

Propuesta de San Cristóbal

*Sobre Puntos Mínimos para la Sociedad de la Información
en América Latina y el Caribe*

Antecedentes

(Documento Referencial 1)

Índice:

Existentes

Políticas de Seguridad de la Información para el sector público.

Uso de software libre en la administración pública.

Lucha contra el SPAM

Sobre Delitos Informáticos

Aspectos de Derechos de Autor en el entorno digital.

Sobre la Internacionalización del Ciberespacio

Pendientes

Aspectos tributarios del comercio electrónico.

Validez del documento electrónico.

Privacidad y Protección de Datos Personales.

Acceso a la Información Pública / Transparencia de la Gestión Pública

Responsabilidad de los ISP.

Competencia desleal en el entorno digital.

Políticas de Seguridad de la Información para el sector público.

El uso de las tecnologías de la información permite a cualquier organismo del Sector Público obtener y procesar gran cantidad de información imprescindible para su normal funcionamiento. Así, gran parte de la información que utiliza un organismo es tratada electrónicamente, habiéndose por consiguiente incrementado el número de amenazas y vulnerabilidades que rodean a los activos de información.

La información que maneja un organismo del Sector Público es de suma importancia para el desarrollo de sus actividades y su obtención en tiempo y forma es esencial para la continuidad de su operatoria. Asimismo, gran parte de dicha información reviste un alto grado de confidencialidad lo cual requiere establecer controles en su resguardo y divulgación.

Así las cosas, surge a las claras que cualquier violación a la seguridad de la información podría afectar la operatoria del organismo, poniendo en riesgo la prestación continua e ininterrumpida de los servicios brindados para satisfacer las demandas de los ciudadanos.

Es por ello que resulta necesario implementar medidas que procuren la protección de la información, lo cual implica preservar las siguientes características:

- **Confidencialidad:** garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** asegurar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

La primera medida para gestionar en forma adecuada la seguridad de la información consiste en realizar una declaración formal de las pautas que deben ser respetadas para el manejo de la información, cualquiera sea su representación y ubicación. En otras palabras, definir una Política de Seguridad de la Información.

En nuestros países encontramos hoy una ausencia casi total del Estado en lo relativo a la adopción y/o sugerencia de estándares de seguridad de la información, tanto para el mismo sector público como para el sector privado.

Como consecuencia inevitable, encontramos que nuestras entidades públicas tienen niveles de seguridad paupérrimos, que suelen obedecer más a la interpretación que un consultor privado ha hecho de un estándar aceptado en la industria que a una aplicación estricta y completa del mismo. Por su parte, salvo por los sectores financiero, bancario y bursátil, en los que existen regulaciones que les obligan a realizar estudios de riesgo y a implementar medidas mínimas de seguridad, encontramos que el sector privado se encuentra mayoritariamente desprotegido.

Esta situación es a todas luces inaceptable y no se justifica que, a la fecha, los estados hayan

permanecido completamente inactivos frente a la seguridad de su propia información y de relativa a sus ciudadanos. Si bien es comprensible que la prioridad para nuestros países sean temas como la lucha contra el hambre, la violencia y la corrupción, también es cierto que hoy la información es el activo más precioso en la sociedad, razón por la cual debe ser debidamente protegida.

En mérito a lo expuesto es que recomendamos a los estados de LAC que desarrollen e implementen políticas de seguridad de la información, siendo conveniente que todas ellas compartan los mismos criterios. Para ello entendemos necesario que las políticas a desarrollarse se basen en un mismo modelo, siendo el más adecuado la norma ISO 17799, toda vez que se trata de un modelo que ya ha sido analizado, probado e implementado en forma satisfactoria, habiendo obtenido ya el reconocimiento del mercado.

Solo de esta forma entendemos que los estados de LAC estarán en condiciones de proteger a la información que procesan de una amplia gama de amenazas, lo cual permitirá garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de sus objetivos y obligaciones para con el ciudadano.

Propuestas

- Elaborar planes y proyectos generales y atenerse a ellos en la planificación, aplicaciones, controles de calidad, detallando lo más posible las aplicaciones, el desarrollo y tiempos previstos, etc, aplicar criterios de calidad, eficiencia, etc. Esto hace a la no a la improvisación, teniendo en cuenta la realidad en la cual se implantará en el tema concreto, la política de seguridad. Esto se considera muy importante en cuanto a la realidad humana y posibilidades de cambio de mentalidad..y también a atenerse a los recursos con que se cuenta.
- Tener en cuenta que el tema Seguridad de la Información es uno de los puntos básicos, y que es uno de los puntos fundamentales, junto a la Seguridad Jurídica y a la Seguridad Legal.
- Auditorias serias periódicas, controles de calidad estrictos.
- Políticas y planes ajustados a los recursos: tener en cuenta recursos materiales y humanos, en cuanto a los primeros, el plan debe tener resuelto su financiación total antes de ponerse en marcha. En recursos humanos: capacitación, que incluye concientización de la importancia de la calidad (y sobre todo en el tema seguridad) y su relación con el ahorro de costos a largo plazo: la ineficiencia es muy cara.
- Estándares técnicos y control de cumplimiento (auditorias) establecerlos específicamente.
- En seguridad: tener en cuenta no solo seguridad física y lógica de los equipos sino seguridad física general: locales, control del personal, accesos, etc.
- Importancia de las políticas, normas y procedimientos, y su puesta en práctica, difusión, cumplimiento estricto, no un papel vacío, respetar normas internacionales de calidad en la elaboración de las políticas.
- Equipos humanos de trabajo calificados, responsables, menos políticos y más técnicos (técnico jurídicos-técnico informáticos) especializados (no cualquier jurista sabe



elaboración de normas jurídicas por ej. conscientes además de la importancia de estos temas..)

- Formación adecuada y existencia legal y real de peritos informáticos en el Poder Judicial: sin eso no hay garantías de seguridad que valgan.

Uso de software libre en la administración pública.

Fundamentos comunes de las normativas en torno a Software Libre

Si bien cada uno de las normas y proyectos de ley que actualmente existen en la región, poseen características particulares y fueron concebidos en contextos determinados, se advierten ciertos fundamentos y principios subyacentes compartidos por la mayoría de ellos:

1. Posibilidad de evaluar el software

Al disponer del código fuente de los programas en su completitud, éste puede ser analizado por personas ajenas a sus autores en busca de fallos de diseño o de implementación, pudiéndose realizar auditorías de dicho código.

Eventualmente, las evaluaciones pueden derivar en adaptaciones y/o mejoras, que también pueden disminuir los riesgos de seguridad debido a la aparición de fallos desconocidos, a la introducción de funcionalidades no deseadas en el código o la incorrecta implementación de algoritmos públicos.¹

2. Aprovechamiento más adecuado de los recursos

Muchas aplicaciones utilizadas o promovidas por los estados son también utilizadas por muchos otros sectores de la sociedad. Por ello, cualquier inversión pública en la adquisición y desarrollo de software libre beneficiará tanto a la propia administración como a todos los ciudadanos que podrán usar libremente ese producto para sus tareas informáticas. Ello en virtud de no mediar las restricciones impuestas por las licencias del software propietario ya mencionadas.

3. Fomento de la industria local

La adquisición de software libre por parte del estado puede impulsar el desarrollo de la industria local de software, ya que cuando se usa productos propietarios, el capital gastado en licencias en su mayor parte son giradas a las casas matrices en conceptos de regalías por el derecho de autor.

El ahorro que implicaría adquirir software libre -derivado de los costos de licencias y de la optimización de la inversión- se podría orientar a la contratación de desarrollos a terceros promoviendo el uso de la mano de obra local calificada.

Así, las empresas locales podrán competir proporcionando servicios (y el propio programa) al estado, en condiciones muy similares a cualquier otra empresa. Mediante la adquisición de software libre, el estado estaría generando un mercado más competitivo en el que las empresas locales pueden usufructuar ventajas competitivas, tales como el mejor conocimiento de las necesidades del cliente, la cercanía geográfica, etc.

