GOBERNANZA DE INTERNET: COMPONENTES NORMATIVOS Y SOCIOS CULTURALES DE UN AMBIENTE MULTISTAKEHOLDER

LAURA NAHABETIÁN BRUNET[1]

Resumen: El término "Internet" no abarca todos los aspectos existentes en materia de desarrollos digitales a nivel mundial. Sociedad de la información y el conocimiento es generalmente presentada como más integral y omnicomprensiva.

La gobernanza para algunos especialistas es sinónimo de gobierno.

Esta afirmación lleva a la interpretación que la gobernanza de Internet debe ser el tema de los gobiernos por lo que la participación de otros actores sobre todo no gubernamentales, estará limitada; pero ésta no es la opinión unánime.

Los marcos regulatorios deben desarrollarse para permitir modelos de negocio que sean más baratos, que faciliten la sostenibilidad de los servicios, incluyendo las redes y tecnologías de nueva generación.

Los gobiernos tienen un papel sustancial, y existen lecciones aprendidas en Europa, América del Norte y Asia que pueden ser un sustento para la formulación de políticas públicas que faciliten las acciones a emprender y que además se verifican imprescindibles.

Casi todos los aspectos de la gobernanza de Internet incluyen un componente normativo; sin embargo, la conformación de un marco jurídico adecuado que permita moldear el ágil desarrollo de Internet está en sus primeras etapas.

Aquí se presentan reflexiones asociadas a los componentes normativos y socioeconómicos que implica este nuevo paradigma.

Palabras clave: gobernanza – internet – derechos – libertad – regulaciones normativas

Key words: governance – internet – rights – freedom – rules and regulations

1. INTRODUCCIÓN

Ya en 2003, la revista The Economist comenzó a escribir Internet con una "i" minúscula.

Este cambio en la política editorial se inspiró en el hecho que Internet se había convertido en un elemento cotidiano, ya no único y, lo suficientemente especial como para

1 Docente universitario integrante del Instituto de Derecho Informático de la Universidad Mayor de la República y del Departamento de Derecho Constitucional y Derechos Humanos de la Universidad Católica del Uruguay.

justificar una letra mayúscula inicial. La palabra "Internet" siguió el destino lingüístico de telégrafo, teléfono, radio y televisión, así como otras tantas invenciones.

La cuestión de la escritura de internet / Internet con una "i" mayúscula o minúscula resurgió en la Conferencia Internacional de Telecomunicaciones, celebrada en Antalya en noviembre de 2006, en la que se introdujo una dimensión política cuando apareció el término "Internet" en la resolución de la ITU (Unión Internacional de las Telecomunicaciones) sobre la gobernanza de Internet con una "i" minúscula en lugar de la habitual, "I" mayúscula.

En esa oportunidad David Gross, - embajador de EEUU (Estados Unidos de Norteamérica) a cargo del gobierno de Internet -, expresó su preocupación en el sentido que la ortografía con minúsculas de ITU podría indicar la intención de tratar a Internet al igual que a otros sistemas de telecomunicaciones a nivel internacional que son regidos y regulados en su marco.

Algunos interpretaron esto como una señal diplomática de la intención de la ITU de desempeñar un papel más destacado en la gobernanza de internet.

Internet o internet, en cualquier caso éste fue el significado aceptado por las comunidades de Internet, ya que describe la forma en que se ha regido desde sus primeros días.

Los especialistas en telecomunicaciones consideran a la gobernanza de Internet a través del prisma del desarrollo de la infraestructura técnica. Los especialistas en informática se centran en el desenvolvimiento de diferentes normas y aplicaciones, tales como XML o Java. Los especialistas en comunicación hacen hincapié en la facilitación de la comunicación. Por su parte, los activistas de derechos humanos consideran la gobernanza de Internet desde la perspectiva de la libertad de expresión, la privacidad y otros derechos humanos.

Dependiendo de las áreas se verifican diferentes enfoques. Así, los especialistas en temas jurídicos se concentran en la agenda de derechos y en la competencia y solución de controversias. Los políticos se centran en los temas que se vinculan con sus electorados. Los diplomáticos se ocupan principalmente de los procesos de protección de los intereses nacionales.

1.1. ¿Qué significa la gobernanza de internet?

El término "Internet" no abarca todos los aspectos existentes en materia de desarrollos digitales a nivel mundial. Otros dos términos - sociedad de la información y la comunicación - son generalmente presentados como más integrales y omnicomprensivos. Y esto es así, en la medida que de esta forma se encuentran incluidas áreas que están fuera del dominio de Internet, tales como la telefonía móvil. El argumento a favor de la utilización del término "Internet", sin embargo, se ve reforzado por la rápida transición de la comunicación global hacia la utilización del protocolo de Internet como el estándar técnico principal de las comunicaciones.

Internet sigue creciendo a un ritmo muy ágil, no sólo en términos de la cantidad de usuarios, sino también en términos de los servicios que ofrece, sobre todo de voz sobre protocolo de Internet (VoIP), que puede desplazar incluso a la telefonía convencional.

En el debate sobre la gobernanza de Internet, sobre todo en la primera fase de la Cumbre Mundial de la Sociedad de la Información, la controversia surgió a raíz del término "gobernanza" y sus diversas interpretaciones.

Según una de éstas, la gobernanza es sinónimo de gobierno.

Muchas delegaciones nacionales tuvieron esta consideración inicial, lo que lleva a la interpretación de que la gobernanza de Internet debe ser el negocio de los gobiernos y por lo tanto la participación de otros actores sobre todo no gubernamentales, debe estar limitada.

La confusión desde el punto de vista tecnológico se vio subrayada a partir de la forma en que el término gobernanza solía ser utilizado por algunas organizaciones internacionales. En efecto, el término buena gobernanza ha sido utilizado por el Banco Mundial para promover la reforma de los estados a partir de la introducción de mayor transparencia, reducción de la corrupción y el incremento de la eficiencia en la administración. En este contexto el término gobernanza estaba directamente relacionado con el corazón mismo de las funciones gubernamentales.

A esta interpretación se enfrentaron quienes con un sentido más amplio del término "gobernanza", que incluye la gestión de los asuntos de cualquier institución, incluidas las no gubernamentales, entienden que la gobernanza es un espacio de construcción multistakeholder.

La confusión terminológica se complica aún más por la traducción del término "gobernanza" a otros idiomas.

En español, el término se refiere principalmente a las actividades públicas o de gobierno (Gestión Pública, Gestión del Sector Público, y Función de Gobierno). La referencia a las actividades públicas o gobierno también aparece en francés (Gestion des Affaires Publiques, Capacité de l' Administration, Qualité de l' administration y Mode de gouvernement). En Portugués sigue un patrón similar al referirse a los sectores público y gobierno (Gestão Pública y Administração Pública).

2. DE LA ASIMETRÍA AL DESARROLLO UNIVERSAL: COMPONENTES NORMATIVOS

Los marcos regulatorios han dado forma al mercado de las telecomunicaciones convirtiéndolo en lo que es hoy.

Los diferentes actores han sido más que relevantes en todo el proceso, no obstante lo cual, los gobiernos han desarrollado un papel más que trascendente, siendo los actores relevantes en la definición y el establecimiento de las diferentes disposiciones normativas que hoy por hoy rigen en todo el planeta.

Ahora bien, es importante tener presente que en muchas zonas, los cambios más importantes en estos marcos regulatorios no solo surgen y se desarrollan bajo lógicas gubernamentales sino que se han cumplimentado a partir de la conclusión de los procesos de privatización.

Estos cambios han sido sustanciales y en algunos casos dramáticos; a los tradicionales servicios caracterizados por las antiguas redes, con escasa penetración y prácticamente nula renovación, la densidad de la penetración ha sido exponencial.

Indudablemente las mayores demandas de conectividad se produjeron en las grandes ciudades y zonas urbanas densamente pobladas, donde se verifica tradicionalmente el más amplio mercado, debido a la mayor densidad de población.

Por lo tanto a la fecha es factible señalar que existen amplias zonas con excelentes niveles de conexión y conectividad mediante la utilización de diversas tecnologías y con posibilidad de acceso a una amplísima gama de servicios.

Sin embargo, no se trata de una situación generalizada, sino que por el contrario, subsisten amplias zonas del planeta, donde la rentabilidad de los servicios no es la adecuada y las carencias de conexión son de una cotidianidad avasallante. De aquí que no sea posible afirmar que el planeta vive inmerso en la sociedad de la información y el conocimiento, ya que ésta no es una realidad efectiva para más de la mitad de la población mundial.

Con la finalidad de afrontar el reto de la apertura de los mercados a la competencia, los nuevos marcos regulatorios incluyen el concepto de servicio universal, y la creación de fondos de acceso para subvencionar servicios no rentables. Asimismo, disposiciones normativas vinculadas con la concesión de licencias han sido aprobadas en varios países a los efectos de permitir, facilitar e incentivar la competencia y con ella la reducción de los costos de servicio a la población.

El hecho que la mayoría de las redes se verifiquen instaladas en las zonas urbanas significa que la disponibilidad de la infraestructura para el acceso a Internet es baja o muy baja en zonas rurales o en los pequeños pueblos del interior[2] que se encuentran lejos de las ciudades capitales. Si un ISP (proveedor de servicios en internet) quiere establecer un negocio en estas zonas, su precio para el usuario final debe incluir los costos de enlace de datos partiendo de la pequeña ciudad hacia la ciudad capital – lo que es muy caro – y a esto debe sumarse Internet con los cargos de conectividad, lo que lo dificulta enormemente por lo que se comprenden las contrariedades existentes en razón de la ecuación económica señalada.

El acceso a Internet y a las redes de telecomunicaciones significa e implica un sinnúmero de temas. No obstante, sólo llegan a ser verdaderamente importantes si ésta permite efectivamente la comunicación entre las personas y facilita la obtención de nuevas fuentes de conocimiento y aprendizaje. Las empresas y los países se benefician del acceso a Internet si se les ayuda a mejorar su productividad, mantener y aumentar sus

2 La situación de Uruguay es un tanto diferente a la realidad general de Latinoamérica ya que las estadísticas oficiales refieren a niveles de conexión que prácticamente estarían implicando a todo el territorio nacional.

ganancias y generar más puestos de trabajo para la gente.

La extrema pobreza que aún interpela a diferentes regiones del planeta producto de una asimetría vergonzante, y que, en muchos casos obedece a profundos cambios económicos, podría ser aliviada por un uso inteligente de Internet y las tecnologías de la información y la comunicación como mecanismos de acceso a nuevas fuentes de información.

Hay algunas iniciativas en ese sentido, pero el discurso es mayor que la incidencia efectiva, al menos eso es lo que ha demostrado la evidencia y nada hace indicar un cambio en el corto y mediano plazo.

Indudablemente lo que se necesita son servicios que sean asequibles para las poblaciones más pobres, pero es una determinación económica que el Estado debería sanear; si no son rentables para las empresas no tendrá sostenibilidad y ésta es la clave para ese tipo de proyectos, que deben comprender tanto a los servicios de acceso a Internet como a la telefonía móvil.

