XV de la Universidad de los Andes, Agosto de 2001

19 LEAFFER, MARSHALL (1995) Understanding Copyright Law (9), New Haven.

20 U.S. House of Representatives, 105th Congress, Report 105-796

derechos de terceros. Una corte holandesa, por el contrario, consideró que los PSI ponían simplemente a disposición de terceros la posibilidad de publicar contenidos.[21]

Con el fin de unificar los criterios de responsabilidad de los PSI, la Unión europea adoptó una Directiva[22] en la cual se establecen los criterios de responsabilidad y las excepciones cuando son meros transmisores de datos, a condición que (a) el prestador del servicio no haya iniciado él mismo la transmisión, (b) no seleccione al destinatario de la comunicación y (c) no seleccione ni modifique la información transmitida.[23]

Tampoco es responsable el prestador de servicios en el caso que se límite su actividad al almacenamiento automático, provisional y temporal de esta información realizado con la única finalidad de hacer más eficiente la transmisión (memoria tampón-caching).[24]

En el caso del alojamiento de los datos, la prestación de servicios no implica un deber de supervisión sobre la información almacenada, pero si de comunicación inmediata a las autoridades sobre hechos ilícitos, como todo guardián de un bien.[25]

La actividad de los PSI podría tener una evolución similar a la de los transportadores que vieron su actividad impactada por la teoría de la "actividad peligrosa" con eximentes de responsabilidad y los límites pecuniarios a la indemnización.[26] En Colombia, la evolución y fortalecimiento de los PSI debería tener como consecuencia una posición del legislador en la cual limite la responsabilidad a ciertos eventos como los citados en Estados Unidos o la Unión Europea. En el estado actual de las cosas, los PSI colombianos o que tengan actividades en territorio colombiano estarían sujetos a la teoría tradicional de la responsabilidad.

Respecto de la responsabilidad frente a los datos personales de los usuarios de internet, recientemente la Corte Constitucional[27] condicionó las facultades de la administración tributaria DIAN –Dirección de Impuestos y Aduanas Nacionales– a que en la solicitud de información se respeten los siguientes derechos:

• El derecho a la intimidad de quienes realicen transacciones electrónicas.

---

21 Notas tomadas de The Link, informativo electrónico bajo el auspicio de Stephen Le Goueff

22 Directiva del Parlamento Europeo y del Consejo relativa a ciertos aspectos jurídicos del comercio electrónico en el mercado interior del 1 de septiembre de 1999.

23 Artículo 12 de la Directiva

24 Artículo 13 de la Directiva

25 Artículos 14 y 15 de la Directiva

26 MAZEAUD–CHABAS, Traité Théorique et Pratique de la Responsabilité Civile Délictuelle et Contractuelle, Tomo III. Editions Montchrestien, Paris, 1983

27 CORTE CONSTITUCIONAL Sentencia Número C-1147 De 2001. Exp. D-3495 Magistrado Ponente Manuel Cepeda, 31 de octubre de 2001, Bogotá

• El principio de relevancia, el cual supone, en cada caso concreto, que sólo puede requerirse y revelarse la información que esté relacionada con las funciones legalmente atribuidas a la entidad que la solicita.
• El principio de finalidad de modo que la información requerida y revelada sea:

(i.) estrictamente necesaria para cumplir los fines de la administración en ese caso concreto, y
(ii.) sólo sea utilizada para los fines autorizados por la ley que, en el presente caso, tienen que ver con la inspección, recaudo, determinación, discusión y administración de asuntos tributarios en los términos específicos que señalan las disposiciones legales para cada tributo en particular.

La Corte aclaró que es posible que la administración de impuestos requiera en casos concretos y excepcionales, de información más detallada acerca de las transacciones que se realizan por internet. En estos eventos el ejercicio legítimo de las facultades de investigación que se le conceden a la DIAN exige justificar la pertinencia de tales datos, de manera que se demuestre la relación directa entre lo que se solicita y la materia que es objeto de estudio, en aplicación del principio de relevancia. Además, en estas circunstancias tendrán que respetarse los criterios que velan por la adecuada conservación y destinación de la información recaudada.

Si bien es cierto estas reglas se aplican de manera restringida a los aspectos tributarios de las transacciones electrónicas, quedando sin resolver el tema más general de la protección a la intimidad en la red. Es evidente que cualquier interpretación sobre el *habeas data* en internet debería tener como base los principios establecidos por la Corte Constitucional, al menos mientras comienza la aplicación de la recientemente aprobada ley de protección de datos. Paradójicamente, los datos personales exportados al exterior pertenecientes a los ciudadanos colombianos estarían más protegidos bajo la regulación de la Unión Europea o las regulaciones de la Comisión Federal de Comercio.