¹ Muchos de los proyectos de software libre, entre ellos el núcleo de Linux, el proyecto Apache, y la distribución OpenBSD realizan auditorías del código para asegurar su integridad, seguridad y ajuste a las especificaciones de funcionalidades requeridas

4. Independencia de proveedor

Desde una perspectiva económica, un mercado o segmento del mercado no será atractivo para el consumidor cuando los proveedores estén muy bien organizados, tengan fuertes recursos y puedan imponer sus condiciones de precio del producto. La situación será crítica si los insumos que suministran son claves para la actividad del usuario y no existen sustitutos o son pocos y de alto costo.

En caso que el Estado no pueda disponer del código fuente, queda obligado a depender de una aplicación cerrada para acceder a sus propios datos. Al emplear formatos cerrados, la información volcada por el propio Estado sólo puede ser decodificada correctamente por el diseñador del formato, sea éste una empresa o persona física de cualquier origen o dimensión.

Como estos formatos cerrados son cambiados periódicamente por los fabricantes, se genera una dependencia tecnológica constante, obligando al estado a actualizar permanentemente las versiones de software que utiliza, so riesgo de quedar incomunicado en el universo informático como de perder valiosa información disponible, la cual, en la mayoría de los casos, le fuera confiada por los ciudadanos por exigencias de distintos organismos estatales.² Cuando un estado emplea el tipo de herramientas cerradas para intercambiar información digitalizada con sus ciudadanos, termina actuando como promotor del producto de los diferentes fabricantes o como cómplice involuntario de prácticas comerciales indeseables.

En el supuesto de adquirir software libre, cualquier empresa interesada estará en condiciones de proporcionarlo, así como también cualquier tipo de servicio asociado, eliminándose todo tipo de dependencia con un único proveedor.

La pluralidad de oferentes fortalece el debilitado poder de negociación de los estados a la hora de adquirir software, lo cual se verá necesariamente reflejado en una mejora en el precio, calidad, servicio u otros términos de venta.

5. Adaptación a las necesidades exactas

En el supuesto del software propietario, a fin de ajustar el producto a nuevas necesidades, las cuales pueden ir variando con el transcurso del tiempo, será necesario llegar a un acuerdo con el titular de sus derechos. Habida cuenta de la asimetría existente en el proceso de negociación en esta clase de productos, el costo por parte del estado de realizar alguna adaptación será muy elevado.

Por el contrario, usando un producto libre, el organismo puede modificarlo a su antojo, bien sea utilizando su personal, bien sea contratando externamente la modificación para el caso de no tener personal capacitado.

² Estos datos pueden tratarse de información íntima de sus ciudadanos, la cual el Estado tiene la obligación de salvaguardar, como también de información sensible relacionada con cuestiones de Estado. Son numerosos los ejemplos ocurridos en países de primer orden mundial donde no ha sido posible recuperar antiguos archivos digitales por haber cesado sus actividades comerciales la empresa fabricante que proveyera el software y desconocerse los formatos empleados en su diseño.

Nuevamente, el estado se verá beneficiado económicamente al ver que sus costos disminuyen y la calidad de su software se incrementa.

6. Seguridad de la Información

La prohibición de acceso tanto al programa fuente, como al código fuente, que constituyen el sistema operativo de la computadora, como a los formatos y aplicaciones, implica una imposibilidad de control por parte del Estado sobre la información propia que disponga bajo soporte digital.

La información puede ser objeto de una amplia gama de amenazas, debiéndose preservar su confidencialidad, integridad y disponibilidad, a fin de garantizar la prestación continua e ininterrumpida de los diversos servicios prestados por los estados a los ciudadanos.

El Sector Público debe proveer sus servicios con las máximas garantías de seguridad para satisfacer apropiadamente las demandas de la población y para evitar la comisión de ilícitos, por lo que deviene necesario implementar políticas de seguridad que contemplen procedimientos internos y sistemas de defensa adecuados.

Resulta fundamental garantizar que los sistemas informáticos hagan sólo lo que está previsto que hagan a fin de evitar interrupciones en los sistemas así como también fuga de datos personales o confidenciales (pensemos en datos fiscales, penales, policiales, electorales, etc.). La incompatibilidad entre el modelo de licenciamiento privativos y la seguridad requerida por el estado, proviene de la prohibición expresa, o de las insuperables restricciones de orden práctico, que representa el mecanismo privativo para llevar a cabo las tareas que permitan fiscalizar y asegurar el cumplimiento de dichos principios.

Difícilmente si se usa una aplicación propietaria sin código fuente disponible, se pueda asegurar que efectivamente esa aplicación procese esos datos como debe.³ Sólo contando con el código fuente una institución pública podrá auditar el funcionamiento del programa y realizar las mejoras y adaptaciones pertinentes.

7. Disponibilidad en el largo plazo e inmediata

El estado maneja gran cantidad de información y requiere de diversos programas para procesarla, los cuales deben estar disponibles por un largo período de tiempo. La vida útil de los programas o el ciclo de vida de la empresa proveedora pueden no satisfacer esta exigencia, lo cual puede hacer peligrar la disponibilidad del programa dentro de algunos años. Es muy posible que el proveedor haya perdido interés en el producto y no lo haya

³ Se ha descubierto que el producto *Microsoft Windows XP* se conecta sin intervención del usuario y sin su conocimiento, en 16 circunstancias distintas a servidores de Microsoft, entregando información a dicha empresa. Los problemas de privacidad que surgen con este tipo de prácticas son evidentes. Para profundizar en el tema ver: <http://www.hevanet.com/peace/microsoft.htm>

portado a nuevas plataformas, o que sólo esté dispuesto a hacerlo ante grandes contraprestaciones económicas.

Por el contrario, en el caso del software libre la aplicación está disponible para que cualquiera la porte y la deje funcionando según las necesidades de la administración. Si la empresa titular del software no quiere hacerlo o ya no existe, o bien el organismo carece de personal capacitado para desarrollar la tarea, la administración siempre puede dirigirse a varias empresas buscando la mejor oferta para hacer el trabajo. Así, se puede llegar a garantizar que la aplicación y los datos que maneja estarán disponibles cuando haga falta.

Sin perjuicio de los beneficios expuestos, lo cierto es que la mayoría de los proyectos todavía no han sido aprobados. Ello en virtud de una multiplicidad de obstáculos, cuyo análisis excede el marco del presente trabajo, pero que a continuación trataremos de sintetizar.⁴

El primer obstáculo con que se encuentra el software libre para su introducción en las administraciones es su desconocimiento por los tomadores de decisiones, por lo que su adquisición supone la asunción de ciertos riesgos que nadie está dispuesto a tomar.

La falta de decisión política, motivada en parte por la ignorancia respecto al tema, implica asimismo la ausencia de un plan estratégico cuyo objetivo sea la promoción y el desarrollo de las tecnologías de la información y el conocimiento en la comunidad.

Por su parte, la falta de experiencias exitosas difundidas y conocidas tampoco ayuda a impulsar estos proyectos. En muchos casos, el software libre comienza a usarse en una administración simplemente porque el coste de adquisición es más bajo, y hasta a veces nulo. Es habitual en estos casos que el producto en cuestión se incorpore al sistema informático sin mayor planificación, y en general sin una estrategia global de uso y aprovechamiento de software libre, lo cual puede importar altos costos de transición, haciendo que experiencias aisladas de uso de software libre en la administración puedan resultar fallidas y frustrantes.

Finalmente, la implantación de software libre en cualquier organización puede chocar con la falta de alternativas libres de calidad adecuada para cierto tipo de aplicaciones. En esos casos, el estado puede esperar que aparezca el producto requerido, o bien puede tratar de promover la aparición del producto libre que se necesita.

Afortunadamente, los funcionarios públicos lentamente están empezando a interesarse en el tema y advertir las cualidades del software libre, lo cual les permite analizar seriamente si conviene fomentar, o incluso financiar o cofinanciar el desarrollo de esta clase de productos⁵, lo cual puede realizarse mediante acuerdos con las universidades creando las condiciones de desarrollo necesarias.