Las alianzas público - privadas, en las que cada actor ofrece su mejor capacidad, a priori podrían ser la respuesta para estos problemas; de hecho existe un buen número de ejemplos al respecto.

Los fondos de servicio universal podrían utilizarse para subvencionar la columna vertebral de los precios por enlace de datos, lo que haría este tipo de proyectos mucho más viable desde el punto de vista de la sostenibilidad.

Internacionalmente considerada, la iniciativa privada podría asociarse en las diferentes regiones con agencias de financiación con la finalidad de instalar más infraestructura en las distintas zonas que así lo necesitan.

A la luz de los cambios provocados por Internet durante las últimas décadas, existe la necesidad de revisar el concepto de acceso universal a fondos por un lado y el servicio universal por otro.

Los nuevos marcos regulatorios deben ser desarrollados para permitir nuevos modelos de negocio que sean más baratos, que faciliten la sostenibilidad de los servicios, incluyendo las redes y tecnologías de nueva generación.

Los gobiernos tienen un papel sustancial en este tema, y existen lecciones aprendidas en Europa, América del Norte y Asia que pueden ser un sustento para la formulación de políticas públicas que faciliten las acciones a emprender y que además se verifican imprescindibles. Un diálogo abierto entre los organismos de regulación de las diferentes regiones debe promover el intercambio de experiencias y el desenvolvimiento de criterios comunes que se trasunten en normatividad que facilite luego la interacción y solución de conflictos ágilmente.

Todos estos servicios sólo tendrán un verdadero sentido si se determinan disposiciones normativas con el objetivo de visualizar el desarrollo desde una visión humanista

en la que el centro sea la persona, y se procure la consolidación de la cultura local y la identidad específicas.

2.1. Instrumentos normativos

Casi todos los aspectos de la gobernanza de Internet incluyen un componente normativo; sin embargo, la conformación de un marco jurídico adecuado que permita moldear el ágil desarrollo de Internet está en sus primeras etapas.

Los dos enfoques prevalentes son:

a.- Una aproximación a la consideración tradicional del derecho, sin perjuicio de un tratamiento diferente a la evolución que han verificado otros mecanismos de comunicación. Internet ha contribuido a una evolución más rápida e integral en materia de comunicaciones, sin perjuicio que ha aportado mayores cambios desde una consideración de tipo cuantitativo antes que cualitativo. Así es que las disposiciones normativas preexistentes le son de aplicación en general.

b.- Una aproximación desde un enfoque de índole cibernético, que se basa en la presunción que internet introduce nuevas formas de relaciones sociales en el ciberespacio.

Así es que se plantea como necesario realizar una formulación integral a los efectos de regular los derechos en la red. Un argumento a favor de este enfoque se verifica en que la velocidad de la comunicación transfronteriza facilitada por internet dificulta el cumplimiento efectivo de la normatividad existente.

Una amplia variedad de instrumentos normativos han sido aprobados y son de aplicación a la gobernanza de Internet.

Cada una de las disposiciones normativas existentes consiste en reglas y sanciones. Reglas que estipulan ciertos comportamientos socialmente aceptados y sanciones que especifican castigos si éstas no son cumplidas.

Hasta la fecha, las áreas prioritarias de la normatividad vinculada con Internet han sido privacidad, protección de datos, propiedad intelectual, tributación y ciberdelincuencia.

Independientemente de qué enfoque sea el que se considere más apropiado, el principio general es que la normativa no determina que un comportamiento prohibido sea imposible, sino que únicamente lo transforma en punible. El hecho que el fraude está prohibido tanto en el mundo cibernético como en el mundo real no significa que el fraude será erradicado como resultado. Esta distinción es relevante debido a que uno de los argumentos frecuentes vinculado con el mundo del ciberespacio hace relación a que las conductas prohibidas en el mundo real no pueden ser utilizadas de manera eficiente en el virtual.

Ahora bien, las relaciones sociales son demasiado complejas, la sociedad es dinámica y muchas veces los desarrollos normativos van a la zaga del cambio social. Esto es espe-

cialmente notable en esta época, cuando el desarrollo tecnológico otorga nueva formulación a la realidad social mucho más rápido de lo que los legisladores pueden ejecutar la discusión y aprobación normativas. A veces, la normatividad se vuelve obsoleta incluso antes de su entrada en vigor y este riesgo de obsolescencia es una consideración importante en la regulación de Internet.

2.1.1 La autorregulación

La autorregulación ha sido el mecanismo propuesto como preferido para la regulación de internet.

Tiene elementos en común con las normas sociales y también múltiples diferencias, siendo la principal el hecho que las normas sociales, implican típicamente reglas tácitas y difusas y la autorregulación se basa en un conjunto explícito y bien organizado de reglas.

Las normas de autorregulación suelen codificar un conjunto de reglas.

La tendencia hacia la autorregulación es particularmente notable entre los ISPs.

En muchos países, los ISPs están bajo una creciente presión de las autoridades para hacer cumplir las normas relacionadas con la política de contenidos. Intentan responder a esta presión a través de la autorregulación mediante la imposición de ciertas normas de conducta para sus clientes.

Si bien la autorregulación puede ser una técnica regulatoria útil, persisten algunos riesgos en su uso para las zonas de alto interés público, como las políticas de contenidos en vínculo con la regulación de la libertad de expresión y la protección de la vida privada.

2.2. Jurisprudencia

La jurisprudencia es una fundamental fuente del Derecho pero además es central en la gobernanza de Internet.

Esto es así ya que las decisiones judiciales son la piedra angular del sistema jurídico norteamericano habiendo sido Estado Unidos de Norteamérica el primer país en abordar las cuestiones normativas de Internet. En este sistema, los precedentes crean derecho, especialmente en los casos relacionados con la regulación de las nuevas cuestiones, como Internet.

Una herramienta jurídica considerada por los jueces es la analogía jurídica, siendo este mecanismo el que mayormente se utiliza para resolver conflictos vinculados con internet.

2.3. Instrumentos jurídicos internacionales

La naturaleza transfronteriza de las actividades de Internet implica la necesidad de la utilización de instrumentos jurídicos internacionales. El derecho internacional público se aplica a muchas áreas de Internet incluidas las telecomunicaciones, los derechos

humanos y los delitos informáticos, entre otros. Asimismo, el derecho internacional privado es igualmente importante, para hacer frente a cuestiones relacionadas con Internet, ya que la mayoría de los casos judiciales implican cuestiones tales como contratos y responsabilidades comerciales.

Debido a la naturaleza global de Internet, las disputas jurídicas que involucran a individuos e instituciones de distintas jurisdicciones nacionales son muy frecuentes.

Sin embargo, sólo en raras ocasiones se ha utilizado el Derecho Internacional Privado para la solución de temas basados en Internet, posiblemente porque sus procedimientos suelen ser complejos, lentos y caros.

El Derecho Internacional Público regula las relaciones entre los Estados y las Organizaciones de Derecho Internacional, existiendo por tanto algunos instrumentos que le son propios que ya se ocupan de temas de interés de la gobernanza de Internet como las regulaciones de telecomunicaciones, los derechos humanos, las convenciones y tratados de protección de datos personales, entre otros.

2.3.1 Las Convenciones Internacionales

A lo largo de los años se han aprobado un conjunto considerable de convenios sobre cuestiones relacionadas con Internet por parte de la Unión Internacional de Telecomunicaciones, siendo la ITU la entidad más importante para la preparación de un marco normativo de las telecomunicaciones para avanzar en la evolución de Internet hacia adelante.

Asimismo, se han comenzado a aprobar una multiplicidad de tratados, convenciones y declaraciones vinculadas con sus temas de análisis.[3]

2.3.2 El Derecho Internacional Consuetudinario

El desarrollo de las normas consuetudinarias incluye dos elementos: la práctica general (consuetudo) y el reconocimiento de que tal práctica es jurídicamente vinculante (opinio juris). Por lo general, requiere un largo lapso de tiempo para la cristalización general de la práctica.

Algunos elementos del derecho consuetudinario emergen claramente en la forma en la que el gobierno de EEUU ejerce la supervisión desde la raíz de Internet. Tiene una constante práctica de no intervención en el tema de la gestión de dominios de país (por ejemplo .ch, .uk, .ge). La práctica general es el primer elemento en la identificación del derecho consuetudinario. Debe ser objeto de consideración el hecho que tal práctica general se basa en la conciencia del gobierno de EEUU de que su gestión de los dominios de país se verifica adecuada con las normas jurídicas internacionales (existencia de una opinio iuris). Si éste es el caso, existe la posibilidad de identificar la norma internacional habitual en la gestión de las partes del sistema de servidores raíz de Internet que tienen

3 Sólo a vía de ejemplo es posible citar al Convenio Nº 108 del Consejo de Europa en materia de Tratamiento Automatizado de Datos Personales, el Convenio sobre Ciberdelincuencia, Convenios de OMPI sobre Propiedad Intelectual, Declaraciones sobre libertad de expresión y acceso a la información pública, entre otros.

que ver con los dominios del país. Sería difícil extender este razonamiento a la situación jurídica de los gTLD (dominio de nivel superior genérico) - .com, .org, .edu, .net -, que no involucran otros países.

2.3.3 Soft law[4]

Soft law se ha convertido en un término que se utiliza con frecuencia en el debate de la gobernanza de Internet. Por lo general, los instrumentos de soft law contienen principios y normatividad general en lugar de las normas específicas que se encuentran habitualmente en documentos internacionales tales como declaraciones y resoluciones. Dado que no es jurídicamente vinculante, no se puede cumplir a través de tribunales internacionales u otros procedimientos de solución de controversias.

Se trata de una expresión que se ha puesto de moda recientemente. Procede de los EEUU y denomina a algunos instrumentos jurídicos que no son obligatorios, pero que influyen en la situación legislativa. Un ejemplo serían los acuerdos interinstitucionales sobre la calidad de la redacción o los actos no vinculantes de las instituciones que un Tribunal de Justicia debe considerar para interpretar los actos imperativos.

Se trata pues de una serie de normas a las que les falta uno de los elementos del concepto de norma jurídica, es decir, el efecto o consecuencia jurídica, esto es, la sanción.

Estas normas vienen a recuperar para el ámbito jurídico la característica básica de las normas sociales, dotadas de una sanción tácita que sólo supone en mayor o menor medida un descrédito o pérdida de consideración pública del que las incumple. Los Estados o instituciones que no cumplen lo que recomiendan estas normas sólo incurren en ese descrédito.

Desde el punto de vista de la finalidad, se trata no tanto de que se cumplan estrictamente sus recomendaciones como de que se cree un estado de opinión favorable a su cumplimiento. Dicho de otro modo, más que obligar, pretenden convencer.

Puesto que les falta la naturaleza de imperativas que caracteriza a las normas jurídicas perfectas, tampoco son condicionales porque su cumplimiento no depende de un hecho externo a la propia norma, y sirven para señalar la dirección que, con ánimo convincente, el legislador desea dar a la evolución de la normativa comunitaria, sería razonable decir que se trata de normas "indicativas".