Muchas de las actividades de los PSI son ahora cubiertas por pólizas de seguros que permiten "trasladar" los costos correspondientes a los riesgos. La cobertura de algunos seguros incluye los riesgos inherentes a las fallas de los sistemas de información.

B. Responsabilidad de los agentes electrónicos, motores de búsqueda y links

Los agentes electrónicos[28] son programas de computador o mecanismos electrónicos que realizan una tarea determinada en reemplazo de un usuario usualmente interactuando

28 La noción de agentes electrónicos ha sido acogida en diversas leyes de los Estados Unidos como el Uniform Computer Information transactions Act (Section 102) y el Uniform Electronic Transactions Act (section 2)

con otros agentes. Existe una variedad de tales agentes que son clasificados dependiendo de sus características: móviles, inteligentes, de interfase y de información.

La característica más importante de estos agentes es que interpretan la información que les es presentada. Las tareas de las que se encargan en los actos de comercio electrónico son complejas y tienen como finalidad eliminar algunos de los pasos necesarios para que el consumidor realice sus actos en la red, entre ellas están la búsqueda y clasificación de información, la comparación de precios y calidad de productos y servicios ofrecidos en la red global, la respuesta automática en el caso de contratación masiva y los identificadores de contenidos digitales.

El caso de los identificadores de objetos digitales[29] sugiere que estos deben ser únicos –sin posibilidad de duplicados–; móviles en la medida que deberían estar presentes sin importar la capacidad de movimiento del objeto en la red; aceptados universalmente y con niveles altos de autenticación.[30]

La responsabilidad por daños cometidos por agentes electrónicos debe estar en quien ejerza el control efectivo sobre los mismos. Llama la atención como los esquemas de *outsourcing*[31] que muchas empresas utilizan para que terceros estén contractualmente encargados del manejo de los sistemas de información de otros, crean un nuevo escalón en la responsabilidad y convierten al contrato en el instrumento idóneo para adjudicar las cargas de responsabilidad entre las partes.[32]

Los *links* son hipervínculos entre las páginas que permiten la navegación mediante la superposición eficiente de textos entre páginas. Para hacer un link no se requiere la autorización o el consentimiento del propietario de la otra página.[33]

Realizar *links* es una preocupación constante del propietario de una página, establecer una política general sobre las condiciones exigidas para que se pueda realizar un *link* a una página también debería ser una preocupación presente.

Las consecuencias de permitir un *link* a una página pueden llegar hasta a constituir una responsabilidad compartida por el contenido ilegal o infractor que tenga la página. La

---

29 Ejemplos de tales identificadores son ISWC, International Standard Work Code y el ISAN, International Standard Audiovisual Number.

30 Materiales presentados en la conferencia WIPO International Conference on e-commerce and Intellectual Property, Ginebra, 1999 por CNRI Handle System

31 Tercerización

32 TEIXEIRA DIOGO. Estado de los medios de pago en Latinoamérica, en 1er Seminario Nacional de Tecnología para el Sector Financiero, Modernización de los Medios de Pago, Asobancaria, noviembre de 1997

33 GATENWOOD, CHRISTOPHER. Click Here: web links, Trademarks and the First Amendment The Richmond Journal of Law & Technology, Volume V, Issue 3, Spring 1999

Comisión Federal de Comercio de los Estados Unidos ha establecido reglas especiales, por ejemplo, para sancionar a los intermediarios que presentan información errónea en línea relacionada con compañías que participan del mercado de valores, por ejemplo, en el caso de la colocación de bonos. En este caso no habría responsabilidad por violación de un derecho específico sino por el perjuicio que se cause a terceros que realicen una negociación con base en información inexacta.[34]

Si bien es cierto lo recomendable es regular la relación de *links* entre páginas mediante contratos, la realidad de la industria de internet refleja que muchos de los *links* se hacen de manera espontánea. En ese sentido es importante explorar que la ley de derechos de autor y la Decisión de la Comunidad Andina sobre propiedad industrial establecen el derecho de cita y la utilización de signos distintivos con propósitos informativos como excepción a la protección de la propiedad intelectual, respectivamente.

