# GOBERNANZA DE INTERNET

## ASUNTOS, ACTORES Y BRECHAS

*Jovan Kurbalija • Eduardo Gelbstein*

# GOBERNANZA DE INTERNET

## ASUNTOS, ACTORES Y BRECHAS

*Jovan Kurbalija • Eduardo Gelbstein*

ISBN Number: 99932-53-11-1

Publicado por DiploFoundation y la Sociedad para el Conocimiento Mundial

**DiploFoundation**
Malta: 4th Floor, Regional Building
Regional Rd.
Msida, MSD 13, Malta

Switzerland: DiploFoundation
Rue de Lausanne 56
CH-1202 Genève 21, Switzerland

Dirección de
Correo Electrónico: diplo@diplomacy.edu
Sitio web: http://www.diplomacy.edu

**Secretaría de la Sociedad para el Conocimiento Mundial (GKP)**
Level 23, Tower 2, MNI Twins
11, Jalan Pinang
50450 Kuala Lumpur, Malaysia

Dirección de
Correo Electrónico: gkps@gkps.org.my
Sitio web: http://www.globalknowledge.org

**Patrocinado por la Agencia Suiza para el Desarrollo y la Cooperación (COSUDE)**

Editado por Dejan Konstantinović y Steven Slavik
Ilustraciones de Zoran Marčetić – Marča
Diseño de Portada por Nenad Došen
Diagramación y preprensa Aleksandar Nedeljkov
Traducción al español por Ana María Piza, Communica Traducciones

# CONTENIDO

**Introducción**

Evolución de la Gobernanza de Internet . . . . . 8
Negociaciones Internacionales y la Gobernanza de Internet . . . . . 9
¿A qué se refiere la Gobernanza de Internet? . . . . . .11
Conjunto de Herramientas para la Gobernanza de Internet . . . . . 13
Enfoques y Patrones . . . . . 15
Principios Rectores . . . . . 21
Analogías . . . . . 25
Clasificación de la Gobernanza de Internet . . . . . 30
"Edificio en Construcción" . . . . . 33

**La Canasta de Infraestructura y Estandarización**

Introducción . . . . . 37
La Infraestructura de Telecomunicaciones . . . . . 38
Estándares y Servicios Técnicos (La Infraestructura de Internet) . . . . . 41
Protocolo para el Control de Transporte / Protocolo de Internet (TCP/IP) . .42
Sistema de Nombres de Dominio (DNS) . . . . . 46
Servidor raíz de Dominios . . . . . 51
Proveedores de Servicio de Internet (ISPs) . . . . . 53
Proveedores de Ancho de Banda para Internet (IBPs) . . . . . 54
Modelo Económico para la Conectividad en Internet . . . . . 56
Estándares Web . . . . . 59
Código Abierto . . . . . 60
Convergencia: Internet-Telecomunicaciones-Multimedios . . . . . 61
Seguridad en Internet . . . . . 63
Codificación . . . . . 67
Correo Electrónico Indeseado . . . . . 69

**La Canasta Legal**

Introducción . . . . . 75
Mecanismos Legales . . . . . 76
Legislación . . . . . 76
Normas Sociales (Costumbres) . . . . . 77
Autorregulación . . . . . 77
Jurisprudencia . . . . . 78
Regulación Internacional . . . . . 78
Jurisdicción . . . . . 80
Arbitraje . . . . . 85

Derechos de Propiedad Intelectual . . . . . 87
Marcas Registradas . . . . . 88
Derechos de Autor. . . . . 89
Patentes . . . . . 94
Cibercrimen . . . . . 95
Firmas Digitales . . . . . 97
Legislación Laboral . . . . . 99
Privacidad y Protección de Datos . . . . . 101

**La Canasta Económica**

Introducción . . . . . .111
Comercio Electrónico . . . . . .112
Protección del Consumidor . . . . . 115
Cargas Fiscales . . . . . .117
Aduanas . . . . . 118
Pagos Electrónicos: Banca Electrónica y Dinero Electrónico . . . . . 118

**La Canasta de Desarrollo**

Introducción . . . . . 125
La Brecha Digital . . . . . 127
Acceso Universal . . . . . 128
Estrategias para superar La Brecha Digital . . . . . 128
Desarrollo de Telecomunicaciones e Infraestructuras para Internet . . . . . 129
Apoyo Económico . . . . . 129
Aspectos Socioculturales . . . . . 130
Política y Regulación de Telecomunicaciones . . . . . 131

**La Canasta Sociocultural**

Introducción . . . . . 135
Política de Contenido . . . . . 135
Derechos Humanos . . . . . .141
Multiplicidad lingüística y Diversidad Cultural . . . . . 142
Bien Público Global . . . . . 143
Educación . . . . . 145

**Anexos**

"Los Ciegos y el Elefante" por John Godfrey Saxe. . . . . .151
Estudio sobre la Evolución en la Gobernanza de Internet . . . . . 152
Un Mapa para un Viaje a través de la Gobernanza de Internet . . . . . 154
El Cubo de Gobernanza de Internet de Diplo . . . . . 155

Sobre los Autores. . . . . 158

SECTION 1

# Introducción

*La Gobernanza de Internet no es un tema sencillo. Aunque trata con un símbolo importante del mundo DIGITAL, no puede ser manejada con una lógica digital – binaria de falso o verdadero y bueno o malo. Por el contrario, las muchas sutilezas y matices de significado y percepción del sujeto requieren un enfoque ANÁLOGO, que albergue un continuo de opciones y compromisos. Por lo tanto, este folleto no pretende brindar declaraciones definitiva sobre los temas relacionados con la Gobernanza de Internet. Su objetivo consiste en proponer un marco práctico para el análisis, la discusión y la resolución de los problemas clave que se presentan en este campo.*

# INTRODUCCIÓN

> En apenas unos pocos años, Internet ha revolucionado el comercio, la salud, la educación y, en efecto, la estructura misma de la comunicación y el intercambio humanos. Es más, su potencial es mucho mayor de lo que hemos percibido en el periodo relativamente corto desde su creación. Al administrar, promover y proteger su presencia en nuestras vidas, necesitamos ser tan creativos como aquellos que la inventaron. Claramente existe una necesidad de gobernanza, pero esto no necesariamente significa que debe llevarse a cabo del modo tradicional, ya que se trata de algo esencialmente diferente.
>
> Kofi Annan - Foro Global sobre la Gobernanza de Internet (Nueva York, 24 de Marzo de 2004)

En un periodo relativamente corto, Internet se ha convertido en un instrumento esencial para la sociedad moderna. Para mediados del 2005, se cree que Internet ya incluye:

- un estimado de 1,000 millones de usuarios a nivel global;
- una rotación en el comercio electrónico de US$ 150,000 millones, con un rápido crecimiento proyectado;
- un impacto social importante en la educación, la salud, el gobierno y otras áreas de actividad;
- ciberdelito, como fraude, apuestas, pornografía y suplantación;
- uso incorrecto y abuso en la forma de código malintencionado y correo electrónico indeseado.

Internet y las estadísticas no han sido siempre buenos compañeros. Desde los primero días de Internet, ha sido difícil identificar el número exacto de usuarios, anfitriones de sitios web, volumen de tráfico e información financiera, entre otros. Además, los números a menudo han sido utilizados para exagerar el crecimiento de Internet. Algunos investigadores atribuyen el desenlace del boom de las punto-com al uso de números inflados sobre el potencial de crecimiento de Internet.

La creciente conciencia del impacto social, económico y político de Internet en la sociedad nos brinda un enfoque más claro sobre el tema de la Gobernanza de Internet.

En el caso de Internet, la gobernanza se requiere entre otras cosas para:

- prevenir o, al menos minimizar, su riesgo de fragmentación;
- mantener la compatibilidad y la interoperabilidad;
- salvaguardar los derechos y definir las responsabilidad de las diferentes partes interesadas;
- proteger a los usuarios finales de la mala utilización y el abuso; motivar un mayor desarrollo.

El proceso de manejo de los asuntos legales así como las consecuencias sociales de los desarrollos tecnológicos invariablemente van a la zaga de la innovación tecnológica. Esto también se aplica a Internet.

Actualmente nos encontramos en la etapa inicial de las negociaciones internacionales sobre la Gobernanza de Internet, la cual se caracteriza por la necesidad de establecer y acordar un marco base y elegir instrumentos apropiados para la discusión de los muchos temas surgidos. ¿Quiénes son las partes interesadas con mayor probabilidad de influir en el desarrollo futuro de Internet? ¿Cuáles serán sus políticas con relación a conectividad, comercio, contenido, financiamiento, seguridad y otros temas fundamentales para nuestra emergente Sociedad de la Información? Estas son algunas de las preguntas clave que deben ser tratadas dentro del marco de la Gobernanza de Internet.

## LA EVOLUCIÓN DE LA GOBERNANZA DE INTERNET

Uno de los aspectos fascinantes de Internet durante su desarrollo y crecimiento iniciales era su modelo singular de gobernanza. Internet se inició como un proyecto gubernamental. A finales de la década de 1960, el gobierno de los Estados Unidos patrocinó el desarrollo de la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPANet por sus siglas en inglés), un servicio de comunicaciones flexible diseñado para sobrevivir en caso de un ataque nuclear.

En las páginas 140-141 se presenta un estudio detallado sobre la evolución de la Gobernanza en Internet.

Para la década de 1980, una comunidad internacional más amplia estaba ya utilizando las facilidades de esta red, la cual para ese momento ya era conocida como Internet. En 1986, se estableció la Fuerza de Tareas de Ingeniería para Internet (IETF por sus siglas en inglés). La IETF administró el sucesivo desarrollo de Internet por medio de un proceso de toma de decisiones cooperativo y consensual que involucraba a una

amplia variedad de individuos. No existía ni gobierno ni planificación central y no se contaba con un diseño maestro.

Hasta este punto, la vida era relativamente simple. Sin embargo, en 1994, la Fundación Nacional de las Ciencias de los Estados Unidos (NSF por sus siglas en inglés) decidió involucrar al sector privado subcontratando la administración del Sistema de Nombres de Dominio (DNS por sus siglas en inglés) a la empresa Network Solutions, Inc. (NSI). Este paso no fue bien recibido por la comunidad de Internet y dio inicio a la "Guerra del DNS".

Esta "Guerra del DNS" involucró a otras partes interesadas: el sector comercial, las organizaciones internacionales y los gobiernos de otras naciones. Esta guerra finalizó en 1998 con el establecimiento de una nueva organización, la Corporación de Internet para la Asignación de Nombres y Números (ICANN).

Desde 1998 y desde la incorporación de ICANN, el debate sobre la Gobernanza de Internet se ha caracterizado por una participación más intensiva de los gobiernos de diferentes naciones, especialmente a través del marco de las Naciones Unidas.

## NEGOCIACIONES INTERNACIONALES SOBRE LA GOBERNANZA DE INTERNET

La Cumbre Mundial de la Sociedad de la Información (CMSI), realizada en Ginebra en diciembre de 2003, colocó oficialmente el tema de la Gobernanza de Internet en las agendas diplomáticas. La Declaración de Principios y el Plan de Acción adoptados por la CMSI propone una serie de acciones en el campo de la Gobernanza de Internet, incluyendo el establecimiento de un Grupo de Trabajo sobre Gobernanza de Internet (GTGI).

A continuación presentamos un extracto sobre Gobernanza de Internet tomado de la Declaración de Principios de la WSIS:

> 50. Los temas relacionados con la Gobernanza Internacional de Internet deben ser tratados de forma coordinada. Le pedimos al Secretario General de las Naciones Unidas que estableciera un grupo de trabajo sobre Gobernanza de Internet con un proceso abierto e inclusivo que garantice un mecanismo para la total y activa participación de los gobiernos, el sector privado y la sociedad civil tanto

de países desarrollados como en vías de desarrollo, y que involucre organizaciones y foros intergubernamentales e internacionales relevantes, con el fin de investigar y realizar propuestas de acción para el año 2005, según corresponda, sobre la gobernanza de Internet.

A continuación presentamos un extracto sobre Gobernanza de Internet tomado del Plan de Acción de CMSI:

> 13. b) Le pedimos al Secretario General de las Naciones Unidas que estableciera un grupo de trabajo sobre Gobernanza de Internet con un proceso abierto e inclusivo que garantice un mecanismo para la total y activa participación de los gobiernos, el sector privado y la sociedad civil tanto de países desarrollados como en vías de desarrollo, y que involucre organizaciones y foros intergubernamentales e internacionales relevantes, con el fin de investigar y realizar propuestas de acción para el año 2005, según corresponda, sobre la gobernanza de Internet. El grupo debe, inter alia:
>
> i. desarrollar una definición operacional de Gobernanza de Internet;
> ii. identificar los temas de política pública relevantes para el Gobierno de Internet;
> iii. desarrollar un entendimiento común de los roles y responsabilidades respectivos de los gobiernos, organizaciones intergubernamentales e internacionales existentes y otros foros, así como del sector privado y de la sociedad civil tanto en países desarrollados como en vías de desarrollo;
> iv. preparar un reporte sobre los resultados de esta actividad a ser presentado para consideración y toma de acción correspondiente durante la segunda fase de la CMSI en Túnez en 2005.

La CMSI y el GTGI probablemente lleven a cabo la primera fase del proceso de Gobernanza de Internet, que como resultado produciría la clarificación de los asuntos relacionados con Gobernanza de Internet, el establecimiento de una agenda, así como la introducción de procedimientos y mecanismos.

**El Proceso de Negociaciones Multilaterales y la Gobernanza de Internet**

| FASE DE NEGOCIACIÓN | ACTIVIDAD DE LA CMSI |
|---|---|
| Negociación Previa | Desde 1998 hasta la CMSI en Ginebra (2003) |
| Preparación de una Agenda y Clarificación de los Asuntos | Se inició en Diciembre 2003 durante la CMSI en Ginebra con la decisión de establecer el Grupo de Trabajo sobre Gobernanza de Internet (GTGI); El GTGI presentó su reporte en junio de 2005; Esta fase del proceso se concluirá en Túnez. |
| La Búsqueda de Fórmulas | Después de Túnez 2005. |
| Negociación de los detalles | |
| Acuerdo | |
| Implementación | |

## ¿A QUÉ SE REFIERE LA GOBERNANZA DE INTERNET?

Durante el Foro Global sobre Gobernanza de Internet, realizado en las Naciones Unidas en Nueva York del 24 al 25 de marzo de 2004, varios conferencistas presentaron diferentes versiones de la historia de los ciegos y el elefante.