Los principales documentos de la Cumbre Mundial de la Sociedad de la Información, incluida la Declaración Final, el Plan de Declaraciones regionales de acción, tienen el potencial de desarrollar cierta normatividad. Ellos no son jurídicamente vinculantes, pero por lo general son el resultado de prolongadas negociaciones y su posterior aceptación por parte de los Estados. El compromiso que tanto los estados nacionales como otras partes interesadas han puesto en la negociación de instrumentos jurídicos no vinculantes para llegar a un consenso que es imprescindible, crea el primer elemento en la consi-

4 Derecho de naturaleza incierta, menos vinculante, menos seguro, que se traduce en una armonización ficticia y una transposición aleatoria de las normas en los ordenamientos nacionales. Informe para el Consejo de Europa sobre el Documento COM(97) 626, "Legislar mejor" (A4-498/98); Resolución del Parlamento Europeo de 18 de diciembre de 1998.

deración de que tales documentos son más que simples declaraciones políticas.

El Soft law ofrece ciertas ventajas en el tratamiento de cuestiones de gobernanza de Internet.

En primer lugar, se trata de un enfoque menos formal, que no implica la ratificación por los Estados y, por lo tanto, no requiere de largas negociaciones.

En segundo lugar, es lo suficientemente flexible para facilitar la experimentación de nuevos enfoques y adaptación a la rápida evolución en el ámbito de la gobernanza de Internet.

En tercer lugar, proporciona una mayor oportunidad para un enfoque de múltiples partes interesadas que un estricto marco jurídico internacional con un enfoque restringido a los estados y las organizaciones internacionales.

2.3.4 Ius cogens

Ius cogens es descrito por el artículo 53 de la Convención de Viena sobre el Derecho de Tratados como una norma imperativa de Derecho Internacional general. Es aceptada y reconocida por la Comunidad Internacional de Estados en su conjunto en tanto norma que no admite acuerdo en contrario.

A partir de esto, no se permite su suspensión y solo puede ser modificada por una norma ulterior de Derecho Internacional general que tenga el mismo carácter.

Son ejemplos de normas de ius cogens los siguientes:

- La prohibición del uso de la fuerza.
- La ley de genocidio.
- El principio de no discriminación racial.
- Los crímenes de lesa humanidad.
- Las normas que prohíben el comercio de esclavos.

En el gobierno de Internet, las normas de ius cogens podrían ser utilizadas para actividades que promuevan algunas de estas reglas en el tratamiento, por ejemplo, de la información que se sube a la web.

2.4. Jurisdicción

"La jurisdicción configura a la vez, una función y un poder, aunque este último deba perfilarse no solo como tal sino como un poder – deber y, más ampliamente aún como un conjunto de poderes y deberes que, precisamente le son asignados al tribunal para que éste pueda desempeñar su función jurisdiccional"[5].

5 Tarigo, Enrique.- *Lecciones de Derecho Procesal Civil*. Fundación de Cultural Universitaria. 2da. Edición. Montevideo, 1994. Tomo I.

Ésta implica la autoridad de los órganos judiciales y estatales para decidir sobre las diferentes situaciones normativas.

La relación entre la competencia e Internet ha sido ambigua, ya que la jurisdicción recae principalmente teniendo en consideración la división geográfica del mundo en territorios nacionales. Cada Estado tiene el derecho soberano de ejercer su jurisdicción sobre su territorio. Sin embargo, Internet facilita considerablemente el intercambio transfronterizo, lo que dificulta considerablemente el monitoreo a través de los mecanismos tradicionales. La cuestión de la competencia en Internet pone de relieve uno de los dilemas centrales asociados con la gobernanza de Internet: ¿Cómo es posible "anclar" a Internet dentro de la geografía política y legal existente?

Son importantes los diferentes principios existentes para la determinación del tribunal competente en casos particulares, entre los que pueden señalarse el Principio de territorialidad que implica el derecho del Estado de gobernar a todo quien se encuentre dentro de su territorio y el Principio de la personalidad que determina el derecho del Estado para gobernar a sus ciudadanos dondequiera que estén (Principio de nacionalidad).

Otro principio importante introducido por el derecho internacional moderno es el de jurisdicción universal. El concepto de jurisdicción universal en sentido amplio determina el poder de un Estado para castigar ciertos crímenes, dondequiera y por quienquiera que se hayan cometido, sin ninguna conexión necesaria para con el territorio, la nacionalidad, o el interés especial del Estado, remitiendo incluso a consideraciones tales como acciones delictivas vinculadas con la piratería, crímenes de guerra y genocidio.

2.4.1 Conflictos de jurisdicción

Ahora bien, es posible que se verifiquen conflictos de competencias. Estos conflictos se plantean – como es sabido - cuando hay más de un Estado que reivindica la jurisdicción en un caso particular. Suele ocurrir cuando la situación de que se trata implica un componente extra-territorial (por ejemplo, involucra a individuos de diferentes estados, o transacciones internacionales). La jurisdicción competente es establecida por diferentes elementos tales como la territorialidad o la nacionalidad. Cuando se sube información en Internet es difícil la determinación de cuál es la normativa aplicable en caso de presentarse una violación al orden jurídico. La pregunta siguiente es cuál es el orden jurídico violentado.

En este contexto, casi todas las actividades de Internet tienen un aspecto internacional que podría dar lugar a múltiples jurisdicciones o al llamado efecto desbordamiento.

Además de las soluciones técnicas (geo-localización y filtrado), existen otros enfoques para resolver el conflicto de competencia que incluyen la armonización de las normativas nacionales y el uso del arbitraje.

En lo que hace relación con la armonización de las normativas nacionales, esto podría resultar en el establecimiento de un conjunto de normas equivalentes a nivel global. Con reglas idénticas en cada Estado, esta cuestión sería menos relevante.

La armonización en áreas donde ya existe un alto nivel de consenso global, como por ejemplo, la pornografía infantil, la piratería, la esclavitud y el terrorismo, se plantea como sustancial y de hecho se verifican varios avances en este sentido.

Sin embargo, en algunos campos, incluyendo las políticas de contenidos, no es muy probable que se pueda arribar a un consenso mundial en el corto plazo, dado que las diferencias culturales siguen sosteniendo un notorio enfrentamiento que no se pone de manifiesto en las primeras líneas de discusión.

Otra posible consecuencia de la falta de armonización es la migración de los materiales web a los países con menores niveles de regulación de Internet.

2.4.2 Arbitraje

El arbitraje es un mecanismo de resolución de conflictos de que se dispone para evitar recurrir a los tradicionales tribunales. En los arbitrajes, las decisiones son tomadas por una o más personas independientes elegidas por las partes en disputa. El arbitraje internacional en el sector empresarial tiene una larga tradición. En general, los mecanismos de arbitraje se establecen en un contrato privado en que se acepta la resolución de cualquier futura disputa por su intermedio. Una amplia variedad de contratos de arbitraje se verifican existentes, especificando cuestiones como la sede donde se desarrollará, los procedimientos, y la elección de la ley aplicable.

En comparación con los tribunales tradicionales, el arbitraje ofrece muchas ventajas, incluyendo mayor flexibilidad, menor gasto, mayor agilidad, elección de la jurisdicción, y la aplicación más fácil de laudos arbitrales extranjeros. Una de las principales ventajas del arbitraje es que supera el posible conflicto de jurisdicción. El arbitraje tiene ventajas particulares en lo que respecta a uno de los temas más complejos en las causas judiciales relacionadas con Internet, cual es la ejecución de resoluciones. La Convención de Nueva York sobre el Reconocimiento y la Ejecución de Laudos Arbitrales Extranjeros regula el cumplimiento de los laudos resultantes del arbitraje.

De acuerdo con este convenio, los tribunales nacionales están obligados a cumplir con los laudos arbitrales. Paradójicamente, a menudo es más fácil hacer cumplir el arbitraje en el extranjero mediante el régimen de la Convención de Nueva York que procurar la ejecución de la sentencia judicial extranjera.

La principal limitación del arbitraje es que no puede abordar las cuestiones de mayor interés público, como la protección de los derechos humanos, los cuales requieren de la intervención de los tribunales establecidos por el Estado para que sea efectiva.

El arbitraje se ha utilizado ampliamente en las disputas comerciales. Hay un sistema de normas e instituciones que se ocupa de las controversias comerciales muy bien desarrollado.

El principal instrumento internacional es la Comisión de las Naciones Unidas sobre Derecho Mercantil Internacional, Ley Modelo sobre Arbitraje Comercial Internacional de 1985.

Tanto el arbitraje como otros sistemas alternativos de solución de controversias se utilizan ampliamente para llenar el vacío generado por la incapacidad del Derecho Internacional Privado para tratar los casos de Internet. Un ejemplo particular de un método de resolución de conflictos en casos de Internet es el de los Nombres de Dominio a través de la Universal Domain – Name Dispute Resolution Policy desarrollada por la OMPI e implementado por ICANN (Internet Corporation for Assigned Names and Numbers) como el procedimiento de resolución de disputas primaria.

Desde el inicio de su trabajo bajo la denominada UDRP (Uniform Domain Name Dispute Resolution Policy) en diciembre de 1999, el Centro de Arbitraje y Mediación de OMPI ha administrado más de 30.000 casos.

La UDRP se estipula de antemano como un mecanismo de resolución de conflictos en todos los contratos que involucran el registro de gTLD (.com, .edu, .org, .net) y para algunos ccTLDs (dominio de nivel superior geográfico) también. Su aspecto distintivo implica que se aplican los laudos arbitrales directamente a través de los cambios en el DNS sin tener que recurrir a la participación de los tribunales nacionales.

De esta forma el arbitraje proporciona una manera más rápida, sencilla y económica de resolver las controversias.

No obstante, el uso del arbitraje como el principal elemento de solución de controversias en Internet tiene algunas limitaciones importantes.

En primer lugar, en la medida que el arbitraje suele establecerse por acuerdo previo, esto implica que no se cubra un área amplia de problemas cuando no hay acuerdo entre las partes (por ejemplo casos de difamación, diversos tipos de responsabilidades, delitos informáticos).

En segundo lugar, muchos analistas ven la práctica actual de fijación de una cláusula de arbitraje a los contratos regulares como una desventaja para la parte más débil en el contrato (por lo general el usuario de Internet o un cliente de e-commerce).

En tercer lugar, algunos autores están preocupados de que el arbitraje haga presión para que se extienda el sistema de utilización del precedente y comience a suprimir los diferentes sistemas de ordenación jurídica nacionales.

En el caso del comercio electrónico, podría llegar a ser más aceptable, dado el ya elevado nivel de unificación de las normas sustantivas del derecho mercantil. Sin embargo, la eventual extensión del sistema del precedente se ha convertido en una de las más delicadas cuestiones socioculturales en mérito a las implicancias de los contenidos de Internet, ya que los sistemas jurídicos nacionales reflejan los contextos culturales específicos.