La discusión sobre responsabilidad se ha vuelto más evidente en la medida en que se desarrolla más competencia entre distintas empresas en la red. El proyecto de presentar libros digitales de Google ha generado reacciones de otras empresas informáticas. Según Tom Rubin, Director de asuntos jurídicos de Microsoft, "Google parece tratar de sobrepasar los límites de los derechos de propiedad de todas las maneras posibles". Este abogado también "rechazó la justificación aducida por el gigante de internet sobre un uso justo bajo la ley de protección de derechos intelectuales, llamándola una nueva interpretación que se extendería a países en los cuales el concepto de uso honesto ni siquiera es reconocido" En relación con la circulación de contenidos Rubin afirmó "Microsoft trata de colaborar con quienes tienen derechos a la propiedad intelectual en el desarrollo de las tecnologías a fin de respetar los derechos de autor sin los cuales ningún artista o escritor y ninguna sociedad que aspira a una cultura viva puede expandirse". [35]

En el mismo sentido Google News también ha sido objeto de demandas por la indexación de periódicos belgas la cual aparentemente omite la información publicitaria y por Viacom con base en derechos de autor violados en la red social You Tube. Ambos casos están pendientes de ser resueltos por los tribunales belgas y de los Estados Unidos respectivamente. [36]

---

34 www.ftc.gov

35 Portafolio "Microsoft acusa a Google de pirata" el 8 de marzo de 2007 p. 22.

36 Mennecke Thomas. "Viacom strikes google, youtube with lawsuit" en http://www.slyck.com/news.php?story=1441

C. El caso de los hackers y sus ataques a la intimidad

Los *hackers* o intrusos de la red que violan las medidas de seguridad de los navegantes o de los propietarios de los sitios de internet son otra amenaza para la privacidad de los individuos y compañías que interactúan en la red.

El costo económico de las intrusiones de los hackers es muy alto. MCI perdió cerca de cincuenta millones de dólares cuando, por ejemplo, una intrusión ilegal accedió a cincuenta mil números de tarjetas de crédito[37] y CitiBank perdió diez millones de dólares cuando los controles de su red fueron violados por un grupo criminal en Rusia[38].

Internet ha exacerbado la actividad de los hackers y ha obligado la creación de mecanismos de seguridad para luchar contra las intrusiones ilegales[39]. Incluso organizaciones internacionales como la OECD –Organización de los Países Desarrollados– ha propuesto que exista un regulador central que estudie medidas de prevención y quizás establecer sanciones por irrupciones a las redes informáticas con repercusiones globales.

Bajo iniciativa de la Organización Mundial de la Propiedad Industrial (OMPI) en el Tratado WCT o tratado de internet sobre Derecho de Autor[40], recientemente aprobado en Colombia y que ha sido incluido en el nuevo código penal, establece como hecho punible el acceso no autorizado a redes de computadoras y la violación a los mecanismos de protección de los derechos patrimoniales de autor.[41]

---

37 GRIPMAN, DAVID. The doors are locked but the thieves and vandals are still getting in. A proposal in tort to alleviate corporate americas cybercrime problem. 16 John Marshall Journal of Computer Law & Information ,1997, p. 169-170.

38 GOODMAN, MARC. Why the police don't care about computer crime, 10 Harvard Journal of Law and Technology, p 465 472 (1997).

39 Un completo resumen de los mecanismos técnicos utilizados por los hackers así como los mecanismos de seguridad se puede consultar en el artículo de LEE MICHEL et al Electronic Commerce Hackers and the Search for legitimacy: a regulatory Proposal , trabajo ganador del Premio de 1998 de la Berkeley Technology law Journal .

40 El artículo 11 del Tratado WCT establece:
Artículo 11. Obligaciones relativas a las medidas tecnológicas.
Las Partes Contratantes proporcionarán protección jurídica adecuada y recursos jurídicos efectivos contra la acción de eludir las medidas tecnológicas efectivas que sean utilizadas por los autores en relación con el ejercicio de sus derechos en virtud del presente Tratado o del Convenido de Berna y que, respecto de sus obras, restrinjan actos que no estén autorizados por los autores concernidos o permitidos por la ley.
En Publicación OMPI # 226(S), septiembre de 1997, Ginebra

41 El artículo 272 de la ley 599 de 2000 (nuevo código penal) establece:
Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones:
Incurrirá en multa quien:
1. Supere o eluda las medidas tecnológicas adoptadas para restringir los usos no autorizados.