La moraleja del poema establece claramente que una discusión sobre el significado de "Gobernanza de Internet" no es meramente pedantería lingüística. Diferentes percepciones del significado de este término, generan diferentes enfoques y expectativas para las políticas.

Había una vez seis hombres del Indostán
Muy Inclinados al aprendizaje,
Que fueron a conocer al Elefante
(Pero todos ellos eran ciegos),
.....
Y estos hombres del Indostán
Discutieron largo y tendido,
Cada uno con su propia opinión,
Sumamente rígida y firme,
Y aunque todos tenían algo de verdad,
Todos estaban equivocados!

Traducción de un pasaje del poema "The Blind Men and the Elephant" escrito por el poeta estadounidense John Godfrey Saxe (1816-1887), el texto completo se encuentra disponible en el Anexo I

Los especialistas en telecomunicaciones ven la Gobernanza de Internet a través del prisma del desarrollo de la infraestructura técnica. Los especialistas en computación se enfocan en el desarrollo de varios estándares y aplicaciones, como XML o Java. Los especialistas en comunicaciones hacen hincapié en la facilitación de la comunicación. Los activistas en derechos humanos ven la Gobernanza de Internet desde la perspectiva de la libertad de expresión, la privacidad y otros dere-

chos humanos básicos. Los abogados se concentran en la jurisdicción y la resolución de disputas. Los políticos a nivel mundial usualmente se enfocan en los medios y los asuntos que combinan bien con sus electorados, como el optimismo tecnológico (más computadoras = más educación) y las amenazas (seguridad para Internet, protección de los menores). Los diplomáticos se preocupan principalmente por los procesos y la protección de los intereses nacionales. La lista de perspectivas profesionales potencialmente conflictivas sobre la Gobernanza de Internet continúa.

La CMSI ha producido la siguiente definición operacional de la Gobernanza de Internet: La "Gobernanza de Internet es el desarrollo y aplicación de principios, normas, reglas, procedimientos para la toma de decisiones y programas comunes por parte de Gobiernos, el sector privado y la sociedad civil con el fin de dar forma a la evolución y uso de Internet."
Esta definición operacional ofrece un buen punto de arranque para el debate sobre la Gobernanza de Internet, el cual inevitablemente delineará con mayor precisión ambos términos clave: "Internet" y "Gobernanza".

Cada uno de los términos "Internet" y "gobernanza" son el objeto de controversiales interpretaciones. Algunos autores discuten que la primer parte, "Internet", no cubre todos los aspectos existentes de los desarrollos globales en Tecnologías de la Información y las Comunicaciones (TIC). Otros dos términos: "Sociedad de la Información" y "Tecnologías de las Infocomunicaciones" usualmente se aceptan como más integrales. Estos términos incluyen áreas que se encuentran más allá del dominio de Internet, como la telefonía móvil.

Sin embargo, el argumento para el uso del término "Internet", se amplía con la rápida transición de las telecomunicaciones globales hacia el uso de TCP/IP como el principal estándar técnico de comunicaciones. La ya omnipresente Internet continúa expandiéndose a un ritmo acelerado, no solamente en términos del número de usuarios, sino también en cuanto a los servicios que ofrece, particularmente el Protocolo de Voz sobre Internet (VoIP), que podría llegar a desplazar la telefonía convencional.

La segunda parte, el término "gobernanza" ha sido motivo de controversia en debates recientes, especialmente durante la CMSI. El malentendido surge principalmente del uso del término gobernanza como sinónimo de gobierno. Cuando el término "Gobernanza de Internet" fue introducido en el proceso de la CMSI, muchos países, especialmente aquellos en vías de desarrollo, relacionaron el término con el concepto de gobierno. Una de las consecuencias de este enfoque fue la creencia de que los temas relacionados con la Gobernanza de Internet deben ser tratados a

nivel intergubernamental con la intervención limitada de otras partes interesadas, principalmente no estatales.

¿Cuáles fueron los principales motivos de esta confusión de términos? ¿Resulta obvio que "gobernanza" no significa "gobierno"? No necesariamente. El término "buena gobernanza" ha sido utilizado por el Banco Mundial para promover la reforma de los estados introduciendo una mayor transparencia, reduciendo la corrupción y aumentando la eficiencia de la administración. En este contexto, el término "gobernanza" está directamente relacionado con las funciones principales del estado.

Otra fuente potencial de confusión es la traducción del término "gobernanza" a otros idiomas. En Español, el término se refiere principalmente a actividades públicas o gobierno (gestión pública, gestión del sector público y función de gobierno). La referencia a actividades públicas o gobierno también es evidente en Francés (gestion des affaires publiques, efficacité del'administration, qualité del'administration y mode de gouvernement). El Portugués sigue un patrón similar al referirse al sector público y al gobierno (gestão pública y administração pública). Esta discrepancia en la interpretación del término "gobernanza" podría brindar una explicación lingüística al hecho de que múltiples delegaciones en la CMSI relacionaran el tema de la Gobernanza de Internet con el sector público, y centraran sus deliberaciones en la necesidad de contar con intervención gubernamental.

## CONJUNTO DE HERRAMIENTAS PARA LA GOBERNANZA DE INTERNET

El régimen de Gobernanza de Internet se encuentra en las etapas más tempranas de su desarrollo. La experiencia de otros regímenes internacionales (p. ej. ambiente, transporte aéreo, control de armamento) ha demostrado que estos regímenes tienden a desarrollar un marco común de referencia, valores, percepción de relaciones de causa y efecto, modos de razonamiento, terminología, vocabulario, jerga y abreviaturas.

En muchos casos, el marco común se encuentra influenciado por la cultura profesional específica (los patrones de conocimiento y comportamiento comunes de los miembros de una misma profesión). El establecimiento de un marco común usualmente ayuda a facilitar una mejor comunicación y comprensión. Sin embargo, en ocasiones también se utiliza para proteger el "terreno" propio y prevenir las influen-

cias externas. Citando al lingüista estadounidense Jeffrey Mirel, "Todo lenguaje profesional es leguaje territorial".

Cualquier régimen de Gobernanza de Internet será complejo ya que requiere involucrar muchos asuntos, partes interesadas, mecanismos, procedimientos e instrumentos. Existen al menos cinco dimensiones de asuntos en el caso de Internet: de Infraestructura, Legales, Económicos, de Desarrollo y Socioculturales. Cada uno de ellos se discute en detalle en los capítulos siguientes. Una variedad de partes interesadas del sector privado y público juegan roles en cada una de estas dimensiones. La mayoría de ellos (operadores de servidores raíz, ISPs, abogados de marcas registradas, especialistas en desarrollo, activistas de la sociedad civil, etc.) cuenta ya con culturas profesionales muy específicas y bien desarrolladas.

Cada combinación de asuntos y partes interesadas tiene un propósito, objetivo, terminología y esfera de colaboración e influencia. Aparentemente muchas, sino la mayoría, de estas combinaciones están operando en relativo aislamiento de las demás. Si agregamos a esto la multiplicidad de lenguajes operacionales que reflejan la naturaleza global de los problemas, tendremos claro el desafío de unir estos elementos y constituir una arquitectura de gobernanza coherente que pueda ser manejable gracias a la buena voluntad de las partes involucradas.

La siguiente ilustración, inspirada por el artista holandés M.C. Escher, demuestra algunas de las perspectivas paradójicas asociadas con la Gobernanza de Internet.

La complejidad de implementar una Gobernanza de Internet demuestra que el pensamiento lineal, monocausal y de "uno u otro" no se adapta a los asuntos relacionados con este tema. Por lo tanto, existe la necesidad de encontrar nuevas herramientas cognitivas que atiendan esta complejidad e introduzcan enfoque comunes y principios rectores.

El propósito primordial de un conjunto de herramientas para la Gobernanza de Internet sería:

- organizar las herramientas utilizadas actualmente en el debate sobre la Gobernanza de Internet;
- desarrollar herramientas cognitivas adicionales;
- facilitar la naturaleza inclusiva del proceso de la Gobernanza de Internet brindado a las partes interesadas las herramientas para comprender los asuntos, perspectivas y desarrollos.

El Conjunto de Herramientas para la Gobernanza de Internet consiste en:

- patrones y enfoques;
- Principios Rectores;
- analogías.

Al igual que el proceso de Gobernanza de Internet, el conjunto de herramientas cambia continuamente. Los enfoques, patrones, principios rectores y analogías surgen y desaparecen dependiendo de su relevancia en un momento dado del proceso de negociación.

## ENFOQUES Y PATRONES

La Gobernanza de Internet como un todo, así como asuntos específicos relacionados con el tema, han sido parte de las discusiones de políticas y los intercambios académicos desde hace algún tiempo. Una serie de enfoques y patrones ha surgido gradualmente, representando los puntos en los cuales es posible identificar las diferencias en las posiciones de negociación, así como en las culturas profesionales y nacionales. La identificación de enfoques y patrones comunes puede reducir la complejidad de las negociaciones y contribuir a la creación de un sistema común de referencia.

### Enfoque Estricto versus Amplio

La Gobernanza de Internet "limitada versus amplia" ha sido uno de los principales asuntos hasta el momento y refleja los diferentes enfoques e intereses dentro del proceso. El enfoque "estricto" se concentra en la infraestructura de Internet (Sistema de Nombres de Dominio, números de IP y servidores raíz de dominio) y en la posición de ICANN como parte interesada clave en este campo.

Según el enfoque "amplio", las negociaciones de Gobernanza de Internet deben ir más allá de los asuntos de infraestructura y tratar otros asuntos legales, económicos, de desarrollo y socioculturales. La distinción entre estos dos enfoques es particularmente importante durante la fase inicial de fijación de una agenda para las negociaciones sobre Internet.

Según el enfoque "amplio", las negociaciones de Gobernanza de InEl enfoque amplio es implícitamente apoyado por la Declaración de la CMSI, que otorga al GTGI el mandato de "identificar asuntos de política pública que sean relevantes para la Gobernanza de Internet". Este enfoque también es predominante en discusiones políticas y académicas relacionadas con la Gobernanza de Internet.

El debate actual ha pasado del escenario de "uno u otro" hacia la identificación de prioridades y el balance apropiado entre el enfoque "estricto" (asuntos relacionados con ICANN) y el enfoque "amplio" (otros aspectos de la Gobernanza de Internet).

### Aspectos Técnicos versus Políticos

Un desafío importante en el proceso de Gobernanza de Internet será la integración de aspectos técnicos y políticos, ya que es difícil establecer la distinción entre ambos. Las soluciones técnicas no son neutrales. En última instancia, cada solución/opción técnica promueve ciertos intereses, faculta a ciertos grupos y, hasta cierto punto, tiene un impacto en la vida social, política y económica.

En algunos casos, el objetivo inicial de una política para una solución técnica ha variado. Por ejemplo, la arquitectura de Internet de redes punto a punto y conmutación de paquetes fue diseñada con el objetivo político de crear una red robusta que pudiera sobrevivir un ataque nuclear. La misma arquitectura se convirtió más adelante en el cimiento para el desarrollo de la creatividad y la libertad de expresión en Internet.

Otras soluciones técnicas, como los medios electrónicos para la protección de derechos de reproducción, han sido creadas intencionalmente para remplazar o imponer ciertas políticas (en este caso una protección más estricta de los derechos de reproducción).

En el caso de Internet, por mucho tiempo tanto los aspectos técnicos como de políticas fueron regidos por un solo grupo social – la primera comunidad de Internet. Con el crecimiento de Internet y el surgimiento de nuevas partes interesadas en la década de 1990, principalmente el sector comercial y gubernamental, se fragmentó esa unidad entre tecnología y política. La reforma de la Gobernanza de Internet, incluyendo la creación de ICANN, fue un intento por restablecer el balance perdido. Este tema permanece inconcluso, y es muy probable que constituya uno de los tópicos controversiales de la CMSI/GTGI.

### El Enfoque "Viejo y Real" versus el "Nuevo y Cibernético"

Existen dos enfoques que se aplican a casi cualquier asunto relacionado con la Gobernanza de Internet. El enfoque "viejo y real" – o "vino nuevo en botellas viejas" – discute que Internet no introduce nada nuevo al campo de la gobernanza. Internet es tan solo otro dispositivo nuevo y desde la perspectiva de la gobernanza, no presenta diferencias con sus predecesores: el telégrafo, el teléfono o la radio.

Por ejemplo, en discusiones legales, este enfoque establece que la legislación existente puede ser aplicada a Internet realizando ajustes menores. En el tanto involucre la comunicación entre personas, Internet no difiere del teléfono o el telégrafo y puede ser regulado como cualquier otro dispositivo de telecomunicaciones. En el campo económico, este enfoque discute que no existe diferencia entre el comercio regular y el comercio electrónico. Consecuentemente, no es necesario brindar un tratamiento legal especial al "comercio electrónico". El enfoque "verdadero" también se opone a las moratorias fiscales.

El enfoque "nuevo y cibernético" – o "vino nuevo en botellas nuevas" – discute que Internet es un dispositivo fundamentalmente diferente de todos los anteriores. Por lo tanto requiere una gobernanza fundamentalmente diferente. Este enfoque fue particularmente popular en los primeros días de Internet. Existía incluso la esperanza de que el innovador método utilizado inicialmente para gobernar Internet – "consenso básico y código funcional" – pudiera convertirse en un modelo para la regulación de otras áreas de la actividad humana. La principal

premisa del enfoque "cibernético" es que Internet desliga nuestra realidad social y política del mundo de los estados soberanos. El ciberespacio es diferente del espacio real y por lo tanto requiere una forma diferente de gobernanza.

La influencia de este enfoque fue notable en el proceso de creación de ICANN, que por ejemplo minimizó la influencia de los gobiernos del mundo "real". El enfoque "cibernético" fue suavizado por la reforma de ICANN de 2002, que fortaleció el rol de los gobiernos y atrajo un poco más a ICANN a la realidad política.


En el campo legal, la escuela "cibernética" de pensamiento discute que la legislación existente sobre la jurisdicción, el ciberdelito y los contratos, no puede ser aplicada a Internet y es necesario crear leyes nuevas.

Dada la interacción continua entre estos dos enfoques, el dilema entre el "viejo y real" y el "nuevo y cibernético" tiene probabilidades de continuar e influenciar fuertemente las negociaciones relacionadas con la Gobernanza de Internet.