2.5. Propiedad intelectual

El conocimiento y las ideas son los recursos clave en la economía global. La protección de conocimientos e ideas, a través de los derechos de propiedad intelectual, se ha

convertido en una de las cuestiones predominantes en el debate sobre la gobernanza de Internet, y tiene un fuerte componente orientado hacia su desarrollo.

Los derechos de propiedad intelectual se han visto afectados por el desarrollo de Internet, principalmente a través de la digitalización de los conocimientos y la información, así como a través de nuevas posibilidades para su manipulación. Los derechos de propiedad intelectual relacionados con Internet incluyen los derechos de autor, marcas registradas y patentes. Otros derechos de propiedad intelectual incluyen diseños, modelos de utilidad, secretos comerciales, indicaciones geográficas, y las variedades vegetales.

2.5.1 Derechos de autor

Los derechos de autor sólo protegen la expresión de una idea cuando ésta se ha materializado en diversas formas, tales como un libro, un CD o un archivo de computador. La idea en sí no es protegida por los derechos de autor. En la práctica, a veces es difícil hacer una clara distinción entre la idea y su expresión.

El régimen de derechos de autor ha seguido de cerca la evolución tecnológica y cada nuevo invento, como la imprenta, la radio, la televisión y el vídeo, ha realizado afectaciones en la aplicación de las normas de derechos de autor; Internet no es la excepción. El concepto tradicional de derechos de autor ha sido cuestionado de múltiples formas, desde el tan simple "cortar y pegar" para los textos de la Web como para actividades más complejas, tales como la distribución masiva de música y materiales de vídeo a través de Internet.

También permite a los titulares de derechos de autor, controlar la utilización de éstos poniendo a su disposición poderosas herramientas técnicas para su protección y contralor.

Estos acontecimientos ponen en peligro el delicado equilibrio entre los autores, los derechos y el interés del público, que es la base misma de la normativa de derechos de autor.

El interés público ha sido vagamente percibido por lo que los derechos no están suficientemente protegidos. Esto, sin embargo, tiende a su modificación lentamente, sobre todo a través de las numerosas iniciativas globales centradas sobre el libre acceso al conocimiento y la información como por ejemplo Creative Commons.

A nivel internacional, la protección de los dispositivos digitales se introdujo por el Tratado de Derechos de Autor de OMPI (Organización Mundial de la Propiedad Intelectual) de 1996. Este tratado contiene disposiciones para incrementar el régimen de protección de los derechos de autor a partir de disposiciones más estrictas vinculadas con las limitaciones de los derechos exclusivos de los autores, la prohibición de eludir la protección tecnológica de los derechos de autor y otras medidas conexas.

En EEUU, la protección más estricta de los derechos de autor se introdujo a través del DMCA (Digital Millennium Copyright Act) de 1998.

Más recientemente, varias regulaciones han sido adoptadas a nivel nacional e interna-

cional, con el objetivo de hacer cumplir un control más estricto, obligando a los intermediarios en Internet a filtrar o controlar la difusión de contenidos con derechos de autor.

Francia adoptó la ley conocida como HADOPI[6] en 2009, que introduce el denominado procedimiento contra la violación de los derechos de autor en línea, que puede llegar a la suspensión de acceso a Internet para el suscriptor en cuestión[7].

Luego, durante 2011 en Estados Unidos fueron promovidos dos proyectos de ley - SOPA (Stop Online Piracy Act)[8] y la PIPA (IP Protection Act)[9]- que preveían nuevos medios para luchar contra la piratería en línea, incluyendo el bloqueo del acceso de sitios web y la prohibición a los motores de búsqueda de vincularse con dichos sitios.

Por otra parte, se estableció el ACTA (Acuerdo Comercial contra la Falsificación)[10] que se negociara fuera de los marcos institucionales internacionales adecuados habilitando regulaciones permisarias de acciones privadas inconvenientes, lo que motivó severas críticas sobre todo de asociaciones vinculadas con los derechos y libertades.

Las herramientas que son utilizadas por los delincuentes pueden ser usadas por los defensores, también. Tradicionalmente, las autoridades estatales y las empresas llevan a cabo sus responsabilidades a través de mecanismos normativos. Sin embargo, el uso de herramientas de software "alternativos" por el sector empresarial contra los infractores de derechos de autor, está en aumento.

Como un enfoque a largo plazo y de carácter más estructural, el sector empresarial presentó diversas tecnologías para la gestión de accesos a los materiales protegidos por copyright.

Microsoft introdujo el software de administración de derechos digitales para gestionar la descarga de archivos de sonido, películas y otros materiales protegidos por copyright. Similares sistemas fueron desarrollados por Xerox (ContentGuard), Philips y Sony (InterTrust).

El uso de herramientas tecnológicas para la protección de los derechos de autor encontró fundamento jurídico, tanto a nivel internacional - Tratado de OMPI - como en la DMCA. Por otra parte, ésta criminaliza la actividad que tiene por objeto eludir la protección tecnológica de materiales con derechos de autor.

Frente a todo este panorama, las preguntas son, por un lado, cuál debe ser la política a asumir por los Estados, esto es, modificar la existente o desarrollar nuevos mecanismos de derechos de autor. Por otro lado, es necesario ajustar éstos para reflejar los profundos

6 HADOPI.- Disponible en: http://en.wikipedia.org/wiki/HADOPI_law (visitado el 2/02/2014).

7 Fue derogada por Decreto 0157, del Ministerio de Cultura francés, en julio de 2013 luego de su aprobación pero con importantes recortes a sus medidas centrales por parte del Consejo Constitucional.

8 Stop Online Piracy Act.- Disponible en: http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act (visitado el 2/02/2014).

9 Protect IP Act.- Disponible en: http://en.wikipedia.org/wiki/PROTECT_IP_Act (visitado el 2/02/2014).

10 Anti-counterfeiting Trade Agreement.- Disponible en: http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement (visitado el 2/02/2014).

cambios efectuados por la evolución de las TIC y de Internet, o no.

Una respuesta sugerida en el Libro Blanco sobre la Propiedad Intelectual de EEUU indica que solamente cambios menores son necesarios en la regulación existente, principalmente a través de la "desmaterialización" de los derechos de autor. Establece que conceptos tales como "fijación", "distribución", "transmisión" y "publicación" fue el enfoque adoptado en los principales tratados de derechos de autor, incluyendo los aspectos relacionados con los Derechos de Propiedad Intelectual relacionados con el comercio de la Organización Mundial del Comercio y las convenciones de copyright de OMPI.

Sin embargo, la opinión contraria sostiene que los cambios en el sistema normativo deben ser profundos, ya que el derecho de autor en la era digital no se refiere únicamente al "derecho a impedir copiar", sino también al "derecho a impedir el acceso". En última instancia, cada vez son mayores las posibilidades técnicas de restringir el acceso a materiales digitales pudiéndose cuestionar si la protección del derecho de autor es necesaria en forma absoluta o no. Frente a esto, resta considerar cómo se protege al interés público que es la segunda parte de la ecuación del derecho de autor.

2.5.2 Protección del interés público - el justo uso de materiales con copyright

El Derecho de Autor fue inicialmente diseñado para fomentar la creatividad y la invención. Esto se debe a que combina dos elementos: la protección de los derechos de autor y la protección del interés público. El reto principal es establecer la forma en la que el público puede acceder a los materiales con derechos de autor con el fin de mejorar la creatividad, el conocimiento, y el bienestar global. Operativamente hablando, la protección del interés público está garantizada a través del concepto de "uso justo" de los materiales.

Cualquier restricción del uso justo podría debilitar la posición de los países en desarrollo.

Internet es para los investigadores, estudiantes y todos quienes estén interesados provenientes del mundo en desarrollo, una poderosa herramienta para la participación en el ámbito académico mundial y el desarrollo de intercambios científicos. Un régimen de derechos de autor restrictivos podría tener un efecto negativo en el desarrollo de capacidades en los países en desarrollo. Otro aspecto es la creciente digitalización de los oficios artísticos y culturales de los países en desarrollo.

Paradójicamente, éstos pueden llegar a tener que pagar por su patrimonio cultural y artístico cuando éste es digitalizado. En estos casos, mayormente pasa a ser propiedad de extranjeros que son quienes ostentan la calidad de titulares de las compañías de entretenimiento y medios.

2.5.3 OMPI y ADPIC

Existen dos principales regímenes internacionales de derechos de propiedad intelectual. La Organización Mundial de la Propiedad Intelectual que gestiona el régimen de Derechos de Propiedad Intelectual, sobre la base de la Convención de Berna y el Con-

venio de París y el otro régimen dirigido por la Organización Mundial del Comercio en base a los ADPIC (Acuerdo de la OMC sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio). El cambio de coordinación internacional de los Derechos de Propiedad Intelectual de la Organización Mundial de la Propiedad Intelectual a la Organización Mundial del Comercio se llevó a cabo con la finalidad de fortalecer su protección, especialmente en el ámbito de la observancia y la ejecución. Éste fue uno de los principales logros de los países desarrollados durante la ronda de negociaciones de la Organización Mundial del Comercio celebrada en Uruguay.

Muchos países en desarrollo tienen relación con estas modificaciones y desenvolvimientos. Los mecanismos de aplicación de la Organización Mundial del Comercio son muy estrictos, sin embargo podría reducirse el margen de maniobra de los países en desarrollo y la posibilidad de equilibrar el desarrollo necesita la protección internacional de los derechos de propiedad intelectual.

Hasta ahora, el principal foco de la Organización Mundial del Comercio ha estado en varias interpretaciones relacionadas con los derechos de propiedad intelectual para productos farmacéuticos. Es muy probable que los futuros debates se desenvuelvan en relación con los Derechos de propiedad intelectual e Internet.

2.5.4 Responsabilidad por infracción de derechos de autor

Los mecanismos internacionales de aplicación en el ámbito de la propiedad intelectual con el devenir del tiempo, se han fortalecido considerablemente por lo que los ISPs responsables del alojamiento en eventual violación del derecho de autor, han debido adoptar medidas en caso que el material no sea retirado después de la notificación de infracción. Esto ha hecho que el régimen de derechos de propiedad intelectual tradicional sea directamente exigible en el ámbito de Internet.

El enfoque adoptado por la DMCA de EEUU y la UE es muy interesante[11] e implica la eximición al proveedor de servicios de toda responsabilidad por la información transmitida o almacenada en la dirección de los usuarios. Se demanda que el servicio del proveedor se desarrolló de acuerdo con un procedimiento establecido que implica notificación y retiro de los materiales en infracción[12]. Esta solución proporciona cierta comodidad a los ISPs, ya que están a salvo de las sanciones jurídicas, pero también, potencialmente, los transforma en jueces del contenido[13] y sólo parcialmente resuelve el problema, ya que los contenidos impugnados podrían ser publicados en otro sitio web, alojado por otro ISP.

11 Considérense: Directiva europea 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico y la Directiva europea 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, sobre la armonización de determinados aspectos de los derechos de autor y derechos afines en la sociedad de la información. Disponibles en:

http://europa.eu/legislation_summaries/consumers/protection_of_consumers/l24204_en.htm (visitado el 2/02/2014).