D. Responsabilidad por infracción de marcas en internet

La infracción más extendida de las marcas en internet se presenta como consecuencia del registro de los nombres de dominio similares o iguales a las marcas registradas por otros. El bajo costo, un dominio puede llegar a valer en promedio U$ 10 dólares, y la facilidad de registro han propiciado la práctica de la ciber-ocupación, es decir la usurpación de marcas, en su mayoría notorias, por personas que obtienen el registro de un nombre de dominio igual o similar.[42]

El ánimo de fácil lucro ha sido, como en el caso de otros casos de piratería, la fuerza e impulso de quienes registran dominios similares o iguales a marcas notorias. Muchas compañías establecidas y con tradición en el mundo de los negocios han tratado infructuosamente de registrar dominios que corresponden a sus marcas como consecuencia de que piratas se les han anticipado en el registro de un dominio determinado.

El principal y más utilizado mecanismo creado para evitar dichas infracciones es la Política Uniforme de Resolución de Disputas de ICANN[43] que permite a un titular de una marca cancelar el registro de un dominio si se configuran los tres elementos necesarios, a saber, (a) el dominio sea igual o similar a la marca registrada; (b) el registrador de dominio no tenga un derecho legítimo y (c) el registro del dominio haya sido obtenido de mala fe y el dominio esté siendo usado de mala fe.[44]

Es interesante observar como los paneles del Centro de Arbitraje y Conciliación de la OMPI – y en general los centros de Conciliación que deciden los casos bajo la Política Uniforme de Disputas de ICANN han sido favorables en un amplio porcentaje en más de 12000 casos, a los titulares de marcas y en una proporción aún mayor a favor de los titulares de marcas notorias.

---

2. Suprima o altere la información esencial para la gestión electrónica de derechos, o importe, distribuya o comunique ejemplares con la información suprimida o alterada.
3. Fabrique, importe, venda, arriende o de cualquier forma distribuya al público un dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal, o de cualquier forma de eludir, evadir, inutilizar o suprimir un dispositivo o sistema que permita a los titulares del derecho controlar la utilización de sus obras o producciones, o impedir o restringir cualquier uso no autorizado de éstos.
4. Presente declaraciones o informaciones destinadas directa o indirectamente al pago, recaudación, liquidación o distribución de derechos económicos de autor o derechos conexos, alterando o falseando, por cualquier medio o procedimiento, los datos necesarios para estos efectos.

42 PEÑA VALENZUELA, DANIEL la piratería en internet, Revista La Propiedad Inmaterial N.º 2 del Centro de Estudios de la Propiedad Intelectual de la Universidad Externado de Colombia, Agosto 2001

43 Una descripción de la Política Uniforme de Resolución de Disputas se encuentra en la dirección http://eon.law.harvard.edu/udrp/process.html

44 Cfr. En la dirección electrónica www.icann.org

Colombia no ha sido la excepción a esta práctica, muchas empresas establecidas han sido sujetos pasivos de la conducta de los piratas de los dominios. Han sido reportados dos casos resueltos por los panelistas en el sistema de la Política Uniforme de Resolución de Disputas de ICANN relacionados con Colombia.

Varios de esos casos, por ejemplo, los relacionados con los nombres de dominio BANCOLOMBIA.COM, BANCOCAJASOCIAL.COM, AVVILLAS.COM, CASAEDITORIALELTIEMPO.COM, TRANSMILENIO.COM, BANCODEOCCIDENTE.COM y BANCOTEQUENDAMA.COM[45], involucran actos de infracción de marcas notorias de esas reconocidas compañías. Estos casos fueron fallados a favor de los titulares de las marcas.

Desde la óptica de la responsabilidad, la mala fe en el registro es incluida como requisito para que el panel de expertos pueda decretar el traspaso o cancelación del nombre de dominio. Sin embargo, es evidente que el daño se configura por el simple registro de un nombre de dominio, sin derecho legítimo, similar o igual a una marca registrada. La jurisprudencia, en particular, la de los panelistas del Centro de Arbitraje de la OMPI, ha demostrado que el requisito de la mala fe ha sido morigerado en el sentido de inferir la mala fe de hechos o actos y darle un gran valor a la prueba de indicios de mala fe.

La aplicación concreta de la PURD ha sido, en consecuencia, una demostración del carácter objetivo de la responsabilidad a pesar de que uno de sus requisitos era "absolutamente" subjetivo: la mala fe. Además es importante tener en cuenta que la Política Uniforme de Resolución de Disputas fue adoptada por el Nic-Colombia como la forma de resolver las disputas entre los dominios locales *".co"*.