⁴ Los siguientes obstáculos han sido desarrollados en el estudio realizado en el libro *Introducción al Software Libre*, de Jesús González Barahona, Joaquín Seoane Pascual y Gregorio Robles, Fundació per a la Universitat Oberta de Catalunya.

⁵ A tales efectos resulta importante recordar que sus fines deben contemplar que sus administrados puedan acceder mejor a la sociedad de la información, así como también el fomento del tejido industria local.

Sin duda, la creación y difusión de muchos programas libres incidirá positivamente en el desarrollo de una industria de software local y en el fomento de la sociedad de la información.

El Software Legal en la Administración Pública

En Colombia existen dos Directivas Presidenciales que establecen un concepto que se ha venido utilizando, que se denomina "software legal".

La primera directiva, es del 25 de Febrero de 1999, cuyo asunto es: "respeto al derecho de autor y a los derechos conexos", y la segunda es del 12 de Febrero del 2002, que "instruye a las personas encargadas en cada entidad de la adquisición de software para que los programas de computador que se adquieran estén respaldados por los documentos de licenciamiento o transferencia de propiedad respectivos".

Una norma similar fue establecida en Perú (Decreto Supremo 013-2003-PCM: Decreto que dicta medidas para garantizar la legalidad del Software en el Estado).

Ambas normas tienen un espíritu en común, que el software a utilizar debe ser legal, y que manera mas clara de evitar la "*ilegalidad del no tener licencia*" es usar software libre, de hecho este es el camino que han seguido muchos organismos públicos para adecuarse a esta norma y de paso fomentar el uso de software libre.

Siendo esto entendible en el marco de una política de respeto a la Propiedad Intelectual (de acuerdo a los tratados internacionales, y hasta que no se retiren los países de dichos tratados, son normas vigentes), es un camino altamente recomendable para el fomento e impulso de implementación del software libre en la administración pública de los países.

Conclusiones y Recomendaciones

La protección por el régimen de derecho de autor de los programas informáticos existe en la mayoría de los países y ha quedado armonizada en diversos tratados internacionales a tal efecto, y a menos que los países repudien dichos tratados, son normas vigentes y efectivas en los países de la región.

En virtud de las libertades que confieren, las licencias utilizadas para distribuir el software pueden clasificarse en "libres" y "propietarias", siendo la primera de ellas la única que permite al usuario ejecutar el programa en tantas computadoras como desee, estudiarlo, adaptarlo, distribuirlo, mejorarlo y publicarlo.

Como resultado de estas libertades, existe un importante movimiento a favor de la adquisición de software libre en los gobiernos latinoamericanos, sustentado en múltiples razones que se traducen inequívocamente en beneficios concretos, tal como se ha expresado en este reporte.

La mayoría de los proyectos mencionados, sin embargo, no han sido aprobados por una serie de motivos que escapan al marco del presente trabajo pero que intentamos resumir bien que sucintamente, teniendo sobre todo una problemática de corte constitucional, al expresarse la libertad de mercado así como la no intervención directa del gobierno/estado en dicho mercado, siendo que normas de “uso obligatorio” generarían una distorsión, mientras que normas de “fomento” tendrían mayor probabilidad de éxito.

Sin perjuicio de ello, y en mérito a lo expuesto, se advierte que el software libre proporciona a los estados de LAC, tanto en su faceta de consumidor como en su faceta de promotor, enormes beneficios, no sólo por el ahorro que su adquisición implica, sino también, y fundamentalmente, por su potencial como parte integrante de una estrategia nacional que procure fomentar la industria local y alcanzar una mejor gestión para con sus administrados mediante la economía de medios, eficiencia de procesos y eficacia de resultados.

Los marcos normativos no solo deben estar entendidos en la temática del software libre, sino también en el del fomento de la industria nacional de software, con beneficios tributarios para la exportación de bienes digitales; así como beneficios en el área de hardware que es donde se monta el software que se pueda crear.

Es importante señalar que la regulación tiene que ser armónica con las políticas nacionales y regionales en materia de Sociedad de la Información.

Lucha contra el SPAM

La estructura y desarrollo de los pueblos, las formas de gobierno y sus instituciones son resultado indispensible de sus raíces, cultura e historia.

Y son precisamente esas raíces, cultura y aunque corta, pero muy prolífica historia, las que distinguen a los pueblos de América Latina y que han determinado su desarrollo, estructura social, gobierno e instituciones.

La tecnología no puede ser y, de hecho no ha sido asumida, de la misma forma en todo el mundo, pues no obstante el nivel y contexto de desarrollo tecnológico y económico de cada país, esta no llegó para ser asimilada bajo un mismo contexto social, político o cultural.

Así el establecimiento de reglas y mecanismos que permitan su integración, adopción y principalmente su instrumentación, debe partir del principio de que dichas reglas y mecanismos, de ningún modo, deben atentar contra el desarrollo y estructura propia de cada pueblo.

La búsqueda de un contexto común de desenvolvimiento mundial mediante la creación de sistemas que permitan la interrelación de economías y sociedades a través de los medios tecnológicos debe considerar el ámbito particular de cada continente y de cada pueblo, no solo en cuanto a su desarrollo económico o científico, sino en cuanto a su estructura e instituciones, a su sociedad e idiosincrasia.

De modo que, los temas relevantes en el desarrollo de la Red, sus usos y sus medios, deben ser enfrentados partiendo de la base que el contexto de apreciación y estructura de organización en la adopción tecnológica varía en cada continente y cada país; por tanto, ni estructural, ni socialmente, nos es posible asumir la tecnología e instrumentar los sistemas de interacción internacional que deriven de ella, del mismo modo.

De este modo, la determinación de reglas y políticas comunes debe ser afrontada con una visión amplia, a fin de que las formas creadas resulten elementos maleables que sin perder su propiedad de conducir a objetivos comunes, puedan ser instrumentadas conforme a las formas y estructuras de cada estado, a fin de que sean efectivamente aplicables y ejecutables y, no constituyan una visión utópica sobre el desarrollo e interacción de los pueblos a través de la Red o, peor aún, elementos de discriminación y verdaderos obstáculos para el desarrollo de los pueblos.

Partiendo de lo antes dicho, que aplica por igual a todos los temas, ya dentro del tema del Spam conviene establecer como principios de acción y de análisis del tema las consideraciones siguientes:

1. Es innegable la necesidad de la acción latinoamericana en la adopción de políticas y mecanismos de combate al Spam a nivel nacional e internacional; ya que su incidencia

comienza a generar serias consecuencias dentro del marco del uso y confianza en las comunicaciones electrónicas, operación de las redes de telecomunicaciones y el comercio electrónico.

2. Debe considerarse dentro del tema del Spam el daño e implicaciones que dicha conducta tiene sobre las RPT's y el sector de las telecomunicaciones.

3. Las acciones identificadas hasta ahora en el combate al Spam han sido dirigidas en dos ámbitos, el legislativo, sea a través de la aplicación de leyes específicas o reformas legislativas y; a nivel regulatorio, sea por autoaplicación o por disposición regulatoria expresa; ante lo cual valga desde ahora establecer que en el contexto del combate mundial al Spam la emisión de leyes específicas antispam ha demostrado no ser la clave, más aún, si esta no va acompañada de un paquete de acciones que involucren por igual al gobierno, industria y usuario en la promoción del uso correcto del correo electrónico, medidas autoregulatorias y educación al usuario.

4. La experiencia internacional advierte que el establecimiento de leyes específicas no garantiza la eficacia en el control del Spam. En realidad, el análisis del tema, especialmente en el contexto latinoamericano, de economías en desarrollo, con limitados recursos, ha llevado a advertir que las implicaciones del Spam tocan materias ya reguladas, que quizá implican más la necesidad de incluir los conceptos relativos a esta práctica nociva en el contexto de las leyes existentes, proveyendo de eficacia y dirección a las leyes y entidades existentes, que mediante la creación de disposiciones y entidades específicas que indirectamente generan mayores cargas administrativas y uso de recursos al país, con que en ocasiones no se cuenta, dando origen a leyes aplicables pero no ejecutables.