12 El procedimiento de "notificación y retiro" se refiere a la obligación de los proveedores de servicios de eliminar el contenido de los sitios web bajo su administración si reciben una notificación o queja con respecto a la legalidad de dicho contenido específico.

13 Por temor a enfrentarse a posibles sanciones legales, algunos ISP prefieren restringir el acceso a los contenidos indicados, incluso cuando no se tiene certeza de la comisión de una infracción.

Un caso particularmente relevante para el futuro de los derechos de autor en Internet es el caso contra Grokster y StreamCast, dos compañías que producen intercambio de archivos de software. Siguiendo las disposiciones de la DMCA, la RIAA (Recording Industry Association of America) pidió a estas empresas que desistieran del desarrollo de la tecnología de intercambio de archivos que contribuye a la infracción de los derechos de autor. En un principio, los tribunales de EEUU optaron por no responsabilizar a estas empresas de software por la posible infracción de los derechos de autor, bajo circunstancias razonables. Sin embargo, en junio de 2005, la Suprema Corte de EEUU dictaminó que los desarrolladores de software fueron responsables de cualquier posible uso incorrecto de su software. La EFF (Electronic Frontier Foundation) señaló este caso como el preludio de la ola de demandas que siguió en los subsiguientes años contra individuos y proveedores de Internet[14]. Aunque la RIAA abandonó sus demandas de infracción de derechos de autor, aún permanecen en el centro de atención y ha sido necesario diversificar al mismo ritmo los desarrollos tecnológicos.

2.6. Marcas y patentes

2.6.1 Marcas comerciales

Las marcas comerciales son relevantes para Internet debido a la inscripción de los nombres de dominio. En la fase temprana del desarrollo de Internet, el registro de nombres de dominio se basó en llegar primero. Esto llevó a la ciberocupación, es decir, la práctica de registrar nombres de las compañías y venderlos después en un precio elevado o elevadísimo.

Esta situación obligó al sector empresarial a colocar la cuestión de la protección de las marcas en el centro de la reforma de la gobernanza de Internet, dando lugar a la creación de ICANN en 1998. En el Libro Blanco sobre la creación de ICANN, el gobierno de EEUU exigió que éste desarrollara y pusiera en práctica un mecanismo para la protección de las marcas en el campo de los nombres de dominio. Poco después de su creación, introdujo el desarrollo de la propiedad intelectual, sobre todo en lo que hace relación con las disputas vinculadas con los procedimientos de resolución de controversias de carácter universal.

2.6.2 Patentes

Tradicionalmente, la patente protege un nuevo proceso o producto de carácter técnico o el proceso de producción. Los registros de patentes dan lugar a múltiples casos judiciales que implican grandes cantidades de dinero. En algunos casos se han concedido patentes para los procesos de negocio, y algunos de ellos fueron controvertidos, como la petición de British Telecom para la obtención de los derechos de licencia de patente en los enlaces de hipertexto, que se registrara en la década de 1980. En 2002, British Telecom[15] ganó el proceso, sin perjuicio que a los usuarios de Internet se les exigiría que

14 EFF - RIAA v. The People: Five Years Later.- Disponible en: https://www.eff.org/wp/riaa-v-people-five-years-later (visitado el 2/02/2014).

15 Loney, Matt.- "*Hyperlink patent case fails to click. CNET News.com*", 2002. Disponible en: http://news.com.com/2100-1033-955001.html (visitado el 2/02/2014).

pagaran una cuota por cada enlace de hipertexto creado o usado.

Es importante subrayar que la práctica de conceder patentes para software y otras relacionadas con procedimientos de Internet no ha sido aceptada en Europa y otras regiones[16].

2.7. Cibercrimen

La responsabilidad penal en aplicación de la tecnología electrónica, informática y telemática si bien no es una temática nueva, implica avanzar en la catalogación de conductas inimaginables hasta hace relativamente poco tiempo y que por la vertiginosidad con que avanzan las tecnologías impone la necesidad de encontrar soluciones a una realidad que se impuso.

En efecto, las transformaciones económicas producidas por la globalización en todas sus manifestaciones han implicado un desenvolvimiento masivo de las tecnologías de la información y la comunicación con incidencias directas en todas las manifestaciones de la vida social.

A ésta no escapa la aparición de conductas que por medio de la aplicación de los sistemas informáticos y de internet, generan trastornos importantes en la comunidad nacional e internacional, los que se ven agravados por la inexistencia de disposiciones normativas acordes que faciliten la punición de las mismas.

Es imprescindible entonces, avanzar en una regulación normativa a efectos de que los diferentes países incluyan – los que aún no lo han hecho[17] - en sus ordenamientos jurídicos un marco apropiado que facilite el combate a la ciberdelincuencia. Sin embargo, es importante considerar que el régimen que se adopte debería ser minimalista y sin posiciones definitivas en términos tecnológicos, de forma tal de evitar una obsolescencia inexorable pero no inmediata.

La referencia a delitos informáticos debe entenderse efectuada a "la realización de una acción que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos de un titular en un elemento informático, ya sea hardware o software"[18].

El Prof. Carlos Casabona indica que se trata de conductas que atentan de forma grave a determinados bienes del individuo – pero también personas jurídicas – que presentan una configuración específica y exclusiva de la actividad informática y telemática y han sido sometidos a una tipología técnico criminológica: acceso, alteración, destrucción, no autorizados de datos contenidos en un sistema, reproducción completa o parcial de esos datos, creación de ficheros clandestinos, venta de ficheros informáticos, sustracción del

16 Información acerca del debate europeo de la patentabilidad del software, disponible en: http://eupat.ffii.org/ (visitado el 2/02/2014).

17 La República del Perú aprobó en el mes de diciembre de 2013, su Ley de Delitos informáticos.

18 Davara, Miguel.- Delitos y fraudes informáticos. 2010. Disponible en:
http://www.davara.com/areas/otras-delitos.html (visitado el 2/02/2014).

tiempo de sistemas de redes informáticas, telemáticas, etc. De esta forma, el computador así como los sistemas de telecomunicación a su servicio y el de sus elementos, son el objeto del delito.

Finalmente, la Organización para la Cooperación Económica y el Desarrollo ha indicado que es "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la trasmisión de datos"[19].

Es muy trascendente entonces a estos efectos la consideración que ha efectuado el Prof. Enrique Pérez Luño quien ha señalado que la esfera de acción de internet hace propicia la comisión de delitos en seis ámbitos, a saber:

1. La intimidad, la imagen y el honor de las personas.
2. La libertad sexual.
3. La propiedad intelectual.
4. El orden público y la seguridad del Estado.
5. La hacienda pública.
6. La propiedad.

En este sentido es a su vez muy importante tener en cuenta tres áreas que son fundamentales y en las que la colaboración fáctica y también normativa son centrales, a saber:

2.7.1 Ciberseguridad

El término Ciberseguridad se define como los procedimientos aplicados para la gestión y protección del uso, procesamiento, almacenamiento y transmisión de datos e información, a través de las tecnologías de información y comunicación al momento de navegar en el ciberespacio. La Ciberseguridad es vital para los internautas ya que la confidencialidad de sus sistemas puede ser vulnerable a los ataques de virus informáticos.

La ciberdelincuencia se ha expandido mucho en los últimos años debido a la difusión de Internet. Tal es así que entre los principales avances de 2013 en la materia se destaca la creación del Centro Europeo del Cibercrimen EC3 dentro del seno de Europol[20], así como las múltiples regulaciones surgidas en los diferentes países que han iniciado el camino de la normatividad en esta temática[21].

2.7.2 Ciberdefensa

La determinación conceptual específica de ciberdefensa, ha sido y sigue siendo de una importante complejidad, sin perjuicio que no se trata de una actividad novedosa ya que puede remontarse a finales del siglo pasado.

19 OCDE.- Computer related criminality: analisys of legal policy in the OECD Area. 1984.

20 Información disponible en: https://www.europol.europa.eu/ec3 (visitado el 2/02/2014).

21 Es el caso por ejemplo de EEUU, España y Colombia.

Sin embargo, es posible afirmar que se trata de un concepto estratégico de los gobiernos que requiere la comprensión de variables tales como las vulnerabilidades en la infraestructura crítica de un Estado, las garantías y derechos de los ciudadanos en el mundo online, la renovación de la administración de justicia en el entorno digital y, la evolución de la inseguridad de la información en el contexto tecnológico y operacional.

En función de lo antedicho y su vínculo con la ciberguerra es central que se posicione el pensamiento estratégico vinculado con la defensa no solo en su consideración tradicional sino en aquélla de índole global mediante las tácticas, técnicas y procedimientos que otorguen seguridades a los ciudadanos. Por lo tanto es imprescindible avanzar a partir de una aproximación holística de todos los actores que deben implicarse en la defensa del bienestar, intereses y valores de estados libres y democráticos, de ahí su centralidad para la gobernanza de internet.

2.7.3 Ciberguerra

La referencia a ciberguerra debe considerarse efectuada al desplazamiento del conflicto - tradicionalmente bélico - al ciberespacio, mediante la utilización de las tecnologías de la información que sustituyen a los tradicionales campos de batalla. La ciberguerra es rentable y anónima permitiendo ataques a gran escala en la medida que no se verifican barreras de índole física que impidan que se propaguen los ataques.

Se trata de un hacking cuya motivación es de orden político y su objetivo es el sabotaje y el espionaje. La finalidad es la producción de alteraciones en la información y sistemas de quien se determina como enemigo conjuntamente con la protección de la información y sistemas propios.

La Resolución del Consejo de Seguridad de Naciones Unidas sobre ciberguerra estableció que se trata del uso de computadores o medios digitales por un gobierno, sea con conocimiento explícito o aprobación de ese gobierno contra otro estado, o propiedad privada dentro de otro estado incluyendo: accesos intencionales, interceptación de datos o daño a infraestructura digital e infraestructura controlada digitalmente".

Desde el punto de vista geoestratégico es posible visualizar a futuro que la ciberguerra en la actualidad no es más que la escaramuza primaria de futuros conflictos. Por lo mismo, es central tener conciencia de la gravedad de la situación y analizar las capacidades de reacción y discusión políticas seria y negociada.

Entre las amenazas más importantes a la seguridad mundial se encuentra en tercer lugar después de la guerra mundial convencional y las armas de destrucción masiva, sobre todo en la consideración que varios países han declarado tener lo que se denomina ciberarmada.

Los escenarios más complejos y difíciles de la ciberguerra hacia el futuro son:

1.- La relación entre EEUU y China que en teoría funciona sin mayores contratiempos, pero que es una relación de tensión permanente y que tiene múltiples aristas de cuidado.

En efecto, se han verificado un sin número de acusaciones en los últimos tiempos vinculadas con espionaje, denegación de servicios, acceso a infraestructuras, intervenciones en la red, ataques que parten de equipos zombies que operan como una Botnet (red de operadores infestados), entre otras. Más de la mitad de los casos reportados de seguridad comprometida remiten a ataques desarrollos desde o hacia Estados Unidos o China.