La Comunidad Andina ha previsto una nueva acción para reprimir las infracciones de las marcas notorias cometidas por el registro de los dominios o por la utilización de direcciones de correo electrónico. El artículo 233 de la Decisión 486 de la Comunidad Andina de 2000 establece la acción de nulidad o modificación de un dominio o dirección de correo electrónico, a presentarse ante la Autoridad Nacional Competente –Superintendencia de Industria y Comercio– si viola los derechos del titular de una marca notoria. Además de la cancelación o nulidad se pueden solicitar los perjuicios causado por la infracción.

E. Responsabilidad de las entidades de certificación

Existe una variedad de maneras de firmar en la "era digital". Incluir el nombre en un mensaje de correo electrónico o enviar un correo electrónico desde su cuenta de correo electrónico propia –la cual en muchos casos incluye algún elemento relacionado con

45 Consultar fallos en www.wipo.int.

el nombre y apellido del propietario de la cuenta, permite un grado de certeza sobre la identidad de quien envía el mensaje.[46]

El art. 7.º de la ley 527 de 1999 es la norma esencial de las firmas que aplicadas a los mensajes de datos tienen el valor que se concede a las firmas manuscritas siempre y cuando se haya utilizado un método apropiado de identificación del iniciador. Ese método debe ser confiable y apropiado para los fines de las partes.

Con base en el art. 7.º citado se podría, por ejemplo, afirmar que un mensaje de e-mail enviado desde una cuenta de correo electrónico determinada y vinculada a su creador podría ser considerado como firmado. Lo anterior teniendo en cuenta que por muchas razones comerciales y técnicas la utilización de una cuenta personal de correo electrónico constituye un método adecuado para identificar a una parte, dependiendo claro está de la finalidad específica. Nadie osaría afirmar que un contrato de compraventa de mercancías de varios millones de dólares sea celebrado con base en un mensaje relativamente anónimo utilizando una cuenta gratuita de *hot mail, yahoo o google.*

Sin embargo, para lograr un grado de certeza comparable al de una firma manuscrita, una firma electrónica puede ser firma digital, para lo cual se requiere que ésta sea:

(1) Única respecto del firmante.
(2) Creada usando mecanismos o medios que estén bajo el control exclusivo del firmante.
(3) Capaz de ser relacionada con un documento determinado de tal manera que cualquier cambio posterior a los documentos o a la información contenida en el mismo sea detectable.

La certificación por parte de un tercero de confianza o entidad de certificación sobre la identidad del firmante la reviste de una mayor certeza similar a la de una firma que haya sido autenticada ante notario.

Con una función similar al de notarios de las transacciones electrónicas se han instituido bajo el modelo de la CNUDMI, las entidades de certificación que son terceros que permiten reestablecer la confianza en las transacciones electrónicas. La desconfianza proviene usualmente del desconocimiento del sujeto con quien se negocia.

La entidad de certificación verificará la identidad del emisor del mensaje de datos –por ejemplo revisando los datos del documento de identidad o de la identificación societaria– y emitirá un certificado digital, firmado con la firma digital de la entidad de cer-

46 Artículo 7 de la ley 527 de 1999

tificación para corroborar su autenticidad, el cual permitirá verificar que el originador del mensaje es quien afirma ser.[47]

En el caso de las entidades de certificación cerrada, los certificados digitales deberán indicar expresamente que sólo podrán ser usados entre la entidad emisora y el suscriptor. Los certificados digitales emitidos por las entidades de certificación cerradas no permiten cumplir como satisfechos los requisitos de la firma digital, en consecuencia quien desee beneficiarse de la presunción de autenticidad inherente a ese tipo de firma deberá probar el cumplimiento de las condiciones previstas en el artículo 28 de la ley 527 de 1999. Los certificados de las entidades de certificación abiertas podrán desempeñar sin limitación las actividades enunciadas en el artículo 30 de la ley 527 de 1999.