### Estructura Descentralizada versus Centralizada para la Gobernanza de Internet

De acuerdo con la perspectiva descentralizada, la estructura de gobernanza debe reflejar la naturaleza misma de Internet: una red de redes. Esta compleja configuración no puede ser colocada bajo un solo paraguas de gobernanza, como sería una organización internacional. Otro argumento es que la falta de gobernanza centralizada es uno de los principales factores que permite el rápido crecimiento de Internet. Esta perspectiva es apoyada principalmente por la comunidad de Internet y los países desarrollados.

Por otro lado, el enfoque centralizado se basa parcialmente en la dificultad práctica que enfrentan los países con limitados recursos humanos y económicos para seguir las discusiones sobre Gobernanza de In-

ternet en un ambiente descentralizado que involucra a múltiples instituciones. Para estos países ya es de por sí difícil asistir a las reuniones en los principales centros diplomáticos (Ginebra, Nueva York), sin mencionar dar seguimiento a las actividades de otras instituciones como ICANN, el Consorcio del World Wide Web (W3C por sus siglas en inglés) e IETF. Estos países, principalmente en vías de desarrollo, piden que "todo se concentre en un mismo punto", preferiblemente dentro del marco de una organización internacional.

### Internet y el Bien Público

La mayor parte de la infraestructura técnica sobre la cual se canaliza el tráfico de Internet es propiedad de compañías privadas y estatales, típicamente operadores de telecomunicaciones. Esta situación es análoga a una empresa de transporte marítimo de contenedores. Sin embargo, los canales de navegación son abiertos y regulados por la Legislación Marítima que establece que los mares abiertos son res communis omnium, mientras que las redes troncales sobre las cuales se transporta los datos son propiedad de empresas de telecomunicaciones. Esto plantea una serie de preguntas:

- ¿Es posible pedir a las empresas privadas que manejen su propiedad privada – redes troncales – a favor de los intereses públicos? ¿Puede Internet o algunas de sus partes ser consideradas como bien público global?
- ¿Podrá el antiguo concepto romano res communis omnium ser aplicado a Internet, como en el caso de algunas partes de la Legislación Marítima?
- ¿Podrá el antiguo concepto romano res communis omnium ser aplicado a Internet, como en el caso de algunas partes de la Legislación Marítima?

El principal desafío de este dilema de lo público versus lo privado será, por un lado, brindar al sector privado un ambiente comercial apropiado y por otro, garantizar la continuación del desarrollo de Internet como recurso público constituido por conocimiento e información comunes. Para mayor información por favor consulte la página 131.

### Geografía e Internet

Una de las primeras percepciones de Internet fue que superaba las fronteras nacionales y erosionaba el principio de soberanía. En su fa-

mosa "Declaración de Independencia del Ciberespacio", John Perry Barlo envió el siguiente mensaje a todos los gobiernos nacionales: "Ustedes no son bienvenidos entre nosotros. Ustedes no ejercen soberanía en los lugares donde nos reunimos. Ustedes no tienen derecho moral de regirnos ni cuentan con métodos de coerción que efectivamente nos produzcan temor alguno. El Ciberespacio no está localizado dentro de sus fronteras".

Esta declaración es un ejemplo del optimismo técnico predominante a mediados de la década de 1990. Muchas cosas han sucedido desde la declaración de Barlow, incluyendo la creación de software de localización geográfica más sofisticado. Y aunque hoy en día todavía es difícil identificar con precisión quién está detrás de la pantalla, es relativamente fácil saber a través de cuál proveedor de servicios de Internet (ISP) se está estableciendo el acceso. Además, la legislación mundial más reciente requiere que los ISPs identifiquen a sus usuarios y, en caso de solicitud, que revelen a las autoridades información pertinente sobre ellos.

Entre mayor sea el anclaje de Internet en la geografía, menor singularidad implicará su gobernanza. Por ejemplo, al tener la posibilidad de localizar geográficamente a los usuarios y transacciones de Internet, la compleja cuestión de la jurisdicción de Internet puede resolverse con mayor facilidad por medio de los canales existentes.

### El Enfoque "Acciones más que Palabras"

El enfoque "acciones más que palabras" promueve el uso de herramientas en línea para la negociación de los asuntos relacionados con el mundo en línea. El proceso de negociación de la Gobernanza de Internet presenta un desafío considerable para la diplomacia multilateral que amerita el uso de técnicas de negociación ampliamente comprobadas y eficientes, así como la introducción de enfoques innovadores. Una de las principales técnicas innovadoras podría ser el uso de herramientas en línea para las negociaciones.

Las negociaciones basadas en Internet deben facilitar la participación de un grupo más amplio de interesados, especialmente aquellos que no pueden permitirse el lujo de participar en conferencias diplomáticas tradicionales. Una prioridad será asistir a los países en desarrollo para que participen de manera significativa en el proceso de Gobernanza de Internet.

## PRINCIPIOS RECTORES

Los principios rectores representan ciertos valores e intereses que deben ser promovidos a lo largo del régimen emergente de Gobernanza de Internet. Algunos de estos principios han sido adoptados por la CMSI, tales como la transparencia y la inclusión. Otros principios han sido introducidos, principalmente de forma tácita, durante las discusiones sobre Gobernanza de Internet.

### "No Reinventes la Rueda"

Cualquier iniciativa en el campo de Gobernanza de Internet debe partir de las regulaciones existentes, las cuales pueden ser divididas en tres amplios grupos:

a) aquellas inventadas para Internet (p. ej. ICANN);
b) aquellas que requieren ajustes considerables para poder tratar asuntos relacionados con Internet (p. ej. protección de marcas registradas, régimen tributario electrónico);
c) aquellas que pueden ser aplicadas a Internet sin requerir ajustes significativos (p. ej. protección de la libertad de expresión).

La utilización de las reglas existentes aumentaría significativamente la estabilidad legal y reduciría la complejidad en el desarrollo del régimen de Gobernanza de Internet.

### "¡Si no está descompuesto, no lo repares!"

La Gobernanza de Internet debe conservar la funcionalidad y robustez actual de Internet, y a la vez ser suficientemente flexible para adoptar cambios que aumenten las funcionalidades y la legitimidad. El consenso general reconoce que la estabilidad y funcionalidad de Internet debe ser uno de los principios rectores de su Gobernanza. La estabilidad de Internet debe ser preservada por medio del enfoque inicial de "código funcional", que involucra la introducción gradual de cambios debidamente probados en la infraestructura técnica.

Sin embargo, algunos actores se preocupan de que el uso del lema "si no está descompuesto, no lo repares" ofrezca inmunidad indiscriminada contra cambios en la Gobernanza actual de Internet, incluyendo cambios no necesariamente relacionados con la infraestructura técnica. Una solución es utilizarlo como criterio para la evaluación de decisiones específicas relacionadas con la Gobernanza de Internet (p. ej.

introducción de nuevos protocolos y cambios en los mecanismos de toma de decisiones).

### Gobernanza y Desarrollo de Internet

El debate actual sobre la Gobernanza de Internet resalta la gran importancia que tiene el desarrollo de los siguientes asuntos relacionados con el tema: cargos por interconexión, distribución de números de IP, inversión, protección de propiedad intelectual y promoción del comercio electrónico. El proceso de Gobernanza de Internet debe ser guiado por los objetivos generales de desarrollo de la CMSI y los Objetivos del Milenio de las Naciones Unidas.

### Promoción del Enfoque y la Priorización Holísticos

El enfoque holístico debe facilitar no solo el trato de los aspectos técnicos del desarrollo de Internet, sino también los temas legales, sociales, económicos y de desarrollo. Este enfoque debe considerar además la creciente convergencia de tecnologías digitales, incluyendo la migración de servicios de telecomunicaciones hacia protocolos de Internet.


„No poder ver el bosque a través de los árboles"

Las partes interesadas en las negociaciones de Gobernanza de Internet deben mantener un enfoque holístico, pero a la vez identificar temas dependiendo de sus intereses particulares. Ni los países desarrollados ni aquellos en vías de desarrollo constituyen grupos homogéneos. Entre los países en desarrollo hay diferencias considerables en las prioridades, niveles de desarrollo y preparación para informática (p. ej. desde países con infocomunicaciones avanzadas

como India, China y Brasil hasta los menos desarrollados como el África del sub-Sahara).

El enfoque y la priorización holísticos en la agenda de Gobernanza de Internet debe ayudar a los interesados, tanto en países desarrollados como en vías de desarrollo, a enfocarse en un conjunto particular de temas. Esto debería conducir hacia negociaciones más sustantivas, y posiblemente, menos politizadas. Los interesados deberían agruparse alrededor de asuntos en lugar de alrededor de las tradicionales líneas divisorias altamente politizadas (p. ej. desarrollado – en vías de desarrollo, gobierno – sociedad civil).

PRINCIPIOS RECTORES DE ICANN

El Libro Blanco de los Estados Unidos sobre Gobernanza de Internet (1998) especifica los siguientes principios rectores para el establecimiento de ICANN:

- Estabilidad; el funcionamiento de Internet no debe ser interrumpido, especialmente en la operación de sus estructuras clave, incluyendo los "dominios primarios".
- Competencia; es importante motivar la creatividad y la flexibilidad, ya que contribuirán al mayor desarrollo de Internet;
- Toma de decisiones; el nuevo sistema debe dar cabida a algunos de los principios y reglas iniciales de Internet, incluyendo la organización a nivel de las bases, la apertura, etc.;
- Representación; el nuevo marco debe dar cabida a las principales partes interesadas: tanto geográficas (diferentes países) como profesionales (diferentes comunidades profesionales).

### Convertir las Soluciones Técnicas Tácitas en Principios Explícitos de Políticas

Es una creencia común dentro de la Comunidad de Internet que algunos valores sociales, como la libre comunicación, se ven facilitados por la forma técnica en que Internet ha sido diseñada (el principio de "punto a punto"). Esta creencia podría conducir a la conclusión errónea de que las soluciones técnicas son suficientes para promover y proteger los valores sociales. Los más recientes desarrollos en Internet, como el uso de tecnologías de cortafuegos para restringir el flujo de información, comprueban que la tecnología puede ser utilizada de muchas maneras aparentemente contradictorias. Principios como la libre comunicación deben ser claramente establecidos a nivel de políticas y no tácitamente asumidos a nivel técnico.

### El Principio de la Neutralidad Tecnológica

Este principio se encuentra estrechamente ligado con el anterior. Según la neutralidad tecnológica, la política no debe depender de dispositivos tecnológicos o técnicos específicos. Por ejemplo, las regulaciones para la protección de la privacidad deben especificar lo que debe ser protegido (p. ej. datos personales, expedientes de salud) y no la forma en que debe ser protegido (p. ej. acceso a bases de datos, protección por medio de codificación).

La neutralidad tecnológica ofrece muchas ventajas para la gobernanza. Primero que nada, desvincula la gobernanza de cualquier tecnología en particular y la prepara para enfrentar los desarrollos tecnológicos futuros. Segundo, la neutralidad tecnológica es el principio regulador más apropiado para la futura convergencia de las principales tecnologías (telecomunicaciones, medios, Internet, etc.).

La Unión Europea ha introducido la neutralidad tecnológica como una de las piedras angulares de su política de telecomunicaciones. Aunque la neutralidad tecnológica es un principio claramente apropiado, es posible visualizar muchas dificultades en la transición que lleva de las regulaciones de telecomunicaciones existentes a las nuevas. Estas ya se han hecho obvias en áreas como Voz sobre IP.

### El Riesgo de Manejar la Sociedad por medio del Código de Programación

Un aspecto clave de la relación entre tecnología y política fue identificado por Lawrence Lessig, quien observó que con la creciente confianza depositada en Internet, la sociedad moderna podría terminar siendo regulada por código de software en lugar de leyes. Algunas funciones legislativas de los parlamentos y los gobiernos podrían ser asumidas de facto por empresas de computación y desarrolladores de software. Por medio de una combinación de software y soluciones técnicas podrían influenciar la vida en sociedades cada vez más informatizadas. Si realmente la sociedad se administrara por medio de código en lugar de leyes, la base de la organización política y legal de la sociedad moderna enfrentaría un desafío sustancial .

## ANALOGÍAS

> Aunque la analogía a menudo induce a error, es la cosa menos engañosa que tenemos
>
> *Samuel Butler*

La analogía nos ayuda a comprender nuevos desarrollos en términos de lo que ya conocemos. El establecimiento de paralelos entre situaciones pasadas y actuales, a pesar de sus riesgos, es un proceso mental clave en la legislación y la política. La mayoría de los casos legales relacionados con Internet se resuelven por medio de analogías.

El uso de analogías en la Gobernanza de Internet presenta algunas limitaciones importantes. Primero, Internet es un término amplio que cubre una variedad de servicios, incluyendo correo electrónico (refiérase a la analogía con telefonía), Web (refiérase a la analogía con servicios de difusión – televisión) y bases de datos (refiérase a la analogía con bibliotecas). Una analogía con cualquier sistema particular puede simplificar excesivamente la comprensión de Internet.

Segundo, la creciente convergencia entre diferentes servicios de telecomunicaciones y medios está desdibujando las diferencias tradicionales entre ellas. Por ejemplo, con la introducción de Voz sobre IP es cada vez más difícil establecer una clara distinción entre la telefonía e Internet.

A pesar de estos factores limitantes, la analogía sigue siendo poderosa y la única herramienta cognitiva disponible para la resolución de casos legales y el desarrollo de un régimen de Gobernanza de Internet. A continuación se discuten algunas de las analogías más frecuentes.

### Internet - Telefonía

*Similitudes*: Durante los primeros días de Internet, esta analogía era influenciada por el hecho de que el teléfono era utilizado para tener acceso vía módem. Además, se mantiene una analogía funcional entre la telefonía e Internet (correo electrónico y charla), ya que ambas son herramientas de comunicación directa e interpersonal.

Una analogía más reciente entre telefonía e Internet se enfoca en la posible utilización del sistema de numeración telefónica como solución para la organización del sistema de nombres de dominio.

*Diferencias:* Internet utiliza paquetes en lugar de circuitos (como el teléfono). A diferencia de la telefonía, Internet no puede garantizar ser-

vicios; solamente puede comprometerse a realizar "su mejor esfuerzo". Esta analogía resalta únicamente un aspecto de Internet: la comunicación por medio de correo electrónico o charla. Otras aplicaciones importantes de Internet, como World Wide Web, servicios interactivos, etc., no comparten elementos comunes con la telefonía.