2.- Enemigos como Irán o Corea del Norte. Desde 2010, la intrusión informática en la planta de enriquecimiento de uranio iraní de Nataz y la aparición del Stuxnet[22] deben tenerse como dos hitos fundamentales en la consideración geoestratégica de algunos países como Irán, Siria y Corea del Norte. El mayor problema que presentan estas armas de índole cibernético es su casi independencia de operación ya que una eventual mutación podría implicar una operación a escala no prevista e incluso contra sus propios creadores.

En este mismo sentido, es importante considerar las actividades que ha iniciado Hezbollah en el ciberespacio, así como el desenvolvimiento de la llamada OpUSA y el equipamiento a yihadistas[23] contra Siria.

Las eventuales instalaciones nucleares de Corea del Norte también han sido un objetivo central tanto de Corea del Sur como de EEUU. Así se produjeron ingresos de hackers en las redes norcoreanas lo que implicó una fuerte tensión internacional así como la nulidad del armisticio entre las dos Coreas.

3.- La situación de Rusia. Se han desarrollado importantes ataques de supuestos hackers a diferentes países con vínculo político importante con Rusia, por lo que se han adjudicado éstos a este país, sin que haya sido reconocido en ningún caso. En general se establece que se trataría de hackers por encargo cuya encomienda es la movilización de Botnets.

4.- Anonymous y el Hacktivismo. Si bien se han producido varias detenciones vinculadas con Anonymous o LulzSec, éstas no han determinado una suspensión de las campañas que efectúan estos grupos. Anonymous ha pretendido avanzar en su ubicación como defensor de derechos en la red, pero de todas formas continúa en su prédica y accionar tradicionales.

5.- Los límites difuminados de la guerra contra el terrorismo. En esta línea se verifican múltiples situaciones complejas. Así el yihadismo internacional ha iniciado la visualización de la actividad en la red con mayor extensión que el reclutamiento y comunicación de los miembros, sino que la pretensión es la utilización de metodologías diversas – incluso similares a las de Anonymous – para el desenvolvimiento de sus acciones.

Indudablemente bajo el slogan de lucha contra el terrorismo, es posible identificar consideraciones de índole populista capaz de justificar cualquier decisión bajo la lógica

22 Stuxnet es un gusano informático que afecta a equipos con Windows. Es el primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitorización de procesos, pudiendo afectar a infraestructuras críticas como centrales nucleares.

23 El yihadismo es un neologismo occidental utilizado para denominar a las ramas más violentas y radicales dentro del islam político, caracterizadas por la frecuente y brutal utilización del terrorismo, en nombre de una supuesta yihad.

de la opinión y el interés públicos. Así la ciberyihad ha aparecido como un mecanismo hábil para sostener una suerte de tensión pública suficiente para "estar de acuerdo" con la vulneración de derechos que en otra instancia sería absolutamente intolerable.

El equilibrio entre las medidas es imprescindible para avanzar en la lucha contra el terrorismo y el respeto de los derechos fundamentales. Existe un riesgo real de que algunas medidas de seguridad puedan, directa o indirectamente, socavar los principios y derechos que el terrorismo pretende destruir.

Es peligroso establecer normas para el libre flujo de información, pero por otro lado, es imprescindible.

Esto no sólo puede impedir el intercambio abierto de ideas y opiniones, sino que también puede obligar a las ideas no deseadas - por ejemplo, el discurso y la propaganda por el odio,- que se expresan en forma vil, a ponerse de manifiesto lo que si bien no es difícil de contrarrestar con argumentos informados genera tensiones innecesarias y a veces, insostenibles.

Además, existe el riesgo de que las ideas y opiniones que podrían mejorar el debate abierto sobre temas polémicos sean silenciadas. El verdadero reto consiste en explotar plenamente el potencial de los nuevos medios de comunicación sin poner en peligro los derechos fundamentales, derechos y libertades civiles, incluido el derecho a la privacidad. Todos los ciudadanos tienen derecho a expresar sus ideas y opiniones en todo el mundo así como también lo tienen a buscar información libremente a través de las redes electrónicas.

2.8. Privacidad y protección de datos

Privacidad y protección de datos son dos cuestiones de gobernanza de Internet que se encuentran relacionadas fuertemente entre sí.

La protección de datos es un mecanismo normativo que garantiza la privacidad. Sin embargo, cuando se habla de privacidad a qué debe entenderse efectuada la referencia.

Por lo general se define como el derecho de cualquier ciudadano a controlar su propia información de carácter personal y decidir al respecto por la divulgación o no de tal información. Tanto la intimidad cuanto la protección de datos personales son derechos de carácter fundamental. Múltiples disposiciones normativas internacionales los refieren en las diferentes épocas de su desenvolvimiento, que avanzan desde la intimidad, pasando por la privacidad, la autodeterminación informativa hasta la protección de datos personales. Así es posible citar la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, entre otros muchos acuerdos y convenciones regionales e internacionales de derechos humanos, que los prevén.

Las culturas nacionales y el modo de vida influyen en la práctica de la vida privada. Aunque este tema es importante en las sociedades occidentales, puede tener menor importancia en otras culturas. Las prácticas modernas de la privacidad se centran funda-

mentalmente en la privacidad de la comunicación (ausencia de vigilancia en la comunicación) y privacidad de la información (ausencia de manejo de la información acerca de los individuos). Los problemas de privacidad, que tradicionalmente han sido utilizados para centrarse en las actividades gubernamentales, han visto ampliado su círculo de injerencia y ahora incluyen al sector de los negocios.

2.8.1 Personas y Estados

No es una novedad que la información siempre ha sido una herramienta esencial para que los estados ejerzan la autoridad sobre sus territorios y poblaciones. Los gobiernos reúnen grandes cantidades de datos personales (actas de nacimiento y matrimonio, números de seguridad social, registros de votación, antecedentes penales, información fiscal, registros de vivienda, coches, propiedades, entre otros).

Las tecnologías de la información, usadas por ejemplo en la minería de datos, colaboran en la agregación y correlación de datos de muchos sistemas especializados (por ejemplo, tributos, registros de vivienda, propiedad de automóviles) al realizar análisis sofisticados, la búsqueda de patrones usuales e inusuales así como detección de inconsistencias. Uno de los principales desafíos de las iniciativas de gobierno electrónico es garantizar un equilibrio adecuado entre la modernización estatal y las funciones y las garantías de los derechos de privacidad de los ciudadanos, incluida la restricción de la recopilación de información a lo estrictamente necesario para llevar a cabo el papel de la administración pública.

Sin embargo, los últimos años han sido testigos de un aumento de la voracidad de los gobiernos para la recolección y asociación de más datos personales para la identificación obligatoria de las personas, como es el caso de los datos biométricos.

Después de los acontecimientos del 11 de septiembre de 2001 en los EEUU se dictó el Patriot Act[24] así como normatividad similar en otros países, previéndose entre otras cuestiones las posibilidades de la autoridad para recopilar información, incluyendo previsiones vinculadas con la interceptación de la información. El concepto de interceptación legal en la obtención de pruebas fue también incluido en el Convenio del Consejo de Europa sobre Cibercriminalidad (artículos 20 y 21)[25].

Por otra parte, la UE solicitó la adopción de legislaciones nacionales que permitan la conservación de los datos necesarios para identificar a un usuario durante un período de 6 a 24 meses.

2.8.2 Personas y empresas

La segunda, y cada vez más importante relación social es la que existe entre las personas y el sector empresarial. La persona facilita información personal al abrir una cuenta bancaria, efectuar la reserva de un vuelo o un hotel, realizar el pago en línea con tarjeta

24 Epic.org.- US Patriot Act. Disponible en: http://epic.org/privacy/terrorism/hr3162.html (visitado el 2/02/2014).

25 Consejo de Europa.- Convención sobre Cibercriminalidad, de 23 de noviembre de 2001. Disponible en: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm (visitado el 2/02/2014).

de crédito, o incluso navegar o buscar información en Internet; múltiples rastros de datos a menudo se dejan en cada una de estas actividades.

El éxito y la sostenibilidad del comercio electrónico, depende de la creación de una amplia confianza tanto en las políticas de privacidad de las empresas cuanto en las medidas de seguridad que se establecen para proteger la información confidencial de los clientes contra el robo y el mal uso de la información. Con la expansión de las plataformas de redes sociales (por ejemplo, Facebook, Twitter), las preocupaciones en torno al eventual mal uso de los datos personales - no sólo por el propietario o administrador de una plataforma de redes sociales, sino también por otros individuos participantes en ellas se han incrementado.

En una economía de la información, aquélla sobre los clientes, incluyendo sus preferencias y perfiles de compra, se convierte en un importante producto de mercado.

Para algunas empresas, tales como Facebook, Google y Amazon, la información acerca de las preferencias de los clientes constituye una piedra angular de su modelo de negocios. Básicamente la moneda que los usuarios pagan por los servicios prestados (en línea) "para su utilización libre" son los datos personales, ya sea en forma de una cookie del navegador que indica su comportamiento en línea o una información específica solicitada en el llenado de un formulario web o al momento de hacer un pago. Y con el aumento de la cantidad de información que los usuarios revelan acerca de sí mismos, las violaciones a la privacidad se vuelven cada vez más frecuentes y sofisticadas[26].

2.8.3 Estados y empresas

Otro ángulo de la privacidad – quizás el menos publicitado –, tal vez sea el más importante. Tanto los Estados como las empresas recogen considerables cantidades de datos sobre las personas. Algunos de estos datos se intercambian con otros estados y empresas para impedir, por ejemplo, las actividades terroristas. Sin embargo, en algunas situaciones, como aquéllas a las que la Directiva Europea sobre Protección de Datos se aplica, el Estado supervisa y protege los datos de las personas en poder de las empresas.

2.8.4 Personas ante sí y sus pares

Un último aspecto de la protección de la intimidad, es el riesgo potencial para la privacidad que es generado por los propios individuos. Hoy en día, cualquier persona con suficientes fondos puede poseer poderosas herramientas de vigilancia; incluso un simple teléfono móvil equipado con una cámara puede convertirse en una herramienta de este tipo.

Muchas de las instancias de invasión de la privacidad se han producido, desde un simple voyeurismo al uso sofisticado de cámaras de videovigilancia, de números de tarjetas de registro de los bancos al espionaje económico.

26 Marsan Carolyne.- "*15 worst Internet privacy scandals of all time. Network World*". 2012. Disponible en: http://www.networkworld.com/news/2012/012612-privacy-scandals-255357.html?page=1 (visitado el 2/02/2014).

El principal problema para la protección de este tipo de violación de la privacidad es que la mayoría de la normatividad se centra en los riesgos para la privacidad derivados del Estado pero no de las propias personas en forma individual. Ante esta nueva realidad, algunos gobiernos han tomado importantes medidas iniciales.

Así el Congreso de EEUU ha aprobado la Ley de Prevención de Video Voyeurismo[27], que prohíbe la toma de fotos de personas desnudas sin su aprobación.