La responsabilidad legal de las entidades de certificación está vinculada a los amplios deberes establecidos por la ley, los cuales las convierten en custodios de la información suministrada por los usuarios, además les obligan a implementar sistemas de seguridad adecuados para que los mecanismo de firmas y certificados digitales sean confiables.[48]

La responsabilidad no solo recae en la entidad de certificación, también los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor. [49]

---

47 Concepto 00076258 del 21 de diciembre de 2000 de la Superintendencia de Industria y Comercio

48 Artículo 32 de la ley 527 establece:
"Deberes de las entidades de certificación.
Las entidades de certificación tendrán, entre otros, los siguientes deberes:
a) Emitir certificados conforme a lo solicitado o acordado con el suscriptor;
b) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos;
c) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el su suscriptor; d) Garantizar la prestación permanente del servicio de entidad de certificación;
e) Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores;
f) Efectuar los avisos y publicaciones conforme a lo dispuesto en la ley;
g) Suministrar la información que le requieran las entidades administrativas competentes o judicial es en relación con las firmas digitales y certificados emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;
h) Permitir y facilitar la realización de las auditorías por parte de la Superintendencia de Industria y Comercio;
i) Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación d el servicio;
j) Llevar un registro de los certificados.

49 Artículo 39. Deberes de los suscriptores.
Son deberes de los suscriptores:
1. Recibir la firma digital por parte de la entidad de certificación o generarla, utilizando un mét odo autorizado por ésta.
2. Suministrar la información que requiera la entidad de certificación.
3. Mantener el control de la firma digital.
4. Solicitar oportunamente la revocación de los certificados

Debido a las amplias cargas que el legislador ha atribuido a las entidades de certificación, en el Decreto reglamentario 1747 ha establecido que en la Declaración de prácticas de certificación se deberá incluir los límites de responsabilidad por las actividades que desempeñe y las garantías que ofrece en el desempeño de sus funciones[50]. Estas garantías incluyen seguros y contratos de fiducia.[51]

Finalmente, el decreto reglamentario reitera un principio general "las entidades de certificación responderán por todos los perjuicios que causen en el ejercicio de sus actividades"[52]. Lo anterior ratifica la aplicación de la teoría general de la responsabilidad a las entidades de certificación.

Las entidades de certificación son responsables frente a los prestadores de servicios, los suscriptores o las personas que confíen en los certificados. Es decir que una persona que sufra un perjuicio por la transacción en el que pueda probar que actúo con base en un certificado digital determinado podría demandar no solamente al comerciante sino también a la entidad de certificación.

No nos parece que si el conflicto esta relacionado con el contenido y objeto del negocio electrónico la responsabilidad necesariamente sea de la entidad de certificación. La norma anterior se refiere más a la "representación" que la parte se haga respecto de con quien esté contratando. En un litigio concreto es evidente que separar los dos temas sería complejo pero atribuir *a priori* cualquier responsabilidad a las entidades de certificación respecto de las prestaciones de los negocios electrónicos extiende en exceso su responsabilidad.

La responsabilidad de las entidades de certificación también abarca los eventos cuando contratan repositorios de certificados digitales con terceros y en el caso de que cesen sus actividades sin la autorización previa de la Superintendencia de Industria y Comercio, en el entendido de que posteriormente se causen perjuicios a los suscriptores o terceros.[53] Es evidente que el legislador ha considerado que las entidades de certificación desempeñan una actividad riesgosa, es la única explicación para que se hayan previsto tan extremos requisitos para su operación.

Con la reforma de la ley 80 de contratación estatal, la responsabilidad por contratos públicos por medios electrónicos y por actos administrativos también por esos medios recae en los servidores públicos que estén a cargo de la celebración de contratos o en los que recaiga la competencia para expedir los actos administrativos.

---

50 Artículo 6, numerales 5 y 6 del decreto 1747 de 2000

51 Artículo 8 del decreto 1747 de 2000

52 Artículo 18 del decreto 1747 de 2000

53 Artículos 19 y 20 del decreto 1747 de 2000

V. RETOS DE LA RESPONSABILIDAD EN LA ERA DIGITAL

Luego de analizados los ejemplos de cambios en la responsabilidad por los nuevos sujetos participantes de la sociedad de la información, es pertinente considerar de manera sintética algunos de los retos por las cuales la responsabilidad jurídica adquiere una dimensión global y con esquemas de tiempo y espacio diferentes a los de la visión relativamente estática y tradicional del derecho:

(a) Virtualización de los sujetos:

> La red global ha generado la posibilidad de que usuarios y navegantes participen de manera anónima o seudónima en cuentas de correo y comunicaciones interactivas. En la actualidad en juegos de realidad virtual los sujetos asumen roles diversos en esos mundos imaginarios con la posibilidad de interactuar con otros y ocasionar daños.