*Utilizada por:* Aquellos que se oponen a la regulación del contenido en Internet (principalmente los Estados Unidos). Si Internet es análoga al teléfono, el contenido de la comunicación en Internet no puede ser controlado, como en el caso de la telefonía.

Esta analogía también es utilizada por aquellos que discuten que Internet debe ser regulada, al igual que otros sistemas de telecomunicaciones (p. ej. telefonía y correo tradicional), por autoridades nacionales y organizaciones internacionales como la UIT (Unión Internacional de Telecomunicaciones), con un rol coordinador.

**Internet - Correo Tradicional/Postal**

*Similitudes:* Existe una analogía en la función, específicamente en la entrega de mensajes. El nombre mismo, "correo electrónico", resalta su similitud.

*Diferencias:* Esta analogía cubre únicamente un servicio de Internet, el correo electrónico. Además, el servicio postal cuenta con una estructura mucho más elaborada entre el remitente y el destinatario del correo postal que los sistemas de correo electrónico, en los cuales la función intermedia es realizada por los ISPs o los proveedores de servicios de correo electrónico como Yahoo! o Hotmail.

*Utilizada por:* La Convención Postal Universal establece la siguiente analogía entre el correo postal y el correo electrónico: "el correo electrónico es un servicio postal que utiliza las telecomunicaciones para su transmisión". Esta analogía puede tener consecuencias en cuanto a la entrega de documentos oficiales, por ejemplo la recepción de una decisión judicial por medio de correo electrónico se consideraría una entrega oficial.

Las familias de soldados estadounidenses que fallecieron en Irak también han tratado de establecer una analogía entre el servicio postal (cartas) y el correo electrónico para obtener acceso al correo electrónico y las bitácoras web (blogs) privadas de sus seres queridos, alegando

que ellos deben tener la posibilidad de heredar el correo electrónico y blogs al igual que heredarían cartas y diarios.

Los ISPs han enfrentado dificultades en este asunto de tan alto contenido emocional. En lugar de aceptar la analogía entre las cartas y el correo electrónico, la mayoría de los ISPs ha negado el acceso con base en el acuerdo de privacidad previamente establecido con sus usuarios.

#### Internet - Televisión

*Similitudes:* La analogía inicial fue establecida debido a la similitud física entre computadoras y pantallas de televisión. Una analogía más sofisticada recurre al uso tanto de los medios – web y TV – como de la difusión.

*Diferencias:* Al igual que en el caso de la telefonía, el concepto de Internet es más amplio que el de la televisión. Aparte de la similitud entre una pantalla de computadora y una de televisión, entre ellas existen diferencias estructurales importantes. La televisión es un medio de difusión "uno a muchos", mientras que Internet facilita muchos tipos diferentes de comunicación (uno a uno, uno a muchos, muchos a muchos).

*Utilizada por:* Esta analogía es utilizada principalmente por quienes desean introducir un control más estricto del contenido en Internet. Desde su perspectiva, debido al poder que tiene Internet como medio masivo de comunicación similar a la televisión, el primero debería ser estrictamente controlado. El gobierno de los Estados Unidos pretendió utilizar esta analogía en el influyente caso "Reno vs. ACLU". Este caso fue estimulado por la Ley de Decencia en las Comunicaciones aprobada por el Congreso de los Estados Unidos, la cual establece un estricto control de contenido con el fin de prevenir la exposición de los niños a materiales pornográficos en Internet. La corte rehusó reconocer la analogía con la televisión.

#### Internet - Biblioteca

*Similitudes:* A menudo se percibe a Internet como un amplio repositorio de información y el término "biblioteca" es frecuentemente utilizado para describirla – "gigantesca biblioteca digital", "biblioteca cibernética", "la Biblioteca de Alejandría del siglo XXI", etc.

*Diferencias:* El almacenamiento de información y datos es solamente un aspecto de Internet, y existen diferencias considerables entre las bibliotecas e Internet:

a) las bibliotecas tradicionales buscan servir a individuos que residen en un sitio en particular (ciudad, país, etc.), mientras que Internet es global;
b) los libros, artículos y periódicos son publicados utilizando procedimientos para garantizar su calidad (editores). En Internet no hay editores;
c) Las bibliotecas se organizan utilizando esquemas específicos de clasificación, lo que permite a los usuarios localizar los libros que se encuentran en sus colecciones. Aparte de unos cuantos directorios como Yahoo! y Google, que cubren apenas una pequeña parte de la información disponible,en Internet no existe un esquema de clasificación similar;
d) aparte de las descripciones con palabras clave, los contenidos de una biblioteca (texto en los libros y artículos) no son accesibles hasta que el usuario tiene en su poder el libro en particular. El contenido de Internet está disponible inmediatamente por medio de los motores de búsqueda.

*Utilizada por:* Diferentes proyectos que buscan crear un sistema integral de información y conocimiento sobre temas en particular (portales, bases de datos, etc).

#### Internet – VHS, Fotocopiadora

*Similitudes:* Esta analogía se enfoca en la reproducción y diseminación de contenido (p. ej. textos y libros). Las computadoras han simplificado la reproducción por medio del proceso de "copiar y pegar". Esto ha hecho a su vez que la diseminación de información por medio de Internet sea mucho más simple.

*Diferencias:* La computadora tiene una función mucho más amplia que la reproducción de materiales, aunque la reproducción por sí misma es mucho más simple en Internet que utilizando un VHS o una fotocopiadora.

*Utilizada por:* Esta analogía fue utilizada en el contexto de la "Ley de Derechos de Reproducción para el Milenio Digital" (DMCA por sus siglas en inglés) que penaliza a las instituciones que contribuyen al irrespeto de los derechos de reproducción (desarrollo de software para re-

ducir las protecciones de derechos de reproducción, etc.). El argumento contrario en estos casos es que los desarrolladores de software, al igual que los fabricantes de aparatos de VHS o fotocopiado, no pueden predecir si sus productos serán utilizados ilegalmente. Esta analogía fue utilizada en casos contra los desarrolladores de software como el Napster, un sistema utilizado para compartir archivos entre pares, como Grokster y StreamCast.

#### Internet - Carretera

*Similitudes:* Esta analogía está ligada a la cultura estadounidense y la importancia que esta le asigna a las carreteras y ferrovías, revelando de este modo la fascinación nacional con el descubrimiento y las nuevas fronteras.

*Diferencias:* Aparte del aspecto de transporte de Internet, no existe ninguna otra similitud entre el medio y las carreteras. Internet transporta materiales intangibles (datos), mientras que las carreteras facilitan el transporte de bienes y personas.

*Utilizada por:* La analogía de la carretera fue utilizada extensivamente a mediados de la década de 1990, cuando Al Gore introdujo el término "supercarretera de la información". El término "carretera" también fue utilizado en junio de 1997 por el gobierno alemán para justificar la introducción de un control más estricto del contenido en Internet: "Se trata de una ley liberal que no tiene ninguna relación con la censura, sino que establece claramente las condiciones de lo que es posible o no para un proveedor. Internet es un medio de transporte y distribución de conocimiento… al igual que las carreteras, es necesario tener pautas para ambos tipos de tráfico".

## CLASIFICACIÓN DE LOS TEMAS DE GOBERNANZA DE INTERNET

La Gobernanza de Internet es un campo nuevo y complejo que requiere de antemano el mapeo y clasificación de sus conceptos. La complejidad de la Gobernanza de Internet se sustenta en su naturaleza multidisciplinaria, ya que abarca una serie de aspectos que incluyen la tecnología, los temas socioeconómicos, el desarrollo, la legislación y la política.

La necesidad de llevar a cabo un mapeo inicial de la Gobernanza de Internet responde tanto a un sentido académico como práctico. En la parte académica se está produciendo una gran cantidad de investigaciones sobre Gobernanza de Internet, sin embargo el enfoque principal ha sido ICANN y otros temas relacionados con el llamado enfoque "estricto" de la Gobernanza de Internet. Todavía es necesario desarrollar un marco teórico más amplio, en particular sobre los aspectos internacionales de la Gobernanza de Internet. La necesidad práctica de una clasificación quedó claramente demostrada durante el proceso de la CMSI. Muchos participantes, incluso representaciones de países, tuvieron dificultades a la hora de comprender la complejidad de la Gobernanza de Internet. Un mapeo conceptual del campo debería contribuir a la eficiencia de las negociaciones dentro del contexto de la CMSI, así como a otros procesos de negociación multilateral relacionados con temas de Internet.

La clasificación podría ayudar a los participantes en las discusiones de Gobernanza de Internet en los siguientes aspectos:

- una más clara identificación de los principales temas que deben ser objeto de negociación;
- reducción del "ruido" durante las negociaciones debido a interpretaciones inconsistentes de los conceptos principales;
- evitar la duplicación de esfuerzos tratando los mismos temas en múltiples foros;
- mantener un balance apropiado entre la perspectiva amplia y los asuntos específicos, evitando así el problema de "no poder ver el bosque a través de los árboles".

En última instancia, un mapeo cuidadoso de los asuntos relacionados con Internet debería contribuir positivamente a la eficiencia del proceso de negociación de Gobernanza de Internet. En términos económicos, debería reducir el costo de transacción – en otras palabras, redu-

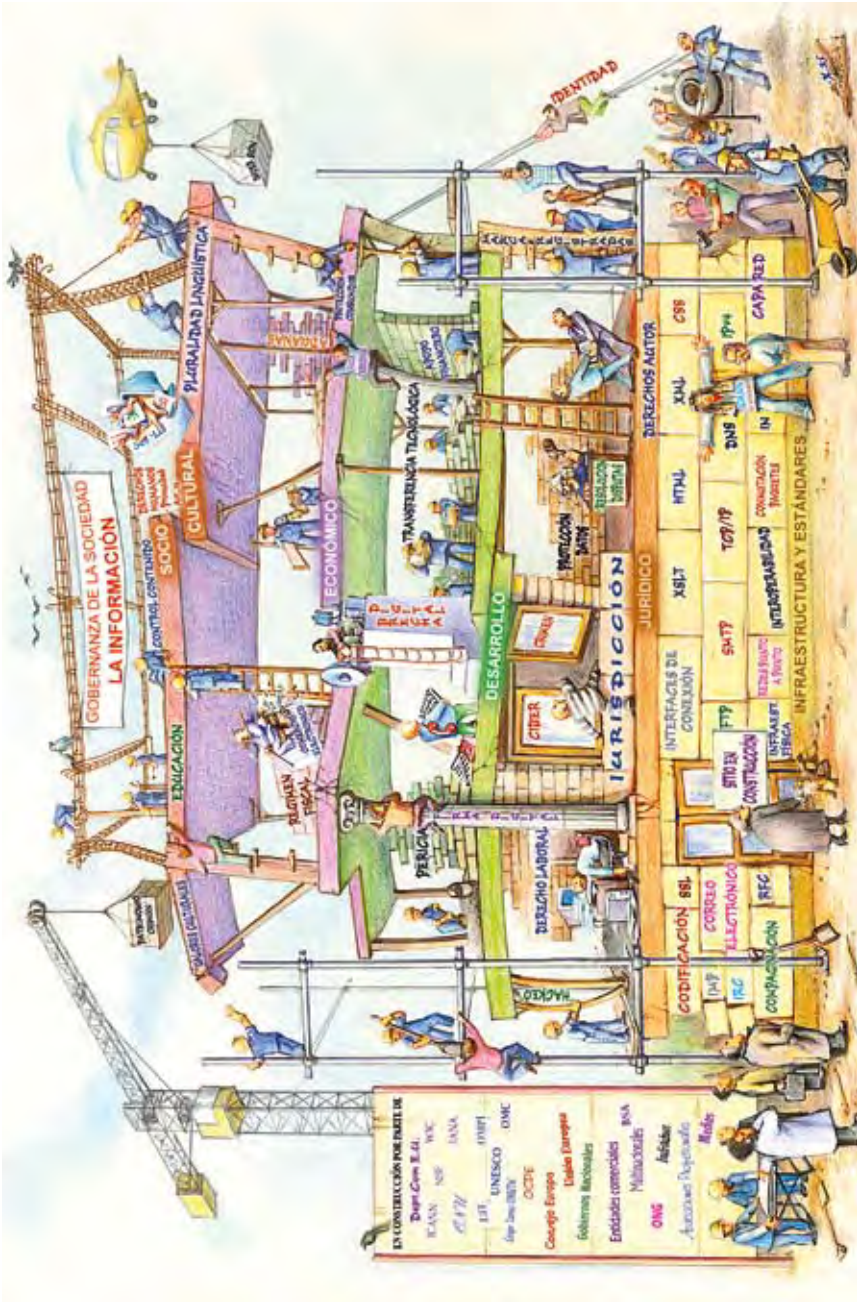
cir el tiempo total requerido para las negociaciones. Esto sería de particular beneficio para países con limitaciones en sus recursos financieros y humanos y contribuiría a aumentar su participación. Los procesos de negociación imprecisos y confusos requieren dedicación y recursos humanos desproporcionadamente superiores.

La clasificación que realiza Diplo de la Gobernanza de Internet divide los temas en cinco grupos: Ajustando la terminología al mundo de la diplomacia, Diplo ha adoptado el término "canasta". (El término "canasta" fue introducido a la práctica diplomática durante las negociaciones de la Organización para la Seguridad y la Cooperación en Europa (OSCE). Las siguientes cinco canastas han sido utilizadas desde 1997, momento en que Diplo empezó a desarrollar su esquema de clasificación:

1) infraestructura y estandarización;
2) legal;
3) económica;
4) desarrollo;
5) sociocultural.

La clasificación de Diplo de la Gobernanza de Internet es la base conceptual para su enfoque general en este campo, incluyendo la capacitación, la educación, la investigación y el desarrollo de herramientas. Desde su introducción en 1997, la clasificación ha sido utilizada en los cursos brindados a más de 300 estudiantes y muchos investigadores. La retroalimentación regular para este esquema de clasificación ha sido la base de constantes ajustes. Por lo tanto, la clasificación actual está basada en múltiples iteraciones así como la suma de conocimientos y experiencias.

El modelo de las cinco canastas es presentado metafóricamente por medio de la ilustración de "Construcción en Proceso" de la página siguiente.