Alemania y algunos otros países han adoptado leyes de privacidad similares, evitando la vigilancia individual.

Uno de los principales instrumentos internacionales en materia de privacidad y protección de datos es el Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento automatizado de Datos de Carácter Personal de 1981[28]. A pesar de que fue adoptado por la organización regional – Consejo de Europa -, está abierto a la adhesión de estados no europeos[29].

Dado que el Convenio es tecnológicamente neutral, ha resistido la prueba del tiempo. Sin embargo, los desafíos planteados por el desarrollo tecnológico han provocado la necesidad de la actualización de su texto y existen borradores de propuesta que están siendo analizados desde 2012.

La Directiva de Protección de Datos de la UE (Directiva 95/46/CE)[30] también ha formado un marco normativo importante para el tratamiento de datos personales en la Unión Europea y ha tenido un gran impacto no sólo en el desarrollo normativo europeo sino también a nivel mundial[31]. Esta regulación también se encuentra en proceso de reforma con el fin de hacer frente a los nuevos desarrollos y garantizar una efectiva protección de la privacidad en el marco del devenir tecnológico.

Otra de las claves internacionales – aunque no vinculante – es el Documento sobre privacidad y protección los datos conocido como las Directrices de la OCDE sobre la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 1980[32]. Estas directrices y el trabajo posterior de la OCDE han inspirado a numerosas organizaciones internacionales, regionales y reglamentos nacionales sobre privacidad y protección

27 Gov.track.Us.- Video Voyeurism Prevention Act. Disponible en:

http://www.govtrack.us/congress/bills/108/s1301 (visitado el 2/02/2014).

28 Consejo de Europa.- Convention for the protection of individual with regard to automatic processing of personal data. Disponible en:

http://conventions.coe.int/treaty/en/treaties/html/108.htm (visitado el 2/02/2014).

29 Uruguay ha sido el primer país en incorporarse al sistema del Convenio Nº 108 fuera de la Unión Europea. Esto fue efectuado por Ley Nº 19.030, de 27 de diciembre de 2012.

30 Disponible en:

http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm

(visitado el 2/02/2014).

31 Ejemplo de ello son las normas aprobadas por ejemplo en Uruguay y Argentina.

32 OECD.- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 1980. Disponible en:

http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

(visitado el 2/02/2014).

de datos. Hoy en día, prácticamente todos los países que integran esta organización han promulgado leyes de privacidad y poseen institucionalidad encabezada por autoridades facultadas para hacerlas cumplir.

Aunque los principios de las directrices de la OCDE han sido ampliamente aceptados la principal diferencia está en la forma de implementación, en particular entre los enfoques europeos y estadounidenses.

En Europa la legislación de protección de datos es muy completa y exigente centrándose principalmente en el carácter de derecho fundamental de la misma, mientras que en los EEUU se desarrolla la regulación de privacidad en forma particular para cada sector de la economía incluyendo la privacidad financiera (Graham-Leach- Bliley Act), la privacidad de los niños[33] (Children´s Online Privacy Protection Act)[34] y la privacidad médica (Health Insurance Portability and Accountability Act)[35], entre otros.

Otra diferencia importante es que, en Europa, la legislación sobre privacidad se aplica por las autoridades públicas, mientras que la aplicación en EEUU descansa principalmente en el sector privado y la autorregulación. Las empresas establecen políticas de privacidad, generando códigos de conducta que aplican hacia el interior de sus empresas. En términos generales, depende de cada una de las empresas y de las propias personas la decisión sobre las políticas de privacidad a aplicar.

La principal crítica del enfoque de los EEUU es que las personas se ubican en una posición relativamente débil, ya que rara vez son conscientes de la importancia de las opciones ofrecidas por las políticas de privacidad y carecen de información real y efectiva en relación con la importancia de la protección de sus datos personales.

2.8.5 Acuerdo de safe harbour entre los EEUU y la Unión Europea

Estos dos enfoques – EEUU y la UE – en relación con la protección de los datos personales han entrado en conflicto. El principal problema radica en el uso de los datos personales por parte de las empresas. En este sentido, las preguntas se suceden y se refieren fundamentalmente a cómo puede la UE imponer sus regulaciones sobre, por ejemplo, una compañía de software con sede en EEUU o cómo puede la UE garantizar que los datos de sus ciudadanos están protegidos de acuerdo con las reglas especificadas en la Directiva sobre Protección de Datos, de acuerdo con qué normativa serán transferidos los datos, que se circulan a través de la red de una empresa de la UE a una que se maneja en los EEUU.

La UE amenazó con bloquear la transferencia de datos a cualquier país que pudiera no garantizar el mismo nivel de protección de privacidad que estableció en su Directiva.

Esta situación llevó inevitablemente a un choque con el enfoque de autorregulación

33 Graham-Keach-Bliley Act.- Disponible en: http://www.ftc.gov/privacy/glbact/glbsub1.htm (visitado el 2/02/2014).

34 Children's Online Privacy Protection Act.- Disponible en: http://www.ftc.gov/ogc/coppa1.htm (visitado el 2/02/2014).

35 Health Information Privacy.- Disponible en: http://www.hhs.gov/ocr/privacy/ (visitado el 2/02/2014).

de EEUU.

Esta diferencia profundamente arraigada ha hecho muy dificultoso el desenvolvimiento de acuerdos entre éstos.

Por otra parte, el ajuste de la ley de EEUU a la Directiva de la UE no habría sido posible, ya que habría requerido el cambio de algunos principios importantes del sistema normativo de los EEUU.

Se produjo un gran avance en medio del estancamiento que se verificaba, cuando el Embajador Aaron de EEUU sugirió en 1998 una fórmula de "puerto seguro" ya que esto replanteaba todo el tema.

Esta solución implicó que las regulaciones de la UE podrían ser aplicadas a las empresas de EEUU dentro de un puerto seguro y con regulación legal. Las empresas estadounidenses manejaban información de ciudadanos de la UE y éstos podrían firmar voluntariamente su consentimiento para el tratamiento de sus datos de acuerdo con los requisitos de protección de la privacidad de la UE. Después de haber firmado estos acuerdos, las empresas debieron observar el cumplimiento formal de los mecanismos acordados entre la UE y los EEUU.

Cuando se firmó en 2000 el Acuerdo de puerto seguro la noticia fue recibida con una gran esperanza en la medida que se consideró como la herramienta normativa que podría resolver problemas similares con otros países. Sin embargo, la situación no ha sido muy alentadora.

El Parlamento Europeo ha criticado esta opción por entender que no se trata de una protección suficientemente fuerte para los ciudadanos de la UE. Las compañías estadounidenses no han sido particularmente entusiastas en relación con el uso de este enfoque.

3. GOBERNANZA DE INTERNET PARA EL DESARROLLO HUMANO: COMPONENTES SOCIO - CULTURALES

3.1. Derechos humanos

El conjunto básico de derechos humanos relacionados con Internet incluye los derechos a la privacidad, la libertad de expresión, el derecho a recibir información, la protección de varios derechos culturales, la lingüística y la diversidad de minorías, y el derecho a la educación.

No es de extrañar que los temas relacionados con los derechos humanos hayan sido muy a menudo objeto de acalorados debates tanto en los procesos de la Cumbre Mundial de la Sociedad de la Información cuanto en los de IGF (Internet Governance Forum).

Si bien los derechos humanos por lo general se abordan explícitamente, también están involucrados en los temas transversales que aparecen cuando se tratan aquéllos

vinculados con la neutralidad de la red (derecho de acceso, libertad de expresión, el anonimato), la ciberseguridad (respeto de los derechos humanos en el ejercicio de actividades de protección de la seguridad cibernética) y el control de contenidos, entre otros. La Cumbre Mundial de la Sociedad de la Información ha reconocido específicamente en sus documentos la importancia de los derechos humanos, en particular el derecho al desarrollo y el derecho a la libertad de expresión.

3.1.1 Los derechos reales vs los derechos cibernéticos

Paralelamente al debate jurídico conceptual que analiza si una determinada normativa se verifica actualizada y alcanza suficientemente para ser aplicada a las regulaciones de Internet o si hay una necesidad de nueva normatividad, mucho se ha debatido en los círculos de derechos humanos acerca de si los conceptos tradicionales vinculados con éstos deben ser revisados con vistas a su utilización en Internet. La APC (Association for Progressive Communication) sostiene que los derechos humanos relacionados con Internet están fuertemente plasmados en el sistema de derechos humanos de las Naciones Unidas sobre la base de la Declaración Universal de Derechos Humanos.

Esta visión determina que los derechos humanos son los mismos en el mundo cibernético que en el mundo real. Las especificidades online de los derechos humanos están relacionadas con su aplicación.

Uno de los principales actores en el campo de los derechos humanos e Internet es el Consejo de Europa. Éste es la institución fundamental para el tratamiento de los derechos humanos en Europa, a partir del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales[36] en tanto éste es su principal instrumento. Desde 2003, el Consejo de Europa ha adoptado varias declaraciones destacando la importancia de los derechos humanos en Internet.[37] El Consejo de Europa es también el depositario de la Convención sobre Cibercrimen[38] como el principal instrumento mundial en este campo. Esto lo posiciona como una de las instituciones clave en encontrar el equilibrio adecuado entre el ser humano, sus derechos y las consideraciones de seguridad cibernética en los futuros desarrollos de Internet.

Asimismo es muy importante señalar que Finlandia es el primer país en garantizar normativamente el derecho de acceder a Internet. A partir de 2010 todos los ciudadanos

36 Consejo de Europa.- Convention for the Protection of Human Rights and Fundamental Freedoms. 2010. Disponible en: http://conventions.coe.int/treaty/en/treaties/html/005.htm (visitado el 2/02/2014).

37 El Consejo de Europa adoptó las siguientes declaraciones en relación con la relevancia de los derechos humanos e internet:

• La Declaración sobre la libertad de las comunicaciones en Internet, de 28 de mayo de 2003. Disponible en: https://wcd.coe.int/ViewDoc.jsp?id=37031 (visitado el 2/02/2014).

• Declaración sobre Derechos Humanos y Estado de Derecho en la Sociedad de la Información, de 13 de mayo de 2005. Disponible en:

https://wcd.coe.int/ViewDoc.jsp?id=849061 (visitado el 2/02/2014).

• Declaración sobre la Agenda Digital Europea, de 29 de setiembre de 2010. Disponible en: https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2829.09.2010_1%29&Language=lanEnglish&Ver=original (visitado el 2/02/2014).

38 Consejo de Europa.- Convención sobre Cibercriminalidad. Ob. Cit.

de Finlandia tienen el derecho a una conexión de banda ancha de un megabit[39].

No obstante, el derecho de acceso a Internet se sostiene más en relación con la libertad de expresión y la información, aunque, también es importante la velocidad real de la conexión a Internet.

Sin embargo, hay opiniones reticentes a considerar la banda ancha como un derecho humano básico, cuando hay personas que todavía luchan por el agua limpia, la atención médica y los alimentos.