5. Desde una perspectiva de control legislativo el abordar el tema del Spam desde un ámbito de protección a la privacidad y protección de datos personales, tal como ha ocurrido en gran parte de Latinoamérica, no es del todo errado, ya que la emisión de Spam implica en principio, necesariamente la posibilidad de utilizar de forma libre los datos de terceros.

6. El combate al Spam no solo tiene que ver con una violación a la privacidad o el respeto al derecho de los consumidores, sino además tiene vinculación con la protección al uso eficiente de los recursos de las redes públicas de telecomunicaciones y a la prestación de servicios de telecomunicaciones de calidad.

7. En todo caso, el combate al Spam requiere hacer partícipes a todos los sectores implicados o afectados por dicha práctica, debiendo cada uno asumir su responsabilidad en el establecimiento y aplicación de acciones para su combate.

8. En cuanto a la creación o reforma legislativa en materia de Spam se requiere la determinación clara del bien jurídico a tutelar, a fin de lograr real eficacia en su aplicación, en principio ejerciendo un equilibrio entre los derechos de libre expresión, ejercicio libre del comercio, protección a la privacidad, protección a los consumidores y potenciales consumidores; evitando una competencia desigual entre derechos.

9. Debe abrirse el abánico de aplicación legislativa y regulatoria a toda la gama tecnológica que permite esta práctica nociva, sin limitar su aplicación solo al uso del correo electrónico, considerando las posibilidades del futuro tecnológico e incluso a la totalidad de medios de comunicación en que ya se presenta dicha conducta nociva y que por igual vulneran los derechos de los usuarios, como consumidores de servicios de telecomunicaciones; por ello, el uso del término de “*comunicaciones electrónicas*” en lugar de correo electrónico resulta más idóneo.

10. En caso de una adopción legislativa específica esta debe instrumentar conceptos definidos y más o menos acordes al consenso internacional de lo que es e implica el spam, de lo que significa un correo comercial, un correo no solicitado o no autorizado, evitando usar términos subjetivos, tales como “indeseado”, que no promueve la claridad y certeza en la interpretación de las disposiciones legales y en consecuencia limita su efectividad.

11. De igual modo, debe delimitarse el concepto de solicitud, identificando si se refiere a una autorización expresa por escrito o verbal, o simplemente a que no sea rechazada una vez que se recibió o a que no incluya elementos que identifiquen el mensaje electrónico como de carácter ilegal.

12. En la identificación y diferenciación de Spam legal e ilegal, es importante analizar que una misma conducta no puede implicar una doble apreciación de legalidad con base en una autorización *a posteriori* a su emisión y recepción. Por ello, la diferenciación debe ir más en el sentido de determinar como Spam a la conducta nociva en sí misma de enviar mensajes no autorizados, no solicitados o no esperados, conceptuando el resto como mensajes publicitarios, autorizados por alguna de las vías determinadas para ello.

13. El aspecto ilícito y, en su caso, delictivo de un mensaje electrónico no corresponde a la acción misma del envío, sino a los fines, objetivos y contenido bajo el cual se da la conducta del envío.

14. La instrumentación legislativa de medios de protección y resarcimiento económico del daño debe dirigirse en primera instancia a los usuarios, a quienes los diversos actores en el tema coinciden en señalar como los principales afectados por esta práctica, no solo en un contexto de potenciales consumidores de bienes y servicios, sino como consumidores de por sí de un servicio de telecomunicaciones; expandiendo en segundo término dicha protección a los prestadores de servicios de Internet, asumiendo que un elemento propio del Spam, es el nulo costo que implica a su emisor su envío.

15. Los proveedores del servicio tienen la responsabilidad de cooperar y establecer medios técnicos en el combate al Spam, así como el Estado de construir el ámbito regulatorio ideal a efecto de que las políticas antispam y la seguridad proporcionada por los prestadores de servicio de Internet sea un elemento de competencia entre ellos, ya sea estableciendo un nivel mínimo de seguridad exigible o, de manera genérica, capacitando en la forma de elección del

prestador de servicios adecuado bajo el contexto de que establezcan políticas de seguridad claras.

16. La determinación de responsabilidades en la emisión de Spam debe ser cuidadosa en considerar la diversidad de prácticas y objetivos bajo los cuales se genera el Spam, no contemplando solo el de carácter comercial y dando consideración al hecho de que un emisor sin consentimiento puede enviar correos electrónicos a nombre de un tercero, generándole responsabilidad por conductas en las que no participó, si bien pudiera conceptuarse como beneficiario.

17. En el análisis de las implicaciones que tiene el Spam, se debe hacer referencia a los daños por transmisión de virus ligados al Spam, por el sobrefiltrado, en la infraestructura y servicios de telecomunicaciones, así como contemplar el que los costos generados a la industria terminan por ser trasladados a los usuarios lo que concluye en servicios de telecomunicaciones más caros.

18. Con relación al rubro de modelos legislativos en su combate, conviene señalar las ineficacias que conlleva el uso del opt-out, cuando ante la posibilidad de uso y recolección libre de datos, dicho mecanismo es aplicado por los spammers para asegurar la existencia de una dirección electrónica.

19. En la implementación de mecanismos de control, tales como el etiquetado de “*publicidad*” a los mensajes no solicitados con dicho tipo de contenido, es imprescindible considerar que el problema del Spam es que no todo es de contenido publicitario de tal forma que aquellos que no incluyen dicho tipo de contenido no estarían obligados al etiquetado, pero no por ello se termina con el problema de recibir Spam, porque bajo un rubro diverso por igual pueden engañarme como usuario y lograr que lo abra con lo cual el problema continua, de modo que lo que debe atacarse es el problema de raíz que es el uso indebido y no autorizado, así como la recolección de direcciones electrónicas y, en general, los datos personales.

20. El etiquetado facilita la identificación del Spam, no obstante no combate las implicaciones del problema y mucho menos el problema de manera directa. Esto es, el etiquetado no limita que el hecho de recibir miles de correos Spam obstaculice el uso de mi capacidad de correo y, con ello, se pierdan correos efectivamente solicitados y deseados, así como en esa medida se socave la confianza en las transacciones y comunicaciones electrónicas.

21. Abundando en el tema de la responsabilidad, la responsabilidad no debe ser de los usuarios, pero tampoco de los ISPs, ya que estos no pueden ser responsables por el contenido de los mensajes que transmiten, por tanto, ni en un caso, ni en el otro conviene establecer legislativamente una liberación o por igual determinación de responsabilidad a cargo de unos u otros. De modo que, así como se evidencia la necesaria cooperación multisectorial en su combate, por igual se hace patente la necesidad de distribuir la responsabilidad en todos los actores.

22. Dentro del Análisis del costo-beneficio del Spam es imprescindible catalogar como punto primordial de la discusión y combate el hecho de que el Spam existe porque constituye un negocio, esto es genera grandes utilidades a sus emisores.

23. Dentro de los mecanismos regulatorios, se debe cuidar que el opt-out no se convierta en una carga para el receptor, esto es, que ahora deba por cada mensaje comercial recibido tener que solicitar no ser receptor del Spam.

Sobre Delitos Informáticos

1. Análisis del estado actual en la región.

Encontramos en la región una preocupante y generalizada falta de legislación en materia de delitos informáticos. Ésta empieza por la misma falta de definición de los bienes jurídicos que deben ser protegidos en la realidad tecnológica en la que estamos inmersos desde hace ya varios años.

Así, por ejemplo, sólo ocasionalmente se protege la información por su valor intrínseco, siendo más frecuente que sea protegida como un anexo de la libertad personal, de la intimidad y de la propiedad intelectual. Para agravar la situación, en los casos en los que se han tipificado delitos informáticos, las definiciones legales han incurrido en errores técnicos y definido penas irrisorias.