GOBERNANZA DE LA SOCIEDAD
LA INFORMACIÓN
SOCIO
CULTURAL
PLURALIDAD LINGÜÍSTICA
EDUCACIÓN
ECONÓMICO
DESARROLLO
JURISDICCIÓN
JURÍDICO
DERECHOS AUTOR
IDENTIDAD
INFRAESTRUCTURA Y ESTÁNDARES
EN CONSTRUCCIÓN POR PARTE DE:
Entidades comerciales
ONG
Gobiernos Nacionales
Consejo Europa
UNESCO
OMC
OCDE
CODIFICACIÓN
CORREO ELECTRÓNICO
CONFIGURACIÓN
DERECHO LABORAL
PERICIA
XSLT
HTML
XML
CSS
SMTP
TCP/IP
DNS
CAPA RED
FTP
SITIOS WEB
CONSTRUCCIÓN
INTERFACES DE CONEXIÓN
INTERNACIONALIZACIÓN
CONVENCIÓN MARCAS

## "Edificio en Construcción" La Gobernanza de Internet – ¿Estamos Construyendo la Torre de Babel del Siglo XXI?

Una pintura del artista Pieter Brueghel el Viejo (1563) que se expone en el Museo Kunsthis-torisches de Viena muestra la construcción de la Torre de Babel. (Otra pintura más pequeña realizada el mismo año y sobre el mismo tema se exhibe en el Museo Boijmans Van Beuningen de Rótterdam). El Libro de Génesis de la Biblia (11.7) se refiere a la construcción de la Torre de Babel: "ahora, pues, descendamos y confundamos allí su lengua, para que ninguno entienda el habla de su compañero".

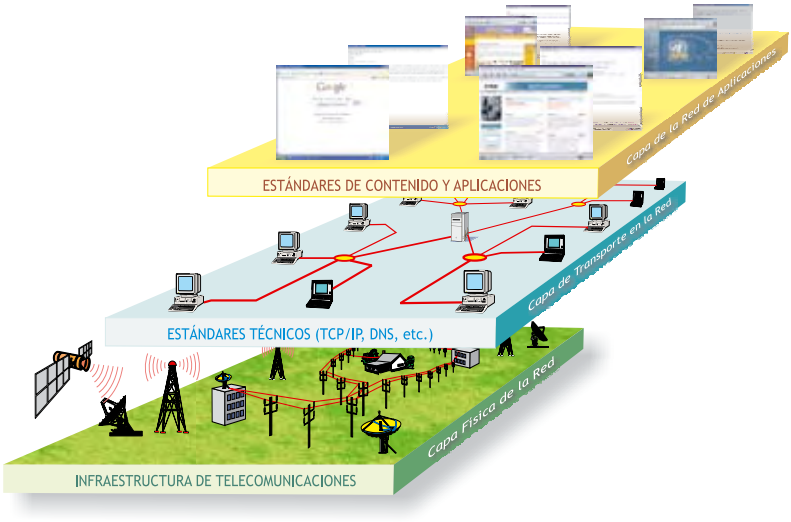
La analogía de la construcción de la Torre de Babel parece ser apropiada cuando observamos los desafíos que nos presenta Internet. Esta comparación ha motivado a los autores a considerar otro edificio en construcción – que no pretende alcanzar los cielos, pero al menos alcanzar a todas las personas en el planeta. Diplo ha desarrollado un marco para la discusión de la Gobernanza de Internet que se ilustra en la imagen de la página anterior. Cada uno de ellos se discute en detalle en los capítulos siguientes. Es importante darse cuenta de que todos los pisos en este edificio se encuentran interrelacionados y que la construcción es continua y eterna.

SECTION 2

# La Canasta de Infraestructura y Estandarización

## LA CANASTA DE INFRAESTRUCTURA Y ESTANDARIZACIÓN

La canasta de infraestructura y estandarización incluye los temas básicos y principalmente técnicos relacionados con la operación de Internet. En la ilustración del "Edificio en Construcción" que utiliza Diplo para la Gobernanza de Internet, el primer piso representa la infraestructura y la estandarización (referirse a la página 28). Los temas que se encuentran en esta canasta se dividen en dos grupos. El primero incluye los asuntos esenciales sin los cuales Internet y World Wide Web no podrían existir, y se representa en las siguientes tres capas:




Una de las fortalezas de Internet es su arquitectura en capas. La capa de infraestructura de Internet permanece independiente de la infraestructura de telecomunicaciones (la capa inferior) y de los estándares de las aplicaciones (la capa superior).

1. l la infraestructura de telecomunicaciones sobre la que fluye todo el tráfico de Internet

2. los estándares y servicios técnicos (la infraestructura que hace funcionar Internet (p. ej. TCP/IP, DNS, SSL); y
3. los estándares de contenido y aplicaciones (p. ej. HTML, XML).

El segundo consiste en asuntos relacionados con la protección de la operación segura y estable de la infraestructura de Internet, incluyendo seguridad, codificación y correo electrónico indeseado en Internet.


## LA INFRAESTRUCTURA DE TELECOMUNICACIONES

### LA SITUACIÓN ACTUAL

Los datos en Internet pueden viajar sobre un amplio rango de portadores de comunicaciones: cables telefónicos, cables de fibra óptica, satélites, microondas y enlaces inalámbricos. Incluso la red eléctrica básica puede ser utilizada para transmitir tráfico de Internet. El rápido crecimiento de Internet ha disparado un aumento considerable en las capacidades de telecomunicaciones. Se estima que desde 1998, la capacidad de telecomunicaciones ha aumentado 500 veces, debido a una combinación de innovación tecnológica e inversión en nuevas facilidades de telecomunicaciones.

Debido a que la capa de telecomunicaciones transporta el tráfico de Internet, cualquier nueva regulación relacionada con telecomunicaciones tendrá además un impacto inevitable en la misma. La infraestructura de telecomunicaciones es regulada, tanto a nivel nacional como internacional, por una serie de organizaciones públicas y privadas.

Tradicionalmente, las telecomunicaciones internacionales han sido coordinadas por la Unión Internacional de Telecomunicaciones (UIT), la cual desarrolla reglas minuciosas que cubren la relación entre los operadores nacionales, la asignación del espectro radioeléctrico y la administración de las posiciones satelitales.

Eventualmente, el enfoque liberal prevaleció sobre los monopolios en las telecomunicaciones. El proceso de liberalización fue formalizado a nivel internacional en 1998 en el Acuerdo Básico de Telecomunicaciones (ABT) de la Organización Mundial del Comercio (OMC). Después de la adopción del ABT, más de 100 países iniciaran el proceso de libe-

ralización, caracterizado por la privatización de los monopolios nacionales de telecomunicaciones, la introducción de competencia y el establecimiento de reguladores nacionales.

La Regulación Internacional de Telecomunicaciones de la UIT de 1988 facilitó la liberación internacional de precios y servicios y permitió que servicios básicos, como el arrendamiento de líneas internacionales, fueran utilizados con mayor innovación en el campo de Internet.

La OMC gradualmente se colocó en el centro del régimen internacional de telecomunicaciones, tradicionalmente regido por la UIT. Sin embargo, los roles de la OMC y de la UIT son significativamente distintos. La UIT establece estándares técnicos detallados, regulaciones internacionales específicas para las telecomunicaciones y ofrece asistencia a los países en desarrollo. La OMC ofrece un marco para las reglas generales del mercado.

Después de la liberalización, el monopolio práctico de la UIT, como institución principal a cargo del establecimiento de estándares de telecomunicaciones, fue erosionado por otros organismos y organizaciones profesionales, como el Instituto Europeo de Estandarización de las Telecomunicaciones (IEET), que desarrolló los estándares GSM, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), que desarrolló los estándares WiFi, y la Fuerza de Tareas de Ingeniería para Internet (IETF) que desarrolló TCP/IP y otros protocolos relacionados con Internet.

La liberalización de los mercados nacionales de telecomunicaciones ha otorgado a las grandes empresas del ramo, como AT&T, Cable & Wireless, France Telecom, Sprint y WorldCom, la oportunidad de extender globalmente su cobertura de mercado. Debido a que la mayor parte del tráfico de Internet es transportado sobre las infraestructuras de estas empresas, ellas ejercen una importante influencia en la Gobernanza de Internet.

## LOS ASUNTOS

### La "Última Milla" – La Disgregación del Bucle Local

El "bucle local" (o "la última milla") es la conexión entre los proveedores de servicios de Internet y sus clientes individuales. Los problemas con el "bucle local" constituyen un obstáculo para aumentar el uso de Internet en muchos países, especialmente aquellos en vías de desarrollo. El motivo es usualmente una infraestructura nacional de telecomunicaciones subdesarrollada. En algunos países en desarrollo con grandes territorios

es difícil conectar ciudades y pueblos remotos utilizando los tradicionales enlaces terrestres de telecomunicaciones.

La comunicación inalámbrica es considerada cada vez más como la mejor solución de bajo costo para el problema del "bucle local". Aparte del creciente número de opciones tecnológicas disponibles, la solución del problema del "bucle local" también depende de la liberalización de este segmento del mercado de las telecomunicaciones.

### La Liberalización de los Mercados de Telecomunicaciones

Un número considerable de países ha liberalizado sus mercados de telecomunicaciones. Sin embargo, muchos países en desarrollo que cuentan con monopolios de telecomunicaciones están enfrentando una difícil decisión: Cómo liberalizar y hacer más eficientes sus mercados de telecomunicaciones y a la vez preservar un importante ingreso presupuestario proveniente de los monopolios de telecomunicaciones.

Algunos métodos sugeridos para resolver este complejo asunto incluyen la asistencia extranjera, la implementación de una transición gradual, o el enlace del proceso de liberalización a la protección del interés público.

### El Establecimiento de Estándares Técnicos de Infraestructura

Cada vez es más común que los estándares técnicos sean determinados por instituciones privadas y profesionales. Por ejemplo, el estándar

**Tecnología, Estándares y Políticas**

El debate sobre los protocolos de red ilustra la manera en que los estándares no son más que política por medios distintos. En tanto que otras intervenciones gubernamentales en los negocios y la tecnología (como las regulaciones de seguridad y las acciones antimonopolio) son vistas con facilidad como de relevancia política y social, los estándares técnicos generalmente se asumen como socialmente neutros y por lo tanto despiertan poco interés histórico. Sin embargo, las decisiones técnicas pueden tener consecuencias económicas y sociales trascendentales, alterando el balance de poder entre empresas o naciones competidoras y limitando la libertad de los usuarios. Los esfuerzos por generar estándares formales colocan las decisiones técnicas privadas de los desarrolladores de sistemas en el plano público; de esta manera las batallas de estándares pueden sacar a la luz supuestos o conflictos de intereses hasta el momento tácitos. Es precisamente la pasión con la cual los interesados impugnan las decisiones tomadas sobre los estándares la que nos debe alertar sobre un significado más profundo que simplemente tornillos y tuercas. (Fuente: Janet Abbate Inventing the Internet, MIT Press)

WiFi, IEEE 802.11b, fue desarrollado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). La certificación de los equipos compatibles con WiFi la lleva a cabo la Alianza WiFi. Es precisamente la capacidad de establecer o implementar estándares en un mercado de tan rápido desarrollo la que le otorga a estas instituciones una considerable influencia sobre el mercado.

## ESTÁNDARES TÉCNICOS Y SERVICIOS – La Infraestructura de Internet

Es en este nivel que Internet toma forma. La mayoría de los asuntos relacionados se encuentran en el corazón del tema de la Gobernanza de Internet y usualmente aparecen listados como parte de la definición "estricta" de la Gobernanza de Internet. Se dividen en dos grupos. El primero comprende los asuntos centrales relacionados con estándares técnicos y servicios: TCP/IP, DNS y servidores raíz; mientras que el segundo cubre los aspectos comerciales de la infraestructura de Internet, incluyendo: los roles de los proveedores de servicios (ISPs) y los portadores de banda ancha, así como los aspectos económicos de la conectividad de Internet (cargos de conectividad de Internet y los Puntos de Intercambio de Internet - IXPs - por sus siglas en inglés).

### Perspectivas Opuestas sobre el Rol de ICANN en la Gobernanza de Internet

| ESTRICTA - TÉCNICA | AMPLIA – POLÍTICA |
|---|---|
| ICANN es simplemente un ente coordinador a cargo de la administración técnica de los números de IP y los nombres de dominio. De acuerdo con esta perspectiva, ICANN simplemente coordina y no gobierna Internet.<br>Perspectiva expresada por: ICANN, la Sociedad Internet, el gobierno de los Estados Unidos, los gobiernos de otros países industrializados. | El trabajo de ICANN involucra más que la simple coordinación técnica. Aunque ICANN debe continuar con las tareas técnicas centrales como la administración de los servidores raíz y la distribución de números de IP, las políticas deben ser establecidas por un ente internacional legitimado que represente a todos los estados. Esto podría ser logrado en la ONU o con un marco internacional de nueva constitución.<br>Perspectiva expresada por: muchos países en desarrollo. |

ICANN es probablemente la organización mencionada con mayor frecuencia dentro del contexto de las discusiones de Gobernanza de Internet. El motivo es la posición central que tiene ICANN en la administración de las direcciones numéricas de Internet (números de IP) y los sistemas de nombres de dominio.


## PROTOCOLO TCP/IP

### LA SITUACIÓN ACTUAL

El principal estándar de Internet que especifica la manera en que se trasladan los datos es el protocolo para el control de transporte / protocolo de Internet (TCP/IP por sus siglas en inglés), el cual se basa en tres principios: conmutación de paquetes, redes punto a punto y robustez.

La conmutación de paquetes es el método utilizado para transmitir datos en Internet. Todos los datos enviados desde una computadora son divididos en paquetes que viajan por Internet y luego son reensamblados por la computadora en el punto de destino.

Las redes punto a punto colocan toda la sofisticación, inteligencia e innovación en los bordes de una red. Este principio ha hecho posible todas las innovaciones relacionadas con Internet. La red entre uno y otro punto terminal es neutral y no evita el desarrollo y la creatividad en los mismos. Esto significa que las aplicaciones que corren en Internet pueden ser diseñadas en los bordes de la red sin requerir permisos por parte de los operadores y otras partes.

La Robustez se alcanza por medio del enrutamiento dinámico. Inicialmente, la red que precedió a Internet, ARPANET, introdujo enrutamiento dinámico para desarrollar redes de defensa robustas capaces de sobrevivir a un ataque nuclear. El enrutamiento dinámico se utilizó para interconectar un conjunto diverso de redes.