3.1.2 La libertad de expresión y el derecho a buscar, recibir y difundir información

La libertad de expresión en línea figura en la agenda diplomática desde 2011/2012, y particularmente en la agenda del Consejo de Derechos Humanos de Naciones Unidas.

La libertad de expresión en Internet también se ha debatido en numerosas conferencias internacionales. El debate sobre la libertad de expresión en línea ha sido un área muy específica que se ha tratado a nivel político en mérito a sus más que trascendentes consecuencias. Éste es un derecho fundamental, y por lo general aparece en el centro de los debates sobre el control de contenidos y la censura. En la Declaración Universal de los Derechos Humanos de la ONU[40], la libertad de expresión (artículo 19) es contrarrestado por el derecho del Estado a limitarla en razón de la moralidad, el orden público y el bienestar general (artículo 29).

3.1.3 Derecho de acceso a Internet

Es importante tener en cuenta que limitar la libertad de expresión en aras de la moral, del orden público, y en general, el bienestar es algo complejo de decidir y más aún de ejecutar. Así, tanto el debate como la aplicación del artículo 19 deben ser puestos en el contexto del establecimiento de un equilibrio adecuado entre dos necesidades. Esta situación ambigua abre muchas posibilidades para diferentes interpretaciones de las disposiciones normativas y en última instancia, las distintas aplicaciones son las que generan controversia en torno a una ponderación adecuada entre los artículos 19 y 29 en la realidad mundial que se refleja en las discusiones acerca de la consecución de este equilibrio en Internet.

La libertad de expresión es el enfoque particular de las organizaciones no gubernamentales de derechos humanos, como Amnistía Internacional y Freedom House, Human Rights Watch, entre otras. De hecho es interesante considerar un estudio realizado por Freedom House donde se evalúa el nivel de penetración de Internet y de los teléfonos móviles para verificar la incidencia que éstos tienen para la libertad promedio experimentada por los usuarios en una muestra de 15 países de 6 regiones. Cubriendo los años

39 CNN Tech.- First nation makes broadband access a legal right. 2010. Disponible en:
http://articles.cnn.com/2010-07-01/tech/finland.broadband_1_broadband-access-internet-access-universal-service?_s=PM:TECH (visitado el 2/02/2014).

40 Declaración Universal de Derechos Humanos. Disponible en:
http://www.un.org/en/documents/udhr/ (visitado el 2/02/2014).

2007 y 2008, el estudio aborda una serie de factores que podrían afectar dicha libertad, incluyendo el estado de la infraestructura de las telecomunicaciones, las restricciones gubernamentales al acceso a la tecnología, la reglamentación marco para proveedores de servicios, la censura y el control de los contenidos, el entorno jurídico, la vigilancia y los ataques extralegales sobre los usuarios o contenidos.

Los indicadores seleccionados reflejan no sólo las acciones de los gobiernos sino también el vigor, la diversidad y el activismo del nuevo dominio de los medios de comunicación en cada país, independientemente de los esfuerzos estatales para restringirla[41].

3.2. Política de contenidos

Una de las principales cuestiones socioculturales es la política de contenidos. A menudo, ésta está dirigida desde el punto de vista de los derechos humanos y encabezada por la libertad de expresión y los derechos a la información y comunicación. Pero muchas veces con contralores de parte del gobierno a los efectos de desarrollar control de contenidos, e incluso restricciones de índole tecnológica vinculadas con las herramientas para llevar a cabo estos contenidos.

Los debates se centran generalmente en tres grupos:

a.- El contenido que tiene un consenso mundial para su control. Se incluyen aquí los derechos de los niños, la pornografía, la justificación del genocidio y la incitación a la organización de actos terroristas, todos prohibidos o reconocidos por el derecho internacional.

b.- El contenido que es sensible a determinados países, regiones o grupos étnicos debido a sus valores religiosos y culturales particulares. La globalización en línea plantea retos para la comunicación de los valores locales, culturales y religiosos en muchas sociedades. El mayor control de contenido se efectúa en Oriente Medio y los países asiáticos, justificándose oficialmente por la protección de los valores culturales específicos. Esto a menudo significa que el acceso a sitios web pornográficos y de azar está bloqueado[42].

c.- Censura política en Internet. Reporteros sin Fronteras está constantemente monitoreando el estado de la libertad de información en Internet y para el año 2013 enumeró trece países como "Enemigos de Internet"[43].

Ahora bien, cómo se lleva a cabo la política de contenido.

41 Freedom House.- "*Freedom on the Net. A Global Assessment of Internet and Digital Media*". Disponible en:
http://www.freedomhouse.org/sites/default/files/Freedom%20OnThe%20Net_Full%20Report.pdf
(visitado el 2/02/2014).

42 Girdwood, Scott.- "*Place your bets ... on the keyboard: Are Internet casinos legal*?". Campbell Law Review Nº 25. 2002. Disponible en:
http://scholarship.law.campbell.edu/cgi/viewcontent.cgi?article=1398&context=clr
(visitado el 2/02/2014).

43 Reporteros sin Fronteras.- El reporte completo correspondiente a 2013 está disponible en http://en.rsf.org/list-of-the-13-internet-enemies-07-11-2006,19603 (visitado el 12/03/2015).

Se verifica la existencia de una serie de temáticas que están presentes para la política de contenidos que presenta una serie de opciones legales y técnicas, que se utilizan en distintas combinaciones.

- Filtrado de contenido gubernamental

Los gobiernos que filtran el acceso a los contenidos por lo general crean un "índice de Internet" en el que se establecen los sitios web bloqueados para el acceso ciudadano. El filtrado de contenido se produce en muchos países, – cantidad que va en aumento – además de los ampliamente reconocidos en este tipo de prácticas – China, Arabia Saudita, Singapur –.

- Los sistemas de clasificación y filtrado privado

Ante el riesgo potencial de la desintegración de Internet a través del desarrollo de diversas barreras nacionales (sistemas de filtración), W3C y otras instituciones de ideas afines tomaron medidas proactivas que proponen la implementación de una calificación controlada por el usuario y los sistemas[44]. En estos sistemas, los mecanismos de filtrado pueden ser implementados por un software colocado en ordenadores personales o verificar control a nivel del acceso al servidor de Internet.

- El filtrado de contenidos basado en la ubicación geográfica

Otra solución técnica en relación con los contenidos es un software de localización geográfica, que establece filtros de acceso a determinados contenidos web de acuerdo con las características geográficas o nacionales de origen de los usuarios.

Las compañías de software de localización geográfica afirman que pueden identificar el país de origen sin error y la ciudad en aproximadamente el 85 % de los casos, especialmente si se trata de una gran ciudad[45]. Desde el caso de Yahoo! en 2000[46], la precisión de geo - localización ha aumentado aún más mediante el desarrollo de software de geo - ubicación sofisticada.

- Control de contenido a través de motores de búsqueda

El puente entre el contenido del usuario final y la Web suele ser un motor de búsqueda. Las autoridades chinas iniciaron uno de los primeros ejemplos de control de contenido a través de motores de búsqueda[47].

44 Resnick, Paul, Miller, James.- "*PICS: Internet Access Controls Without Censorship*". 1996. Disponible en: http://www.w3.org/PICS/iacwcv2.htm (visitado el 2/02/2014).

45 Akami afirma que puede identificar la ubicación geográfica de las personas a partir de sus códigos postales. Éste es el límite tecnológico. La información acerca de las direcciones de la calle no se puede obtener de números IP. Silicon Valley Quova Inc., uno de los principales proveedores de esta tecnología, afirma que puede identificar correctamente el país del usuario de la computadora en un 98 por ciento de las instancias y la ciudad en cerca del 85 por ciento de las veces, pero sólo si se trata de una gran ciudad. Estudios independientes han fijado el índice de precisión de este tipo de programas, que también se venden por empresas como InfoSplit, Digital Envoy, NetGeo y Akami, de 70 a 90 por ciento.

46 Se determinó la posibilidad de conocimiento de acceso de los usuarios a un sitio alojado por Yahoo!, vinculado a propaganda de exaltación del ideario nazi en Francia.

47 Si los usuarios introducen palabras prohibidas en Google Search, pierden su conectividad durante unos minutos. La respuesta del Departamento de Información chino establece: "... es bastante normal con algunos de los sitios de Internet que a veces se puede acceder a ellos y, a veces no se puede. El Ministerio no ha recibido información acerca de que Google esté bloqueado. El filtrado de búsquedas fue una fuente de tensión entre Google y las autoridades chinas que culminó

El peligro de filtrado de los resultados de búsqueda, sin embargo, no viene sólo de la esfera gubernamental; los intereses comerciales pueden interferir también, en forma más o menos obvia y penetrante. Algunos autores han comenzado a cuestionar el papel de los motores de búsqueda - especialmente de Google, considerando su posición dominante en las preferencias de los usuarios - en la mediación de acceso de los usuarios a la información y para advertir sobre su poder de influir en el conocimiento y preferencias de los usuarios.

4. COLOFÓN

Como afirmación definitiva y concluyente es posible sostener que las aristas son múltiples, los centros de interés variados pero el elemento común lejos de ser la tecnología, lo es la persona y sus derechos, desde las diferentes perspectivas y centralidades.

En la medida que el centro de la acción pública es la persona, el individuo humano no puede ser entendido como un sujeto pasivo, mero receptor o destinatario de las decisiones políticas. Como bien se ha destacado, "definir a la persona como centro de la acción pública significa no sólo, ni principalmente, calificarla como centro de atención sino, sobre todo considerarla la protagonista por excelencia de la vida política. Aquí se encuentra una de las expresiones más acabadas de lo que entiendo por buen gobierno, por buena administración en el marco democrático ... Afirmar que la libertad de los ciudadanos es el objetivo primero de la acción política significa, en primer lugar, perfeccionar, mejorar los mecanismos constitucionales, políticos y jurídicos que definen el Estado de Derecho como marco de libertades. Pero en segundo lugar, y de modo más importante aún, significa crear las condiciones para que cada hombre y cada mujer encuentre a su alrededor el campo efectivo, la cancha, en la que jugar libremente su papel activo, en el que desarrollar su opción personal, en la que realizar creativamente su aportación al desarrollo de la sociedad en la que está integrado. Creadas esas condiciones, el ejercicio real de la libertad depende inmediata y únicamente de los propios ciudadanos, de cada ciudadano. El buen gobierno, la buena administración ha de mirar precisamente la generación de ese ambiente en el que cada ciudadano pueda ejercer su libertad en forma solidaria."[48]

con la decisión adoptada por Google en enero de 2010 para redirigir búsquedas realizadas en Google.cn a sus servidores basados en Hong Kong. Sin embargo, más tarde ese año, Google invirtió su decisión bajo la presión de la negativa del gobierno chino para renovar su contenido del proveedor de licencias de Internet.

48 Delpiazzo, Carlos.- "*Marco conceptual de la gobernanza con especial referencia a Internet*". Ponencia preparada para el XII Congreso Iberoamericano de Derecho e Informática. Zaragoza, 2008.