Si bien es cierto que en las definiciones de los delitos tradicionales es posible encuadrar uno informático, dada su propia naturaleza, también es cierto que para obtener de un funcionario judicial una decisión de fondo que extienda el sentido de un tipo penal tradicional hacia una conducta nueva para él, respecto de la que tiene muy poco conocimiento y de la que muy seguramente no comprende su funcionamiento técnico, se requiere de una ardua labor de convencimiento. Adicionalmente, en pocos países de la región existen cuerpos policiales especializados en delitos informáticos y los pocos existentes no cuentan ni con suficiente personal capacitado, ni con la tecnología de la que deberían disponer para ser eficientes y efectivos en su labor.

Un punto que debe necesariamente tenerse en cuenta, es la naturaleza transnacional de esta clase de delitos, que exige de una legislación uniforme, de convenios de cooperación judicial e investigativa y de la existencia de cuerpos de seguridad efectivos.

Actualmente, a conductas como las descritas a continuación no se sigue como consecuencia la imposición de una sanción; usualmente, ni siquiera se sigue de ellas una investigación judicial o prejudicial:

- El acceso no autorizado a un sistema informático.
- La lectura, modificación, copia, eliminación o publicación de datos guardados o administrados en un sistema informático, sin autorización.
- La interceptación no autorizada de comunicaciones electrónicas, v. g., el contenido de conversaciones en línea a través de salas de conversación, del uso de programas de mensajería instantánea y la captura no autorizada de mensajes de correo electrónico y los documentos adjuntos a ellos, entre otros.
- La modificación no autorizada de los contenidos de sitios web.
- Las estafas cometidas a través de técnicas como el *nigerian scam* y el *phising*.
- La instalación y el uso no autorizados, en sistemas informáticos ajenos, de herramientas o aplicaciones de software que permitan, a quien las ha instalado y las usa, atacar a un tercer sistema informático.

- La utilización no autorizada de herramientas de escaneo de redes y vulnerabilidades en contra de sistemas informáticos ajenos.
- El uso de técnicas de anonimización durante la comisión, o la tentativa de comisión, de un delito (IP spoofing, uso de servidores proxies gratuitos y de servidores espejos, etc.).
- El uso de herramientas de cifrado con fines delictivos.

Propuesta⁶: uniformización sustancial y procesal de las legislaciones penales nacionales, mediante la suscripción y la ratificación de la Convención Europea sobre Ciberdelitos.

A la hora de analizar las necesidades que sobre este extenso asunto deben ser hoy satisfechas en nuestros países, debemos tener en cuenta los siguientes aspectos:

1. Es necesario proteger a la sociedad frente a la amenaza de los delitos cometidos por vías informáticas.
2. Debe buscarse la promulgación de leyes uniformes en todos los países.
3. Los procesos y procedimientos forenses digitales deben estandarizarse, al igual que las características de las herramientas usadas por los investigadores, de manera que la evidencia recaudada en un país sea válida en cualquiera otro.
4. La naturaleza volátil de estos delitos hace necesaria la adopción de mecanismos de cooperación nacional e internacional expeditos y funcionales.
5. Es necesario garantizar a la sociedad la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos y de la información archivada y/o administrada en ellos.
6. Debe existir un balance entre los poderes investigativos del Estado y los derechos humanos.
7. Es necesario crear, capacitar y dotar de tecnología a organismos especializados estatales de seguridad.
8. Es necesaria la participación activa de nuestros países en actividades de I+D, de manera que ellos mismos estén en capacidad de detectar vulnerabilidades, generar las soluciones correspondientes y generar sus propias herramientas, técnicas y estrategias de investigación.

Teniendo en cuenta todos estos puntos, es necesario proponer la adopción de regulaciones uniformes en lo penal, que abarquen tanto los aspectos sustantivos como los procesales. Así, al abordar los aspectos sustantivos serán definidas como delitos, en todos los países, las actividades que sean consideradas dañinas; y, al referirse a los temas procesales, se dará cabida a la investigación y al castigo efectivos de delitos tradicionales en cuya comisión hubo utilización de sistemas de información y comunicaciones.

⁶ Los fundamentos de nuestra propuesta se encuentran en la Convención Europea sobre Ciberdelitos y en la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones: creación de una Sociedad de la Información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos.

El Convenio del Consejo de Europa ha definido cuatro categorías de delitos informáticos (entendidos en su más amplia acepción, es decir, cualquier delito en cuya comisión haya intervenido el uso de las tecnologías de la información y las comunicaciones), así: 1) delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y datos informáticos; 2) delitos estrictamente informáticos; 3) delitos relativos al contenido; y, 4) delitos relativos a la violación de los derechos de autor y derechos afines. La Unión Europea ha dado prioridad, en cuanto se refiere a estos aspectos sustanciales, a la pornografía infantil, la piratería, la denegación de servicios, la xenofobia y a temas relacionados con las drogas ilegales.

En cuanto a aspectos procesales, las regulaciones nacionales deben salvar la dificultad planteada por la naturaleza transnacional de estos delitos, junto con sus velocidades de comisión y la flexibilidad que les es propia. Entre estos aspectos los países deben necesariamente tener en cuenta la interceptación de comunicaciones, la retención de datos sobre tráfico, la anonimización, la cooperación internacional, la jurisdicción y el valor probatorio de la evidencia digital.

Ahora bien, conseguir que todos los países de la región lleguen a un consenso, en la redacción de sus normas penales sobre delitos informáticos y en la creación de sus unidades policiales especializadas en estos temas, es una tarea muy difícil cuyo resultado no se puede garantizar. Al respecto, encontramos las siguientes dificultades concretas:

1. El desinterés de los países por uniformizar su ley y la imposibilidad de exigir, por cualquier vía, que lo hagan efectivamente.
2. La posibilidad de deserción parcial de algunos países, queriendo decir con esto que es posible que, en temas puntuales, algunos países definan sus leyes en forma diferente a la estandarizada, fundamentando su disidencia en intereses locales (que bien pueden no corresponder al interés de sus propios pueblos).
3. La inclusión de aspectos técnicos erróneos en las leyes nacionales, que les harían perder toda su efectividad.
4. La no definición legal uniforme de los aspectos relacionados con el valor probatorio de la evidencia digital, que haría imposible la aceptación de la evidencia recaudada en un país, por parte de un juez extranjero.

Y, puesto que, como está dicho, no existe una instancia que obligue a los países a uniformizar sus leyes, proponemos que todos ellos suscriban y ratifiquen la Convención Europea sobre Cibercrimen. Esta propuesta es consecuente con la invitación que los Ministros de Justicia de la Organización de Estados Americanos presentaron a los Miembros en abril de 2004 “a evaluar las posibilidades de implementar los principios de la Convención del Consejo de Europa sobre Cibercrimen de 2001 y a considerar la posibilidad de ser Parte en esa Convención”.

La incorporación global a la Convención será la posición que a este respecto asumirán los 46 países miembros del Consejo de Europa, dentro del marco del WSIS. Esta Convención ha

sido, a la fecha, ratificada por nueve Estados y suscrita por 32; se espera que muchos Estados, incluyendo obviamente no europeos, se conviertan en Parte en ella.

En cuanto a los aspectos prácticos relativos a la forma a través de la cual un Estado puede acceder a ella⁷, se tiene que debe simplemente contactar al Secretariado del Consejo de Europa (Oficina del Consejo del Tratado de Europa o al Departamento de Asuntos Criminales⁸). Una vez presentada la petición, el Secretariado del Consejo de Europa traslada el asunto al Comité de Ministros del Consejo de Europa, que es el órgano responsable de extender, formalmente, la invitación a ser parte de la Convención.

Una vez un Estado no miembro de la Unión Europea se convierte en Parte en la Convención, recibe el derecho de participar en el *Consultation of the Parties* previsto en su artículo 46, en igualdad de condiciones frente a los miembros de la Unión y en el mecanismo de *follow up* de la Convención.

⁷ Según información que nos fuera proveída para el efecto por el *Head of the Economic Crime Section, Department of Crime Problems, Council of Europe*.

⁸ *Secretariat of the Council of Europe (Council of Europe Treaty Office o el Department of crime Problems)*.

Aspectos de Derechos de Autor en el entorno digital.