La Gobernanza de Internet relacionada con TCP/IP presenta dos aspectos importantes: a) la introducción de nuevos estándares; y b) la distribución de números de IP.

Los estándares de TCP/IP son establecidos por la Fuerza de Tareas de Ingeniería para Internet (IETF). IETF ejerce un cuidadoso control sobre TCP/IP debido a su relevancia fundamental para Internet.

Los número de IP son direcciones numéricas que deben ser utilizadas por cada computadora conectada a Internet. Los números de IP son únicos; dos computadoras conectadas a Internet no pueden tener el mismo número de IP. Por este motivo los números de IP son un recurso potencialmente escaso.

El sistema para la distribución de números de IP se encuentra organizado jerárquicamente. En la parte superior se encuentra la Autoridad de Números Asignados de Internet (IANA por sus siglas en inglés) una subsidiaria de ICANN que se encarga de distribuir bloques de números IP entre los Registros de Internet Regionales (RIR).

Los RIR actuales son: ARIN (el Registro Americano de Número de Internet), APNIC (el Centro de Información de Redes de Asia Pacífico), LACNIC (el Registro Regional de Direcciones IP de América Latina y el Caribe), y RIPE NCC (Centro de Coordinación para la Investigación de Redes IP Europeas – que cubre a Europa y el Oriente Medio). En estos momentos se está estableciendo un Registro a nivel Africano denominado AFRINIC.

Los RIR distribuyen los números de IP a los grandes ISPs y a los Registros de Internet a nivel local y nacional. En el siguiente escalón se encuentran los ISPs más pequeños, las empresas y los individuos.

## LOS ASUNTOS

### ¿Existen Suficientes Números de IP?

La reserva actual de números de IP bajo IPv4 (versión 4 del Protocolo de Internet) contiene unos 4,000 millones de números y podría agotarse con la introducción de dispositivos habilitados en Internet, como teléfonos móviles, organizadores personales, consolas de juegos y electrodomésticos.

La preocupación de que se agoten los números IP y que se restrinja el desarrollo de Internet ha llevado a la comunidad técnica a implementar dos acciones importantes.

- La primera fue la racionalización en el uso de la reserva actual de números de IP. Esto se logró con la introducción de la Traducción de Direcciones de Red (NAT por sus siglas en inglés), capaz de conectar una

red privada (p. ej. compañía o universidad) utilizando solo un IP. Si no se utiliza NAT, cada computadora en una red necesitaría su propio número de IP.
- La segunda acción fue la introducción de IPv6/ (una nueva versión del Protocolo de Internet) que brinda una reserva mucho mayor de números de IP (430,000,000,000,000,000,000).

La respuesta de la comunidad técnica de Internet ante un posible faltante de números de IP es un ejemplo de gestión puntual y proactiva. Se siguió el enfoque de "prevenir en lugar de lamentar" (conocido como el "principio de precaución" en el lenguaje de la diplomacia ambiental), aun cuando era incierta la velocidad con la cual los números de IPv4 serían agotados.

Sin embargo, sería posible sufrir una escasez artificial si quienes tienen la responsabilidad de asignar los números IP a nivel local, como los ISPs, decidieran abusar de su poder y condicionar las asignaciones sobre, por ejemplo, la base de compra de servicios adicionales, lo que afectaría la disponibilidad y precio de los números de IP.

### Cambios en TCP/IP y Seguridad en Internet

La seguridad no fue un problema importante para los desarrolladores originales de Internet, ya que en aquel momento se trataba de una red cerrada entre instituciones de investigación. La seguridad se garantizaba principalmente limitando en el acceso físico a las redes y computadoras conectadas. Las computadoras eran utilizadas por un pequeño grupo de especialistas. Los datos eran intercambiados sin ninguna protección en particular.

La expansión de Internet ha provocado un crecimiento en la base de usuarios que supera todas las expectativas de su comunidad inicial y que hoy en día se traduce en aproximadamente 1,000 millones de usuarios a nivel mundial. Internet también se ha convertido en una importante herramienta comercial.

Todo esto coloca la cuestión de la seguridad en un lugar prioritario en la lista de asuntos relacionados con la Gobernanza de Internet. La seguridad ha sido progresivamente mejorada utilizando diferentes soluciones, principalmente ad hoc. Algunas de ellas, como los cortafuegos, los antivirus y el software de codificación han sido efectivos en un grado sustancial.

BDebido a que la arquitectura de Internet no fue diseñada con la seguridad en mente, la incorporación de seguridad intrínseca requeriría de cambios sustanciales a la base misma de Internet, el TCP/IP. Un nuevo protocolo (IPv6) ofrece algunas mejoras en seguridad, sin embargo todavía se queda corto de ofrecer una solución integral. Esta protección requeriría modificar considerablemente el TCP/IP.

#### Cambios en TCP/IP y el Problema de las Limitaciones en el Ancho de Banda

Para facilitar la entrega de contenido multimedios (p. ej. telefonía en Internet o vídeo por demanda) es necesario ofrecer Calidad de Servicio (QoS) capaz de garantizar un nivel mínimo de desempeño. QoS especifica estados de disponibilidad (tiempo de operación), ancho de banda (tasa efectiva de datos), latencia (demora) y errores. Es particularmente importante para aplicaciones sensibles a las demoras, como la transmisión de eventos en vivo. Las limitaciones en el ancho de banda producen imágenes congeladas o en cámara lenta y sonidos con eco. La introducción de QoS podría requerir modificaciones en los protocolos de Internet, incluyendo el compromiso de uno de sus principios fundamentales, las redes punto a punto.

## POSIBLES DESARROLLOS FUTUROS

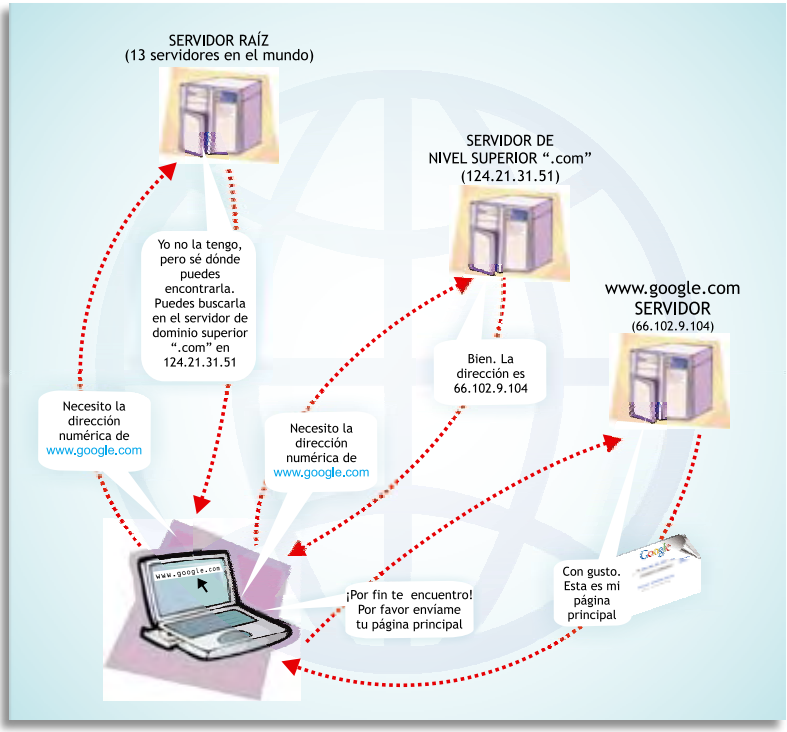
Se espera que se ejerza una mayor presión por la implementación de cambios en la arquitectura actual de redes. Algunas soluciones que buscan una mayor seguridad y aumentos en el ancho de banda no pueden ser logradas sin realizar cambios fundamentales en el Protocolo de Internet.

Otra solución propuesta es la construcción de diferentes opciones de redes sobre el TCP/IP actual. Es muy probable que las empresas privadas continúen desarrollando estas iniciativas, las cuales superarían las limitaciones del Internet actual y la indecisión de los entes estandarizadores de modificar los principios fundamentales de Internet, principalmente "las redes punto a punto".


# EL SISTEMA DE NOMBRES DE DOMINIO (DNS)

## LA SITUACIÓN ACTUAL

DNS toma las direcciones de Internet (como www.google.com) y las convierte en números de IP. Entonces, para tener acceso a un sitio web en particular, una computadora requiere tener acceso primero a un servidor de DNS. Este servidor DNS procede a localizar la dirección numérica (196.23.121.5 en el caso de Google) de ese sitio en particular. DNS está compuesto de servidores raíz, servidores de dominio superior y una serie de servidores DNS localizados alrededor del mundo. La administración de DNS ha sido un tema candente en el debate sobre la Gobernanza de Internet. Una de las principales controversias es la organización jerárquica de DNS y la máxima autoridad que sobre este ejerce el gobierno de los Estados Unidos (a través de su Departamento de Comercio).



DNS involucra dos tipos de dominios de nivel superior. Uno es genérico y el otro se basa en códigos por país. Los dominios genéricos de nivel superior (gTLD por sus siglas en inglés) incluyen:

- .com, .edu, .gov, .mil, y .org (en 1984);
- .net y .int (agregados en 1985); y
- .biz, .info, .name, .pro, .museum, .aero, y .coop (agregados en 2000).

Para cada gTLD existe un registro que mantiene su listado de direcciones. Por ejemplo, el gTLD ".com" es administrado por VeriSign. La función de "ventas" es realizada por los registradores. ICANN se encarga de la coordinación general del sistema DNS concluyendo acuerdos y acreditando registros y registradores. También determina el precio mayorista del "alquiler" que cobra el registro (VeriSign) a los registradores por los nombres de dominio, y establece ciertas condiciones a los servicios que ofrecen el registro y los registradores. En otras palabras, ICANN actúa como regulador económico y legal del negocio de nombres de dominio para los gTLDs.

Una parte importante de la administración de dominios involucra la protección de marcas registradas y la resolución de disputas. En los primeros días de Internet, el registro de dominios se basaba en el principio de "prioridad según el orden de llegada" y cualquiera podía registrar cualquier nombre.

El valor potencial de los nombres de dominio disparó el fenómeno de los ciberokupas, es decir la práctica de registrar nombres de dominio que podrían ser revendidos en el futuro. La imposibilidad de tener dos dominios con el mismo nombre generó un debate sobre los derechos de registro. El problema fue particularmente relevante en el caso de los nombres de dominio que utilizaban nombres de marcas de renombre (p. ej. Microsoft, Nike, Toyota, Rolex).

La reforma en la administración de DNS, con la adopción de la Política Uniforme de Resolución de Disputas de Nombres de Dominio (UDRP por sus siglas en inglés) ha introducido mecanismos para reducir significativamente la ciberokupación. La Política UDRP solamente se encuentra disponible para dominios .com, .net y .org y no cubre los dominios por país. La jurisdicción de la UDRP es automáticamente reconocida cuando un individuo, empresa u organización firma el acuerdo de registro del nombre de dominio. La Política UDRP ofrece algunas ventajas a quienes desean cuestionar los nombres ya registrados, usualmente los poseedores de marcas registradas tradicionales, que incluyen la resolu-

ción rápida de conflictos por medio de arbitraje y la simple implementación de decisiones de arbitraje por medio de cambios directos en el DNS (evitando interminables procedimientos judiciales).

Otro elemento importante en el estudio de la organización actual de la gobernanza del DNS es la administración de los dominios superiores por código país (ccTLDs). Actualmente, los códigos país son administrados por diversas instituciones acreditadas en los primeros días de Internet, cuando algunos gobiernos no estaban todavía muy interesados en estos asuntos. Estas organizaciones incluyen: instituciones académicas, asociaciones técnicas, ONGs e incluso individuos. En muchos casos, la responsabilidad de manejar los códigos por país fue asignada a los primeros que manifestaron su interés.

## LOS ASUNTOS

### La Creación de Nuevos Nombres de Dominio Genéricos

A mediados de la década de 1990, uno de los fundadores de Internet, Jon Postel, procuró infructuosamente agregar una serie de dominios nuevos a la lista básica existente (.com, .edu, .org y .int). La oposición principal provino del sector comercial, cuya preocupación era que el aumento en los dominios dificultara la protección de sus marcas. En ese momento prevaleció el enfoque restrictivo, y solamente unos cuantos dominios nuevos fueron introducidos por ICANN en 2000 (.biz, .info, .name, .pro, .museum, .aero, y .coop).

Otro problema relacionado con los nuevos dominios involucra el enlace de los nombres con el contenido. Por ejemplo, el Congreso de los Estados Unidos adoptó una ley que reserva el dominio "kids.us" exclusivamente para contenido apropiado para niños. La principal dificultad que enfrenta esta propuesta es determinar exactamente qué es apropiado para niños. Diferencias conceptuales y prácticas controversiales podrían surgir con relación al control del contenido. Hasta el momento, el dominio "kids" solamente ha sido utilizado como parte del dominio de país de los Estados Unidos.

### La Gestión de Dominios de País

La gestión de dominios superiores por código país involucra tres temas importantes. El primero se relaciona con la decisión a menudo controversial en la arena política de determinar exactamente cuáles códigos país deben ser registrados al tratar con países y entidades con estatus in-

ternacional poco claro o en discusión (p. ej. países recién independizados, movimientos de resistencia, etc.). Jon Postel recomendó la asignación de nombres de dominio nacionales de conformidad con el estándar ISO, el cual ofrece una fuente común de abreviaturas de dos letras para países y otras entidades. El enfoque de Postel prevaleció y continúa en práctica, a pesar de que el listado de ISO identifica "áreas económicas definidas" en lugar de naciones soberanas.

El segundo asunto se refiere a quién debe manejar los códigos por país. Muchos países han tratado de obtener el control de sus dominios de país, ya que los consideran recursos nacionales. Por ejemplo, Sudáfrica utilizó sus derechos soberanos como argumento para recuperar el control del dominio de su país. Una ley recién promulgada especifica que el uso del dominio de país fuera de los parámetros prescritos por el gobierno de Sudáfrica es considerado un crimen. El modelo brasileño de gestión de dominios de país es usualmente citado como un ejemplo exitoso de un enfoque de múltiples partes interesadas. El ente nacional a cargo de los dominios de Brasil está abierto a todos los interesados clave, incluyendo autoridades gubernamentales, el sector comercial y la sociedad civil. La transferencia del dominio de país de Cambodia del control no gubernamental al gubernamental es a menudo citada como una transición fallida. El gobierno redujo la calidad de los servicios e introdujo tarifas más altas, lo que ha dificultado el registro de dominios en Cambodia.