(b) Velocidad y eficiencia de las transacciones:

> La red global ha impulsado la creación de mercados electrónicos, sea entre empresas y consumidores o entre empresas. Esos mercados electrónicos están relacionados con la propiedad inmaterial por cuanto muchas de las transacciones incluyen directa o indirectamente activos intangibles.

(c) Movilidad de las actividades y transacciones en internet:

> Las actividades en internet relacionadas con la propiedad intelectual, en particular la distribución y licencia de contenidos, obras protegidas, programas de ordenador pueden ser ubicadas en páginas en servidores y luego trasladada en cuestión de segundos a otro sitio virtual. Lo anterior, tiene como consecuencia que existen dificultades probatorias frente a estas actividades. Temas como la notificación y la aplicación de leyes son complejos en un ambiente global, rápido, nómada y sin territorios definidos. La localización del servidor donde está ubicada la página, el lugar donde se registro la dirección del sitio o nombre de dominio, el sitio donde se realiza la oferta electrónica de bienes y servicios son algunos de los criterios utilizados para determinar donde se debe decidir un conflicto y bajo que ley[54].

---

54 La dificultad de establecer el origen de un sitio de internet fue ratificada en un extenso análisis realizado por la Corte Constitucional de Colombia. Sentencia N.º C-1147 de 31 de octubre de 2001. Exp. D-3495. Magistrado Ponente Manuel José Cepeda.

(d) Dificultad de establecer el valor de los intangibles para medir el perjuicio causado:

> Un aspecto que empieza a cobrar importancia al momento de evaluar un litigio relacionado con intangibles es su valor con el fin de fijar los perjuicios materiales y morales causados. Es frecuente que las compañías no registren en sus libros de contabilidad y en el balance general sus intangibles, a pesar de existir la posibilidad –si no la obligación- de incluir esos rubros contables en los estados financieros de las compañías. Esta tendencia aparentemente busca limitar el impacto que tendría la carga tributaria relacionada con los intangibles. Sin embargo, la falta de contabilización de los intangibles puede complicar el cobro de perjuicios relacionados con la violación de tales derechos.[55]

(e) Múltiples jurisdicciones involucradas:

> La aceleración de las comunicaciones, la facilidad para las transacciones electrónicas y la masificación de internet propician que el comercio internacional sobre intangibles sea cada vez más creciente. La industria del entretenimiento y del software son motores de esta revolución.

Las reglas del derecho internacional privado que tradicionalmente han permitido resolver los conflictos de leyes en los casos que involucran varias jurisdicciones, deben ser modificadas con el fin de permitir que dichas reglas resulten más apropiadas para la nueva economía.[56]

El caso fallado por la jurisdicción francesa respecto de la compañía norteamericana Yahoo, Inc., relacionado directamente con responsabilidad por la provisión de contenidos, ha puesto en plena discusión a escala mundial el conflicto territorial de leyes que las tecnologías de la información originan.[57] El caso fue iniciado por la Liga de Defensa de los Intereses Semitas en Francia contra el proveedor de servicios de internet, Yahoo, Inc. con el fin de que este último impidiera la venta de artículos neo-nazis a través de su portal. Luego de un concepto técnico el juez francés ordenó proceder a filtrar los contenidos. El fallo, al momento de su aplicación, fue rechazado por un juez de San Francisco que consideró que este violaba la libertad de expresión establecida en la Constitución americana.[58]

---

55 La valoración de intangibles en la ley colombiana está descrita en el concepto 53011 de la DIAN de junio 23 de 2000 en particular en referencia al artículo 223 de 1995.

56 GOLDSMITH, JACK The Internet and the abiding significance of territorial Sovereignty en http://www.law.indiana.edu/ijgls/archive/05/02/goldsmith.shtml.

57 SWIRE, PETER "Of elefants, mice and privacy: international choice of law and the internet" en The International Lawyer, Winter 1998, Vol. 32, N.º 4, Nueva York.

58 KAPLAN CARL. "French Decision Prompts Questions About Free Speech and Cyberspace" en The New York Times, 12 febrero de 2002 .

Lo anterior muestra que el sistema internacional no está aún bien adaptado a la multiplicidad de sujetos y jurisdicciones involucradas. Actualmente, existen iniciativas como consecuencia de la aparición y desarrollo del ciberespacio, para reformar tratados internacionales que son fundamentales para resolver los conflictos de leyes, en particular, la Convención de la Haya de Derecho Internacional Privado y los Tratados de Montevideo[59]. El sistema jurídico actual es insuficiente y es vulnerable a la impunidad o al incumplimiento de reglas sin sanción.