El entorno digital y la capacidad de explotación de obras del ingenio no ha pasado por desapercibido en los organismos internacionales, teniendo plena conciencia de la necesidad de una adecuada protección de los derechos intelectuales ante el avance tecnológico en el campo de la informática y de las telecomunicaciones interactivas.

Así se llegó a la aprobación, en el año 1996, de dos nuevos tratados de vocación Universal: el Tratado de la OMPI sobre Derecho de Autor (TODA en castellano y WCT en inglés, en lo adelante TODA/WCT) y el Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas (TOIEF en castellano y WPPT en inglés, en lo adelante TOIEF/WPPT).

Es así como diversas naciones han evolucionado sus sistemas legislativos en la materia para adaptarlos a los instrumentos internacionales ya mencionados y a las modernas tecnologías, bien sea a través de reformas o de actualizaciones, entre ellos: Australia, Croacia, Emiratos Árabes Unidos, España, Francia, Hungría, Japón, Nueva Zelanda, Polonia, Rumania, y Tanzania.

Nada distinto ha ocurrido en América Latina, en donde podemos mencionar a Brasil, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Paraguay, Perú y República Dominicana.

Todo lo anterior resalta la necesidad de normas acordes con los estándares internacionales, que adapten las legislaciones internas a los modernos adelantos tecnológicos, para una adecuada protección a los creadores y demás titulares de derechos intelectuales.

El “*entorno digital*” y el advenimiento de la “*sociedad de la información*” plantea nuevos retos, particularmente en relación con el almacenamiento electrónico, las comunicaciones digitales interactivas, la responsabilidad de los proveedores en los servicios de transmisiones digitales y las nuevas modalidades delictivas, fenómenos todos de reciente aparición que aconsejan la introducción de nuevas normas e instituciones que se adecuen a la realidad tecnológica contemporánea.

A los efectos de dar cumplimiento al compromiso contenido en el artículo 11 del TODA/WCT, deberá estipularse la facultad del titular del derecho patrimonial de aplicar o de exigir que se apliquen mecanismos, sistemas o dispositivos de autotutela, incluyendo la codificación de señales u otros medios de protección tangibles o intangibles, con el fin de prevenir o impedir la comunicación, recepción, retransmisión, reproducción o modificación no autorizadas de la obra, y ese mismo derecho, para cumplir las obligaciones asumidas con la ratificación del TOIEF/WPPT (art. 18), se debe incorporar también en relación con los derechos conexos.

Este derecho, como lo comenta la doctrina al analizar el TODA/WCT, obedece a que:

“... las nuevas realidades tecnológicas han demostrado que no basta con el reconocimiento de derechos a los autores (y a los titulares de derechos conexos), ante las inmensas posibilidades de infracción que abren las redes internacionales de la comunicación, como en el caso de Internet, lo que obliga entonces a dichos titulares a instrumentar mecanismos técnicos de «autotutela» dirigidos a impedir, por ejemplo, las reproducciones o transmisiones no autorizadas”⁹.

La incorporación del derecho a instrumentar dispositivos técnicos de autotutela (a veces en forma de tipificación como delito de diversos actos destinados a su desactivación), ya es una realidad en las leyes recientes que han adaptado su contenido a los nuevos Tratados de la OMPI (TODA/WCT y TOIEF/WPPT), tal el caso de la “*Digital Millenium Copyright Act*” de los Estados Unidos y las leyes de derecho de autor de Andorra, Australia, Bielorrusia, Bosnia y Herzegovina, Brunei Darussalam, Bulgaria, Camboya, China, Emiratos Árabes Unidos, Japón, Marruecos, Moldova, Namibia, Nueva Zelanda, Palau, Papua Nueva Guinea, Qatar, Serbia-Montenegro y Tanzania.

Lo mismo ha ocurrido con las últimas reformas o actualizaciones aprobadas en varios países de América Latina y el Caribe (Antigua y Barbuda, Brasil, Dominica, Ecuador, México, Nicaragua, Paraguay, Perú, República Dominicana, Trinidad y Tobago, Uruguay), y en todos los países de la Unión Europea, por mandato de la Directiva 2001/29/CE sobre la armonización del derecho de autor y los derechos afines en la sociedad de la información, cuyo considerando 47 señala que la “*resulta necesario establecer una protección jurídica armonizada frente a la elusión de medidas tecnológicas efectivas y frente al suministro de dispositivos y productos o servicios para tal fin*”.

Se debe plantear la necesidad de introducir el reconocimiento a los derechos de remuneración compensatoria y equitativa por la copia para uso personal de reproducciones reprográficas y de grabaciones sonoras y audiovisuales.

Tales derechos de remuneración obedecen a que, en el pasado, las legislaciones autorales legitimaron, sin autorización del autor ni pago de remuneración, las reproducciones realizadas con fines personales o para uso privado, porque se consideraba que tales utilidades, en los términos del artículo 9,2 del Convenio de Berna, no atentaban contra la explotación normal de la obra ni causaban un perjuicio injustificado a los intereses patrimoniales del autor.

Sin embargo, la popularización de los artefactos que facilitan la copia de los ejemplares gráficos, sonoros o audiovisuales de la obra (lo que se ha incrementado con las nuevas tecnologías y muy especialmente con la digital), ha generado tal número de reproducciones - las cuales desalientan la adquisición de un ejemplar original y desestimulan las inversiones

⁹ ANTEQUERA PARILLI, Ricardo: “*El nuevo Tratado de la OMPI sobre Derecho de Autor*” (WCT, 1996), en Actas de Derecho Industrial y Derecho de Autor. Ed. Instituto de Derecho Industrial. Universidad de Santiago (España). Tomo XVIII. 1997. p. 69.

por parte de los sectores perjudicados- que, como lo afirma la doctrina, no pueden seguir siendo gratuitas ¹⁰, pues se trata de una disociación de acciones “*inocentes*” que en su conjunto producen efectos devastadores ¹¹.

Tal remuneración deberá determinarse en función de los equipos, aparatos y materiales idóneos para realizar dicha reproducción y se causará por el hecho de la fabricación en el territorio del país respectivo o su importación de:

- Las cintas u otros soportes materiales susceptibles de incorporar una fijación sonora, visual o audiovisual.
- Los soportes digitales susceptibles de incorporar obras literarias.
- Los equipos reproductores no tipográficos, de obras divulgadas en forma de publicaciones, así como de fonogramas, videogramas u otros soportes sonoros, visuales o audiovisuales.

Como resulta una constante en todos los países que han consagrado este derecho de simple remuneración, su recaudación debe encomendarse a una entidad de gestión colectiva, quien debe efectuar la distribución de esa remuneración en las proporciones que se indiquen en el texto legislativo correspondiente.

Siendo ilícita cualquier acción destinada a eludir la comentada remuneración equitativa, se debe disponer que los afectados puedan acudir a la vía judicial para intentar las acciones civiles y penales que correspondan y de obtener las medidas cautelares necesarias para prevenir la infracción o que la misma se continúe cometiendo.

De más está decir que la remuneración compensatoria por la copia privada para uso personal no puede entenderse como que legitima aquellas reproducciones destinadas a usos colectivos o que se ponen a disposición del público con fines lucrativos, casos en los cuales se está en presencia de un acto de “*piratería*”, sancionado penalmente, como lo establece en forma obligatoria el Acuerdo sobre los ADPIC (art. 61).

También dentro de la llamada “*sociedad de la información*”, se debe apuntar que tal sociedad utiliza como medios tecnológicos las llamadas “*superautopistas de la información*”, que requieren de varios “*proveedores*”, es decir, las personas naturales o jurídicas que prestan un servicio en la sociedad de la información, para transmitir datos en una red de comunicaciones o que facilitan el acceso a una red de comunicaciones.

Como resulta que con la participación de tales prestadores se hace posible la transmisión y recepción de elementos protegidos por las leyes (y no sólo los tutelados por el derecho de autor y los derechos conexos u otros derechos intelectuales), es necesario establecer las responsabilidades que corresponden a cada uno de ellos cuando se infringen los derechos que

¹⁰ LIPSZYC, Delia: “*La protección de las obras literarias y la política cultural del libro*”, en Memorias del IV Congreso Internacional sobre la protección de los Derechos Intelectuales. Ciudad de Guatemala, 1989. pp. 19-47.