En algunos casos, los dominios de país han sido utilizados con el fin de registrar dominios superiores genéricos, como los listados a continuación:

| CÓDIGO PAÍS | PAÍS | ÁREA DE DOMINIO |
|---|---|---|
| Tv | Tuvalu | Estaciones de Televisión |
| Mu | Mauricio | Música |
| Md | Moldavia | Medicina y salud |
| Fm | Federación de Micronesia | Radio |
| Tm | Turkmenistán | Marcas Registradas |

La mayoría de los países mencionados anteriormente han tratado de recuperar el control de los dominios de su país. Por ejemplo, Mauricio inició una campaña intensiva de cabildeo diplomático en este sentido.

El tercer asunto se relaciona con la renuencia de muchos operadores de dominios por país de integrarse al sistema de ICANN. Hasta el momento, ICANN no ha logrado unir a todos los operadores de dominios por país bajo su paraguas. Algunos operadores de dominios por país han empezado

a crear sus propias organizaciones regionales como el Consejo de Europa de Registros de Dominios Nacionales (CENTR por sus siglas en inglés).

#### El Problema de los Idiomas: Nombres de Dominio Multilingües

Una de las principales limitaciones para el desarrollo futuro de Internet es la falta de características multilingües para correr la infraestructura de Internet. Los nombres de dominio se registran y utilizan en Inglés. Incluso los caracteres en Francés o Alemán que no pertenecen al código ASCII no pueden ser utilizados en las direcciones de Internet (p. ej. café se convierte en cafe). Esta situación se complica aún más con las escrituras no latinas como el japonés, el árabe y el chino.

Entre las diferentes soluciones para los nombres de dominio multilingües, las más relevantes las aportan los sistemas de Nombre de Dominio Internacionalizado (IDN por sus siglas en inglés) y la Dirección de Internet en Lenguaje Nativo (NLIA). IDN es una solución técnica propuesta por IETF que se está convirtiendo en la solución dominante. IDN traduce los nombres nativos a nombres de dominio en Inglés en la máquina cliente y envía los nombres de dominio en inglés al DNS. Otro obstáculo para el uso más amplio de IDN es su migración técnica dentro de los principales navegadores de Internet como Internet Explorer.

Aparte de la dificultades técnicas, el siguiente desafío, probablemente aún más complejo, será desarrollar políticas y procedimientos de gestión. Existe cada vez más presión para que IDN sea administrado por países o grupos de países que comparten un mismo idioma. Por ejemplo, el gobierno de China ha indicado en diversas ocasiones que IDN en Chino debe ser manejado por su país. La introducción de una política para IDN será uno de los principales desafíos de ICANN y una prueba de su enfoque participativo a nivel internacional.


## SERVIDOR RAÍZ DE DOMINIOS

Debido a que se encuentran en la parte superior de la estructura jerárquica de los sistemas de nombre de dominio, los servidores raíz atraen mucha atención. Son parte de la mayoría de los debates políticos y académicos que se llevan a cabo sobre Gobernanza de Internet.

### LA SITUACIÓN ACTUAL

La función y robustez de DNS puede ser ilustrada al analizar la preocupación que genera el hecho de que Internet colapsaría si los servidores raíz fueran alguna vez desactivados. Primero que nada, hay 13 servidores raíz distribuidos alrededor del mundo (10 en los Estados Unidos, 3 en el resto del mundo; de los 10 en los Estados Unidos, muchos son operados por agencias gubernamentales estadounidenses). Si un servidor deja de operar, los 12 restantes continuarían funcionando. Incluso si los 13 servidores raíz dejaran de funcionar a la vez, la resolución de los nombres de dominio (la función principal de los servidores raíz) continuaría siendo realizada por otros servidores de nombres de dominio distribuidos jerárquicamente a lo largo de Internet.

Por lo tanto, miles de servidores de nombres de dominio contienen copias de la zona primaria y un colapso inmediato y catastrófico de Internet no sería posible. Tomaría algún tiempo para que cualquier consecuencia funcional grave fuera perceptible, y durante ese tiempo sería posible reactivar los servidores originales o crear unos nuevos.

Además, el sistema de servidores raíz es fortalecido considerablemente por el esquema de "cualquier difusión" (Anycast), que replica los servidores raíz en más de 80 puntos a nivel mundial. Esto ofrece muchas ventajas, incluyendo una mayor robustez del sistema DNS y una más rápida resolución de las direcciones de Internet (gracias al esquema de cualquier difusión, los servidores encargados de la resolución se encuentran más cerca de los usuarios finales).

Los 13 servidores raíz son manejados por una diversidad de organizaciones: instituciones académicas/públicas (seis servidores), empresas comerciales (cuatro servidores) e instituciones gubernamentales (tres servidores).

Las instituciones que administran los servidores raíz reciben una zona primaria propuesta por IANA (ICANN) y aprobada por el gobierno de los Estados Unidos (Departamento de Comercio). Una vez que el contenido ha sido aprobado por el Departamento de Comercio, se ingresa en el servidor raíz maestro operado por VeriSign por contrato con del Departamento de Comercio. El archivo en el servidor raíz maestro es luego replicado automáticamente a los demás servidores raices. Por lo tanto, para el gobierno de los Estados Unidos es posible introducir modificaciones unilaterales en el DNS. Esto es una fuente de preocupación para muchos gobiernos.

## LOS ASUNTOS

### ¿Debería ser Internacionalizada la Política de Supervisión de los Servidores Raíz?

Muchos países han expresado su preocupación ya que de acuerdo con el procedimiento actual el Departamento de Comercio de los Estados Unidos tiene la decisión final sobre el contenido de los servidores raíz, y se ha sugerido adoptar una "Convención Primaria" que pusiera a la comunidad internacional a cargo de la supervisión de las políticas de los servidores raíz o al menos, otorgar a los países derechos sobre sus propios nombres de dominio nacionales. No es muy probable que las instituciones estadounidenses (principalmente el Congreso) acepten estas propuestas. Un compromiso potencial podría estar basado en dos elementos:

- inicialmente se consideró la transferencia del control de los servidores primarios del Departamento de Comercio estadounidense a ICANN;
- o una reforma sustancial de ICANN, que conduzca a la creación de una organización internacional sui generis, con un marco institucional aceptable para todos los países.

### ¿Cuál es la Probabilidad de Crear Servidores Raíz Alternos (p. ej. Internet B)?

Tal y como se discutió anteriormente, la creación de un servidor raíz alterno es algo técnicamente simple. La principal pregunta es cuántos "seguidores" tendría un servidor alterno o más precisamente, cuántas computadoras en Internet se dirigirían a este a la hora de resolver nombres de dominio. Sin los usuarios, cualquier DNS alterno sería completamente inútil. Ha habido algunos intentos por crear un DNS alterno: Open NIC, New. net, y Name.space. La mayoría de ellos han sido infructuosos, y representan únicamente un pequeño porcentaje de los usuarios de Internet.


## PROVEEDORES DE SERVICIOS DE INTERNET (ISPs)

Los ISPs conectan a los usuarios finales a Internet y a los sitios web anfitriones. Este es el motivo por el cual para muchos gobiernos los ISPs son la opción más directa y simple de imponer control gubernamental y reglas legales en Internet. En este texto, por ISPs nos referimos tanto a empresas que brindan acceso a usuarios individuales como a Proveedores de Servicios de Internet a nivel institucional (universidades, departamentos gubernamentales, etc.).

Durante el auge de Internet en la década de 1990, los ISPs fueron liberados de cualquier responsabilidad por las violaciones de contenido o derechos de reproducción. Se creía que la presión adicional sobre los ISPs podría dificultar el futuro desarrollo de Internet. Con la creciente relevancia comercial de Internet y el aumento en las preocupaciones de seguridad, muchos estados han empezado a concentrar sus esfuerzos de fiscalización en los ISPs.

### LOS ASUNTOS

#### El Mercado de ISPs y el Monopolio de Telecomunicaciones

Es común que en los países con monopolios de telecomunicaciones estos también estén a cargo del acceso a Internet. Los monopolios impiden a otros ISPs ingresar al mercado e inhiben la competencia. Esto produce precios más altos y a menudo una menor calidad de servicio, lo que además no contribuye a reducir la brecha digital. En algunos casos, los monopolios de telecomunicaciones toleran la existencia de otros ISPs, pero interfieren a nivel operativo (p. ej. otorgando anchos de banda menores o provocando interrupciones en los servicios).

#### La Responsabilidad de los ISPs sobre los Derechos de Reproducción

La mayor parte de los sistemas legales coinciden en que un ISP no puede asumir responsabilidad por los materiales que hospeda y que puedan infringir los derechos de reproducción si el hecho no es del conocimiento del ISP. La principal diferencia descansa en la acción legal que se ejerce una vez que el ISP ha sido informado de que el material que hospeda infringe los derechos de reproducción.

La legislación estadounidense y Europea emplea el procedimiento de Notificación de Remoción, por medio del cual se indica al ISP que debe proceder a remover el material en cuestión para evitar ser acusado. La legislación estadounidense y europea ofrece una mayor protección al poseedor del derecho de reproducción, y no ofrece al usuario del material ninguna oportunidad de presentar su caso. La legislación japonesa utiliza un enfoque más balanceado, brindando al ISP una Notificación de la Notificación de Remoción, lo que le otorga al usuario del material el derecho de protestar por la solicitud de remoción.

### El Rol de los ISPs en la Política de Contenido

"No maten al mensajero" es la respuesta de los ISPs ante la creciente presión oficial de imponerles la política de contenido. A regañadientes, los proveedores de servicios de Internet se están involucrando gradualmente en la política de contenido. Es posible que tengan que adaptarse a dos rutas posibles. La primera es imponer la regulación gubernamental. La segunda, basada en la autorregulación, permite a los ISPs definir por si mismos cuál contenido es apropiado. Esto presenta el riesgo de que se produzca una privatización de la política de contenido, teniendo los ISPs que asumir la responsabilidad del estado.

En muchos países se ha adoptado legislación en la cual los ISPs deben asumir responsabilidades adicionales relacionadas con políticas de contenido; tanto en el contenido de los sitios que hospedan como en el contenido al que tienen acceso sus clientes. Este enfoque podría generar gastos adicionales para los ISPs y, eventualmente, aumentos en el costo del acceso a Internet para los usuarios.


## PROVEEDORES DE ANCHO DE BANDA PARA INTERNET (IBPs)

La arquitectura de acceso a Internet está compuesta de tres capas. Los ISPs que conectan a los usuarios finales constituyen la Capa 3. Las capas 1 y 2 corresponden a los portadores de ancho de banda de Internet. La Capa 1 (redes troncales de Internet) es usualmente administrada por empresas grandes como MCI, AT&T, Cable & Wireless y France Telecom. En el campo de los portadores de redes troncales de Internet, las empresas tradicionales de telecomunicaciones han extendido hacia estas su

presencia en el mercado global. Los proveedores de Capa 2 usualmente operan a nivel nacional o regional.

## LOS ASUNTOS

### ¿Debe ser Considerada como Servicio Público la Infraestructura de Internet ?

Los datos de Internet pueden fluir sobre cualquier medio de telecomunicaciones. En la práctica, facilidades como las redes troncales Capa 1 se han hecho críticas para la operación de Internet. Su posición fundamental dentro de la red de Internet le otorga a sus propietarios el poder de imponer precios y condiciones de mercado para los servicios que ofrecen. Dos casos relacionados fueron mencionados en un reporte reciente de la OSCE (la Organización de Seguridad y Cooperación de Europa)

En el primer caso, se inició una acción legal contra una página web con contenido Nazi cuestionable hospedada por Flashback en Suecia. Los tribunales decidieron que la página no violaba la legislación Sueca antinazismo. Sin embargo, un activista antinazismo comprometido con su causa llevó a cabo una fuerte campaña contra Flashback, ejerciendo presión sobre su ISP, Air2Net, y el operador principal de red troncal MCI/WorldCom. Ante la presión de esta campaña, MCI/WorldCom decidió desconectar a Flashback a pesar de no contar con un fundamento legal para hacerlo. Los intentos de Flashback por encontrar un proveedor alterno resultaron infructuosos, ya que la mayoría de ellos también se conectaban a la red troncal por medio de MCI/WorldCom.

El segundo caso se presentó en los Países Bajos donde un pequeño proveedor holandés de ISP, Xtended Internet, fue desconectado por su proveedor basado en los Estados Unidos debido a presiones resultantes de un cabildeo llevado a cabo por una organización de Cientología. Al final de cuentas, la operación de Internet podría depender de las decisiones que toman los propietarios de redes troncales centralizadas. ¿Tiene la comunidad global de Internet algún derecho de solicitar a los principales operadores de telecomunicaciones garantías para el funcionamiento confiable de la infraestructura crítica de Internet? ¿Están estas empresas operando una facilidad de carácter publico?

### La Liberalización de las Telecomunicaciones y el Rol de los ISPs

Existen perspectivas opuestas en cuanto al grado en que los proveedores de servicios de Internet (ISPs) deben sujetarse a las regulaciones actuales de la OMC. Los países desarrollados discuten que la reglas de liberalización giradas por la OMC a los operadores de telecomunicaciones también deben extenderse a los ISPs. Una interpretación restrictiva resalta el hecho de que el régimen de telecomunicaciones de la OMC se aplica únicamente al mercado de telecomunicaciones. La regulación del mercado de ISPs requiere nuevas reglas por parte de la OMC.

.


## MODELO ECONÓMICO PARA LA CONECTIVIDAD DE INTERNET

### LA SITUACIÓN ACTUAL

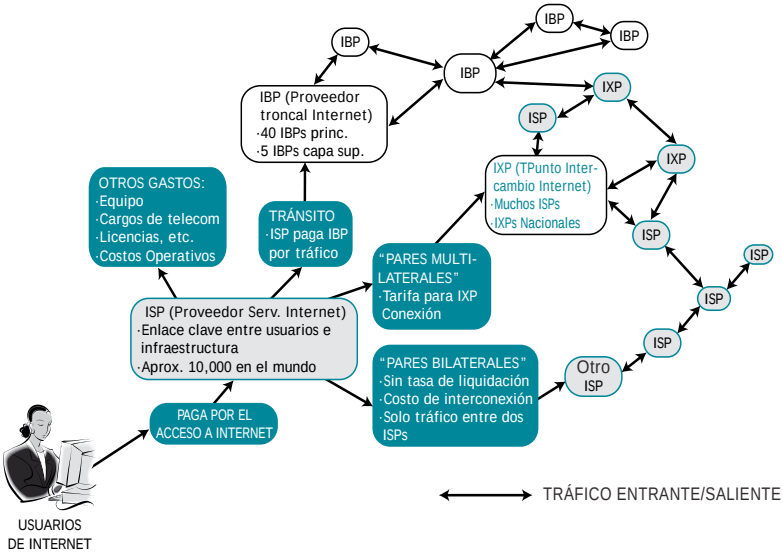
A menudo, las discusiones sobre gobernanza terminan incluyendo un análisis sobre la distribución del dinero y las fuentes de ingresos. ¿Cuál es el flujo de fondos en Internet? ¿Quién paga Internet?