La responsabilidad civil y penal tambalean en su estructura, desarrollo, elementos y fundamentos por cuenta del crecimiento y sofisticación de los modelos de negocios propios del ciberespacio y de la habilidad de las nuevas generaciones para manipular los sistemas de la información. De la perplejidad por los tentáculos de la mafia o de la delincuencia de cuello blanco pasaremos a la avasallante realidad del crimen informático: del robo de identidades, del secuestro virtual, del terrorismo tecnológico, etc.

VI. EPÍLOGO: EL CASO DE RESPONSABILIDAD EN SECOND LIFE

Uno de los casos de responsabilidad legal más novedoso y que genera mayor discusión es el de la red virtual "Second Life". Esta comunidad fue creada por el Linden Lab como un mundo virtual imaginado, creado y poseído por sus residentes-participantes. En la actualidad más de seis millones de personas utilizan esa comunidad. En Second Life cada participante asume una identidad a través de la escogencia de unas características determinadas y se encarna en un *avatar* o personaje ficticio.

Recientemente la televisión alemana denunció que un avatar que "representa" a un adulto había tenido una relación sexual virtual con otro avatar que personificaba a un niño. Los avatares relacionados con el caso de pederastia resultaron ser un hombre de 54 años y una mujer de 27 y ambos fueron inmediatamente expulsados de Second Life. [60] Es decir que en este caso, dos adultos, de mutuo acuerdo, encarnan roles en una fantasía sexual con delito de por medio incluyendo un personaje ficticio menor de edad. En lo virtual se pueden afectar diversos bienes jurídicos y se puede generar daño resarcible pero no se puede olvidar que el ciberespacio y lo que ocurra en ése no es totalmente real y que se pueden afectar derechos sobre bienes intangibles.

---

59 Bueno, Fabio. La recepción de las pruebas judiciales en el extranjero, 1999 Universidad Externado de Colombia

60 Portafolio. "Second Life, tierra virtual sin ley", 16 de mayo de 2007.

CONCLUSIONES

1. La responsabilidad en la sociedad de la información es una consecuencia de la realización por sujetos jurídicos de actividades en la red y a través de ella.
La existencia de daños en el ciberespacio ratifica que éste debe que ser regulado.

2. Las cargas de responsabilidad en los agentes económicos que participan en la red definen sus riesgos y les permiten ser conscientes del impacto jurídico que puede tener participar en la red.

3. Existen diversos intermediarios en la red como los proveedores de servicios de acceso, alojamiento de páginas que por su función esencial en internet han sido objeto de aplicación directa del concepto de responsabilidad legal. La noción, alcance y actividades de los intermediarios ha ido cambiando en la medida de que las tecnologías de la información se han desarrollado habilitando la posibilidad de nuevos negocios.

4. Las entidades de certificación como terceros de confianza en las transacciones electrónicas y como protectores de la fe pública en la red tienen un régimen fuertemente regulado en cuanto a deberes y responsabilidad. Además deben cumplir con requisitos legales en su constitución y en la cesación eventual de sus funciones que añaden riesgos legales a su actividad.

5. Los usuarios también tienen responsabilidad sea por deberes de conducta generales o por relaciones contractuales que adquieren al participar en la red. La protección de los datos personales de los navegantes y, en particular, el uso adecuado que de estos hagan los propietarios de los sitios es un fundamento para que la red no sea instrumento de violación del derecho fundamental de intimidad.

6. La globalización y la red internet hacen parte de un mismo proyecto, uno y otro fenómeno tiene impacto en su desarrollo. El carácter internacional de la red exacerba los conflictos de leyes, la dificultad de las pruebas en el extranjero y las jurisdicciones involucradas.

7. Se propugna por la *objetivización* de la responsabilidad con predominio del daño como base de la estructura de la responsabilidad en la era digital y la teoría del riesgo como sustitutiva de la culpa en ciertas actividades en las cuales la intervención humana no es la preponderante.

8. En Colombia es aconsejable que se establezca, mediante una ley, la regulación de la responsabilidad de los Proveedores de servicios de internet asimilando de manera crítica la experiencia internacional pues hasta ahora además de las reglas tradicionales solo existe la propuesta de regulación por la vía del tratado de libre comercio con los Estados Unidos.