¹¹ VILLALBA, Carlos: “*Fundamentación de la copia privada como límite al derecho de autor. Justificación de la remuneración por copia privada*”, en Memorias del I Congreso Iberoamericano de Propiedad Intelectual. Madrid, 1991. Tomo II. p. 593.

corresponden a los autores, intérpretes o ejecutantes, productores fonográficos, organismos de radiodifusión y otros titulares de derechos.

Por todo lo indicado, debe partirse de las disposiciones del derecho común relativas a la responsabilidad por hecho ilícito, cuando el uso indebido de las mencionadas prestaciones intelectuales protegidas se realiza con intención, imprudencia, negligencia o impericia, pues como lo ha apuntado la jurisprudencia en América Latina, los problemas originados en la red, a falta de una normativa expresa, pueden ser resueltos conforme a las reglas generales sobre responsabilidad civil y penal, pues *“en un sitio web pueden publicarse y divulgarse contenidos ilícitos o nocivos, sean mensajes, avisos o bienes protegidos por propiedad intelectual que no cuentan con autorización ... o incluso ser contrarios a la ley, al orden público, a la seguridad nacional o a la moral o a las buenas costumbres”*¹².

Pero como se destaca en varios considerandos de la Directiva de la Comunidad Europea 2000/31/CE, la misma complejidad del sistema exige establecer reglas claras acerca de las responsabilidades que recaen, o pueden recaer, sobre los diferentes proveedores de la sociedad de la información, de acuerdo a su participación en la prestación del servicio, de modo que las exenciones sólo se apliquen a aquellos que se limiten al proceso técnico, automático y pasivo de facilitar el acceso a una red de comunicación mediante la cual la información facilitada por terceros es transmitida o almacenada temporalmente, siempre que dicho prestador no tenga conocimiento ni control de la información así transmitida o almacenada y, en consecuencia, si ese prestador colabora deliberadamente con la comisión de actos ilícitos, su conducta rebasa la de un mero transporte o la de un simple almacenamiento automático, provisional y temporal.

Una legislación específica sobre el derecho de autor y los derechos conexos sólo podrá regular la responsabilidad de los prestadores de servicios en la sociedad de la información cuando los contenidos que circulan están protegidos por esa ley especial, de modo que si dichos elementos se relacionan con otros bienes jurídicos (por ejemplo, la intimidad o el honor y reputación de las personas, los datos confidenciales, la salud pública, la moral o las buenas costumbres) tales responsabilidades, civiles o penales, deberían estar determinadas en las respectivas leyes especiales o, en su defecto, por la normativa del derecho común.

De allí la necesidad de que cualquier regulación en este sentido se encabece con un dispositivo general, por el cual se aclare que *“sin perjuicio de las responsabilidades civiles, penales o administrativas que correspondan de acuerdo al derecho común y a otras leyes especiales”*, los proveedores de servicios son responsables por sus actos relacionados con las obras y demás prestaciones protegidas por el Derecho de Autor.

Las mismas dificultades prácticas para las autoridades competentes, los titulares de derechos y los usuarios por lo que se refiere a la tarea de ubicar a los distintos prestadores de servicios en las redes digitales y, en su caso, determinar las responsabilidades que les pueda corresponder en razón de su intervención en la transmisión de contenidos protegidos, impone

¹² Sentencia dictada por la Corte de Apelaciones de Concepción, Chile, el 6-12-1999, Rol 249/99. Extracto en <http://www.cerlalc.org/jurisprudencia/index.php>

la necesidad de establecer una obligación para dichos proveedores de suministrar suficiente información que permita su localización, en norma que se incorpora a esta propuesta y que se inspira en la Directiva Europea 2000/31/CE, en cuanto a las obligaciones de los prestadores de servicios en la sociedad de la información.

Como una obligación que debería imponerse a todos los proveedores de servicios, se debe comunicar con prontitud a las autoridades judiciales o administrativas competentes, al tener conocimiento de ello, de los presuntos datos ilícitos o las actividades no autorizadas por los titulares de derechos que se lleven a cabo por destinatarios de sus servicios y también la de suministrar a dichas autoridades, a solicitud de éstas, cualquier información que permita identificar a los destinatarios de tales servicios con los que hayan celebrado acuerdos de almacenamiento, ello en base a las disposiciones contenidas en el mencionado instrumento comunitario europeo.

Con respecto al derecho patrimonial de distribución (llamado también “*de puesta en circulación*” de los ejemplares), se propone que se establezca como un derecho distinto al derecho de reproducción y se que se agregue entre las modalidades que lo conforman al préstamo público, pues una cosa es el préstamo de ejemplares entre particulares, lo que resulta lícito; y otra aquel donde se ponen los ejemplares a disposición del público, lo que concurre con los “*usos honrados*” pues atenta contra la explotación normal de la obra y, en consecuencia, causa un perjuicio injustificado a los intereses patrimoniales del autor.

En cuanto al derecho patrimonial de distribución y su alcance en el entorno digital, se ha dicho que como en la transmisión digital el almacenamiento electrónico de las obras u otras prestaciones, aunque sea temporal, en el computador del usuario que ha accedido a las mismas a través de Internet, constituye una reproducción, quiere decir entonces que hay en ese computador “*un ejemplar más*” y, en consecuencia, la “*puesta a disposición*” a través de la red constituye, además, un acto de distribución, dado que en cada uno de los computadores de los usuarios se ha almacenado un ejemplar.

Así lo consideró la jurisprudencia en los Estados Unidos, en diversos casos donde la transmisión de obras por Internet fue considerado un acto no autorizado de “*distribución por transmisión*”.

El asunto fue muy debatido en los comités de expertos que antecedieron a los nuevos Tratados de la OMPI, en cuya Conferencia Diplomática se aprobó una “*Declaración Concertada*”, que en el texto del WCT y en relación con el derecho de distribución reza así: “*... las expresiones «copias» y «originales y copias» sujetas al derecho de distribución y al derecho de alquiler en virtud de dichos Artículos, se refieren exclusivamente a las copias fijadas que se pueden poner en circulación como objetos tangibles*”.

Lo anterior quiere decir que, a título de “*protección mínima*” en base al WCT, el derecho de distribución no comprende a las transmisiones de “*intangibles*”, como ocurre en las comunicaciones “*on line*”, pero nada se interpone para que las leyes internas de los países u

otros instrumentos legales reconozcan, por encima de esa “*protección mínima*”, un derecho de “*distribución por transmisión*”.

Finalmente, en concordancia y en armonía con lo señalado en el artículo 8.2 de los ADPIC, debe considerarse la implementación de medidas efectivas y eficaces que prevengan el ejercicio de forma abusiva de los derechos intelectuales, tales como el establecimiento de mecanismos alternativos de soluciones de controversias cuando existan diferencias en el establecimiento de tarifas para la explotación de obras.

Sobre la Internacionalización del Ciberespacio

Basados en la propuesta del GIC¹³, grupo liderado por James Graham y Erick Iriarte, Alfa-Redi propone la adopción de la propuesta expresada por el Grupo en sus Declaraciones de Quito¹⁴, Monterrey¹⁵ y Lima¹⁶ en torno a la Internacionalización del Ciberespacio que explícitamente indica lo siguiente:

PREÁMBULO

El Grupo para la Internacionalización del Ciberespacio (GIC¹⁷), patrocinado por la Facultad Libre de Derecho de Monterrey (México)¹⁸ y bajo el auspicio de la Alfa-Redi¹⁹, fue establecido como espacio de propuesta de un marco político internacional para la Sociedad de la Información.

El GIC ha expresado sus posiciones mediante las resoluciones de Quito²⁰, Monterrey²¹, y Lima²².

Tomando en consideración los documentos producidos por la primera fase de la *Cumbre Mundial de la Sociedad de la Información (CMSI)*²³, realizada en Ginebra en el 2003, y con vistas a la declaración que se producirá en Tunez, al culminar la segunda fase de la CMSI.

Adopta la siguiente posición:

Reafirma que el Internet es un nuevo espacio, sea desde el punto de vista sociológico, económico y jurídico – un espacio conocido por sus usuarios como el “Ciberespacio”;

Insiste en que la regulación del Ciberespacio debe ser hecha con una activa participación de todos los sectores que le componen, como se le ha afirmado en la *Resolución 56/183 de la Asamblea General de las Naciones Unidas*²⁴, y subrayado por la “*Declaración de las Organizaciones de las Sociedad Civil presentes y firmantes en la Conferencia Ministerial Regional para América Latina y el Caribe para la Cumbre Mundial sobre la Sociedad de la Información*”²⁵

¹³ <http://www.alfa-redi.org/gic>

¹⁴ <http://www.alfa-redi.org/gic/quito.asp>

¹⁵ <http://www.alfa-redi.org/gic/monterrey.asp>

¹⁶ <http://www.alfa-redi.org/gic/lima-es.asp>

¹⁷ <http://www.alfa-redi.org/gic>

¹⁸ <http://www.fldm.edu.mx/>

¹⁹ <http://www.alfa-redi.org>

²⁰ <http://www.alfa-redi.org/gic/quito.asp>

²¹ <http://www.alfa-redi.org/gic/monterrey.asp>

²² <http://www.alfa-redi.org/gic/lima-es.asp>

²³ <http://www.itu.int/wsis>

²⁴ http://www.itu.int/newsarchive/press_releases/2002/UNGA_res_56_183.html

²⁵ <http://www.alfa-redi.org/cisi/decla-ong-bavaro.doc>

Tomando en cuenta que la Declaración presentada en la *PrepCon de Latinoamérica en Bávaro*²⁶ (Santo Domingo) por *organizaciones de la sociedad civil del Perú*²⁷ donde se refieren expresamente a los principios del GIC;

Compartiendo la mencionada declaración con respecto a la exigencia de un acceso universal y democrático al Ciberespacio; dicho acceso resulta siendo un derecho humano fundamental para cualquier ciudadano en cualquier Estado;

Considerando que por su naturaleza, no es posible para cualquier Estado, solo o junto con otros, proclamar una soberanía sobre el Ciberespacio;

Teniendo conciencia que en el Ciberespacio existen distintas sociedades y que cada una podría tener sus propios códigos y regulación; que sin embargo, todas existen en el mismo espacio que tiene que tener una sola regulación marco;

Proclamando que esta regulación marco tiene que basarse en un consenso internacional;

Sabiendo que ya existe un sistema internacional que podría servir de modelo, a saber la gestión internacional del Alto Mar;

Considerando que como los demás espacios inapropiables, el Internet debe ser reconocido como un Nuevo espacio internacional y que su regulación tiene que ser hecha bajo el derecho internacional, como se ha afirmado en la *Declaración de Bávaro*²⁸, no obstante el falso supuesto de los Estados Unidos de Norteamérica. El marco podrá ser complementado, subsidiariamente, por la regulación local.;

Subrayando la necesidad de establecer a través de una Convención Internacional, tomando en consideración la soberanía de todos los Estados, un orden jurídico para el Ciberespacio que promueve el pacífico, equitativo y eficiente uso de todos sus recursos;

Insistiendo en que el cumplimiento de estos objetivos contribuirá a la realización de un justo y equitativo orden económico internacional que toma en cuenta los intereses y necesidades de la humanidad en su conjunto y, en particular, los intereses y necesidades especiales de los países en vía de desarrollo;

Tomando en cuenta que actualmente la brecha digital es una realidad, la internacionalización del Internet podría contribuir a conceder a los países tecnológicamente subdesarrollados un estatuto especial, dándoles así la oportunidad de superar su retraso con el ayuda de los demás países y asegurar a sus poblaciones un tratamiento igualitario y un acceso a la Sociedad de la Información y al Comercio electrónico, contribuyendo así a su bienestar económico general;

²⁶ <http://www.indotel.org.do/wsis/>

²⁷ http://www.alfa-redi.org/noticia/noticia_descripcion.asp?idNoticia=348

²⁸ http://www.indotel.org.do/wsis/Docs/f_declaration/declaracion_final_Bavaro.pdf

Considerando que el Ciberespacio solo puede ser reglamentado por una autoridad internacional, representando a todos los Estados y sus sociedades civiles; que una tal experiencia se inició con el ICANN, aún en fase de desarrollo, aunque ha tenido fracasos y éxitos en dicho proceso;

Estando preocupados que los Estados pueden suplantar a las sociedades civiles en la Cumbre mundial, invita el UIT y las Naciones Unidas a tomar en cuenta la legítima intervención de estas organizaciones;

Invita a todas las organizaciones de la Sociedad Civil a juntarse a la presente declaración, y; Proclamando los siguientes principios en cuales un futuro “Tratado sobre el Ciberespacio” podría basarse:

§ 1 – Espacio Internacional. Ningún Estado puede proclamar su soberanía sobre el Internet o unos de sus componentes.

§ 2 – Fines pacíficos. El Ciberespacio será utilizado exclusivamente con fines pacíficos.

§ 3 – Libertad de acceso a la tecnología. Ningún Estado u Organización internacional debe prohibir a través de medidas legislativas y/o medios tecnológicos a su población acceder al Internet.

§ 4 – Libertad de información. Ningún Estado u Organización internacional debe prohibir a través de medidas legislativas y/o medios tecnológicos a los individuos u organizaciones publicar información en el Internet. Ningún Estado u Organización internacional debe prohibir a través de medidas legislativas y/o medios tecnológicos a los individuos u organizaciones acceder a información en el Internet. Sin embargo, cualquier Estado u Organización internacional puede limitar el acceso a informaciones predeterminadas si tal necesidad existe en una sociedad democrática por el interés de la seguridad nacional, la seguridad pública o el bienestar económico del Estado, para la prevención de delitos, la protección de la salud, o para la protección de los derechos y libertades de los demás.

Asimismo debe establecerse como prioridad de los gobiernos el permitir a los ciudadanos el acceso a la información pública gubernamental como mecanismo de transparencia de la gestión pública y favoreciendo la participación ciudadana en la toma de decisiones.

§ 5 – Derechos Humanos. Todos los Estados deben garantizar en el Ciberespacio el respeto de los derechos humanos fundamentales declarados como tales en las convenciones internacionales.

§ 6 – Jurisdicción penal. Los Estados deben únicamente ejercer su jurisdicción penal de modo tal que el más mínimo de los derechos humanos fundamentales, definidos como tales en las convenciones internacionales, sea respetado.

Los Estados pueden ejercer la jurisdicción universal para crímenes considerados como

crímenes globales contra la Comunidad de los usuarios de Internet. Tales crímenes tendrían sin embargo ser listados de manera limitativa en una convención internacional.

§ 7 – Jurisdicción civil. Los Estados deberían ejercer la jurisdicción únicamente basándose en los principios de la previsibilidad, de la protección equitativa y de la justicia para todos las partes en el juicio. La cooperación internacional tendría que ser reforzada para este fin.

§ 8 – Tratamiento compensatorio. Los Estados tecnológicamente subdesarrollados o en vía de desarrollo tienen que beneficiarse de mecanismos compensatorios en orden de luchar contra la brecha digital, que no es más que una consecuencia de la brecha social pre-existente.

§ 9 – Autoridad Internacional. Una Autoridad Internacional debe ser establecida, en donde los Estados, las organizaciones de la sociedad civil y los individuos sean representados de manera equitativa, con el fin de delinear las políticas y generar una mayor participación en el Ciberespacio.

En lo que respecta a la administración de recursos del sistema, la labor del ICANN tiene que ser impulsada de manera tal que dicha organización no tenga ninguna sombra de control por parte de ningún gobierno y sus actividades sean desarrolladas a través del consenso y del desarrollo desde la amplia participación de los actores involucrados.