Se llevan a cabo muchas transacciones financieras entre las muchas partes involucradas en Internet.

- Los abonados individuales y las empresas pagan a los ISPs.
- Los ISPs pagan por los servicios de los operadores de telecomunicaciones y por el ancho de banda de Internet.
- Los ISPs pagan a los proveedores por el equipo, el software y el mantenimiento (incluyendo herramientas de diagnóstico y personal para operar sus instalaciones, centros de soporte y servicios administrativos).
- Las partes que registran un nombre de dominio ante un registrador, no solo le pagan al registrador, sino también a IANA por sus servicios.
- Los ISPs pagan a los RIRs por las direcciones de IP.
- Los RIRs le pagan a ICANN.
- Los operadores de telecomunicaciones le pagan a los fabricantes de cable y satélites y los proveedores de servicios de telecomunicaciones les brindan los enlaces necesarios. Como estos operadores a menudo

se encuentran endeudados, a su vez pagan intereses a los diferentes bancos y consorcios.

La lista continúa y la verdad es que "para nadie hay almuerzo gratis". Al final de cuentas, los costos de esta cadena son cubiertos por los usuarios finales de Internet, ya sea individuos o instituciones.




## LOS ASUNTOS

### ¿Quién Debe Pagar los Costos de los Enlaces entre los Países Desarrollados y en Vías de Desarrollo?

Actualmente, el costo lo cubren principalmente los países en desarrollo. A diferencia del sistema telefónico tradicional, en el cual el precio de cada llamada internacional es compartido entre ambos países, el modelo de Internet coloca la carga total de un solo lado, es decir los países en desarrollo que necesitan conectarse a las redes troncales localizadas principalmente en países desarrollados. Paradójicamente, debido a este hecho sería fácil argumentar que los países pequeños y pobres subsidian el sistema de Internet en los países desarrollados.

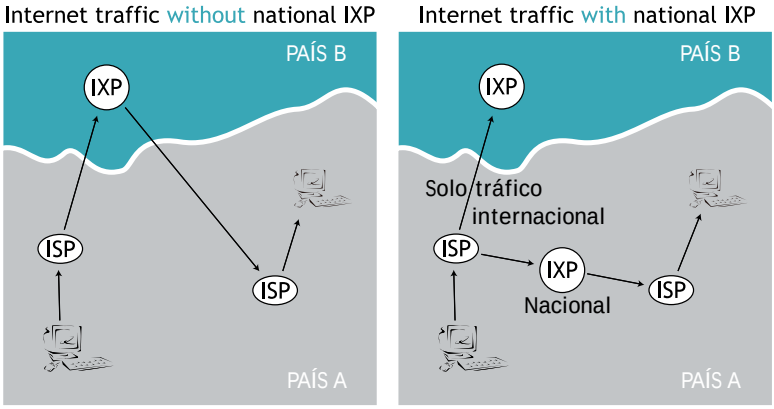
El problema de la tasa de liquidación es particularmente relevante para los países más pobres, ya que cuentan con el ingreso por telecomunicaciones internacionales como una fuente presupuestaria importante. La

situación se ha complicado con la introducción de Voz sobre IP (VoIP), telefonía sobre Internet, que traslada el tráfico telefónico de los operadores nacionales de telecomunicaciones a Internet.

La UIT inició discusiones sobre posibles mejoras en el sistema actual de liquidaciones por gastos de Internet con el principal objetivo de obtener una distribución más balanceada de los costos de acceso a Internet. Debido a la oposición de parte de los países desarrollados, la Resolución D.50 adoptada por la UIT es prácticamente ineficaz.

### Reducción de los Costos de Acceso por medio del Uso de Puntos de Intercambio de Internet (IXPs)

Los IXPs son facilidades técnicas a través de las cuales diferentes ISPs intercambian su tráfico en Internet. Los IXPs usualmente son establecidos para mantener el tráfico de Internet dentro de comunidades más pequeñas (p. ej. ciudades, regiones, países), evitando un enrutamiento innecesario a través de lugares remotos.




Los IXPs también juegan un papel importante en la reducción de la brecha digital. Por ejemplo, en el caso de un país sin IXPs nacionales, una parte considerable del tráfico entre los clientes del mismo país tendría que ser enrutada a través de otro país. Esto aumenta el volumen de tráfico internacional de datos a larga distancia y el costo de brindar el servicio de Internet.


## ESTÁNDARES WEB

Hacia finales de la década de 1980, la batalla sobre los estándares de red había terminado. TCP/IP gradualmente se convirtió en el protocolo de redes, marginando otros estándares, como el X-25 apoyado por la UIT (parte de la Arquitectura de Interconexión de Sistemas Abiertos) y muchos estándares patentados como el SNA de IBM. Mientras Internet facilitaba las comunicaciones normales entre una serie de redes utilizando TCP/IP, el sistema aún carecía de estándares comunes para aplicaciones.

Una solución fue desarrollada por Tim Berners-Lee y sus colegas del CERN en Ginebra, que consistía en un nuevo estándar para el intercambio de información en Internet llamado HTML (Lenguaje de Marcas de Hipertexto, que en realidad es una simplificación de un estándar ISO existente llamado SGML). El contenido desplegado en Internet tenía que ser organizado primero según los estándares HTML. El lenguaje HTML, utilizado como cimiento de la Red de Redes (la World Wide Web) allanó el camino para el crecimiento exponencial de Internet.

Desde su primera versión, el lenguaje HTML ha sido constantemente actualizado con nuevas características. La creciente relevancia de Internet ha traído a colación la pregunta sobre la estandarización del lenguaje HTML. Esto fue particularmente relevante durante la "Guerra de los Navegadores" entre Netscape y Microsoft, instancia en que ambas compañías trataron de fortalecer su posición en el mercado ejerciendo influencia sobre los estándares HTML. Mientras que el lenguaje HTML básico maneja únicamente texto y fotografías, las nuevas aplicaciones de Internet requerían tecnologías más sofisticadas para el manejo de bases de datos, vídeo y animaciones. Esta variedad de aplicaciones requería esfuerzos considerables de estandarización para garantizar que el contenido de Internet pudiera ser visto apropiadamente en la mayoría de los navegadores de Internet.

La estandarización de aplicaciones ingresó en una nueva fase con el surgimiento de XML (Lenguaje Extensible de Marcas), el cual brindaba una mayor flexibilidad en el establecimiento de estándares para el contenido de Internet. Nuevos conjuntos de estándares XML también han sido in-

troducidos. Por ejemplo, el estándar para la distribución de contenido inalámbrico se llama WML (Lenguaje de Marcas para Inalámbricos).

La estandarización de aplicaciones se lleva a cabo principalmente dentro del marco del Consorcio del World Wide Web (W3C), liderado por Tim Berners-Lee. Es interesante señalar que a pesar de su alta relevancia para Internet, hasta el momento W3C no ha atraído mucha atención dentro del debate de Gobernanza de Internet.


## CÓDIGO ABIERTO

El software de código abierto está disponible sin cargo alguno y permite modificaciones por parte de sus usuarios. Las aplicaciones de código abierto son desarrolladas por programadores alrededor del mundo que trabajan utilizando el mismo código.

Al ser introducido, el código abierto prometía ser una alternativa eficiente ante los costosos programas de software patentados. Linux es la iniciativa de código abierto mejor conocida. La proliferación de software de código abierto ha sido más lenta de lo esperado, debido principalmente a la falta de soporte técnico sólido. La decisión más reciente de algunas partes interesadas clave, como IBM e Intel, de utilizar Linux como plataforma principal de código abierto, podría conducir al exitoso desarrollo de esta iniciativa.

Por otra parte, existe un renovado interés en el código abierto con un nuevo nombre y un concepto ligeramente modificado, denominado FLOSS (Software de Código Abierto Libre). La principal diferencia entre el código abierto y FLOSS, es que este último permite el acceso libre al código sin requerir ningún registro.

El código abierto es a menudo citado como la solución para el desarrollo de capacidades tecnológicas de infocomunicaciones en los países en desarrollo. En la CMSI, el intento de la sociedad civil y de algunos países en desarrollo de introducir código abierto y FLOSS en el documento final como una solución para superar la barrera digital, fue diluido con una referencia general a "diferentes modelos de software, incluyendo software patentado, código abierto y libre".


## CONVERGENCIA: INTERNET-TELECOMUNICACIONES-ULTIMEDIOS

El uso amplio y preponderante de los Protocolos de Internet ha disparado el proceso de convergencia de los sistemas de telecomunicaciones, multimedios y entretenimiento. Hoy en día, es posible realizar llamadas telefónicas, escuchar la radio, ver televisión y compartir música a través de Internet. En el campo de las telecomunicaciones tradicionales, el principal punto de convergencia es la Voz sobre el Protocolo de Internet (VoIP). La creciente popularidad de VoIP se basa en su menor precio, la posibilidad de integrar las líneas de comunicación de datos y voz, así como el uso de herramientas avanzadas basadas en computación. TCP/IP también se está volviendo dominante en el campo de los multimedios y el entretenimiento. Mientras que la convergencia técnica avanza a un ritmo acelerado, sus consecuencias económicas y legales requerirán de algún tiempo para evolucionar.

### LOS ASUNTOS

#### Las Implicaciones Económicas de la Convergencia

A nivel económico, la convergencia ha empezado a dar nueva forma a los mercados tradicionales colocando en directa competencia a empresas que anteriormente operaban en dominios separados. Todavía queda por ver quién tomará la delantera en este mercado cada vez más convergente, si empresas de telecomunicaciones como MCI o empresas de tecnologías de infocomunicaciones como IBM.

Lo mismo aplica al mercado de los multimedios. Sin embargo, ante el desafío que plantea la convergencia en este campo, algunas empresas han reaccionado recurriendo al desarrollo conjunto de herramientas informáticas y medios/entretenimiento o al establecimiento de alianzas. Sony es una empresa que ha desarrollado capacidades de tecnología de infocomunicaciones y entretenimiento/medios. La fusión de America Online y Time Warner pretendía lograr la combinación de telecomunicaciones y medios/entretenimiento. Ahora, AOL/Time Warner ha unido bajo un solo paraguas corporativo a proveedores de servicios de Internet, canales de televisión, música y desarrolladores de software.

### La Necesidad de Establecer un Marco Legal

El sistema legal fue el más lento en ajustarse a los cambios producidos por la convergencia tecnológica y económica. Cada uno de estos segmentos: telecomunicaciones, medios/entretenimiento e infocomunicaciones, tiene su propio marco regulatorio especial.

Esta convergencia plantea varias preguntas sobre gobernanza y regulación: ¿Qué va a suceder con los regímenes nacionales e internacionales existentes en los campos de la telefonía y la radiodifusión? ¿Serán desarrollados nuevos regímenes enfocados exclusivamente en Internet? ¿La convergencia debe ser regulada por las autoridades públicas (estados y organismos internacionales) o debe permitirse la autorregulación?

Algunos países como Malasia y Suiza, así como la Unión Europea, han empezado a brindar respuestas a estas preguntas. Malasia adoptó su Ley de Comunicaciones y Multimedios en 1998, estableciendo un marco general para la regulación de la convergencia. Las nuevas directrices que otorga el marco de la Unión Europea y que empiezan a trasponerse en las legislaciones nacionales, también constituyen un paso en esta dirección, así como las leyes y regulaciones de telecomunicaciones adoptadas en Suiza.

### El Riesgo de la Convergencia de los Operadores de Cable y los ISPs

En muchos países, el Internet de banda ancha ha sido introducido por medio de las redes de televisión por cable. Esto es especialmente cierto en los Estados Unidos, donde el Internet por cable es mucho más frecuente que el ADSL, la otra opción principal de Internet de banda ancha. ¿Cuáles son los riesgos asociados con esta convergencia?

Algunas partes discuten que los operadores de cable siendo amortiguadores entre los usuarios e Internet podrían desafiar el principio de redes punto a punto.

La principal diferencia entre la conexión tradicional por marcación y el cable es que el cable no es regulado por las llamadas reglas del "portador común". Estas reglas que aplican al sistema de telefonía, especifican que el acceso no debe producir discriminaciones. Los operadores de cable no están sujetos a estas reglas, lo que les otorga un control total sobre el acceso a Internet de sus abonados. Tienen la capacidad de bloquear el uso de ciertas aplicaciones y controlar el acceso a ciertos materiales. Las posibilidades de vigilancia y consecuentemente de violación de la privacidad son mucho mayores en el Internet por cable ya que el acceso es con-

trolado por medio de un sistema similar al de las redes de área local, es decir un mayor control directo de los usuarios.

En un documento sobre este tema, la Unión Americana de Libertades Civiles ofrece el siguiente ejemplo de los riesgos que conllevan los monopolios de Internet por cable: "Es como si a la empresa de teléfonos se le permitiera ser dueña de restaurantes y luego brindar señales claras y buen servicio a los clientes que llaman a Domino's y señales frecuentes de ocupado, desconexiones y estática a quienes llaman a Pizza Hut".

Este problema de convergencia será resuelto cuando se decida si el Internet por cable es un "servicio de información" o un "servicio de telecomunicaciones". En caso de ser el segundo, tendrá que ser regulado por medio de las reglas del portador común.

## SEGURIDAD EN INTERNET

### LA SITUACIÓN ACTUAL

La seguridad en Internet se empezó a ver con mayor claridad como resultado de la rápida expansión en la base de usuarios de Internet. Internet ha demostrado lo que muchos sospechaban desde hace tiempo: la tecnología puede ser tanto una oportunidad como una amenaza. Lo que puede ofrecer una situación de ventaja para la sociedad también puede convertirse en desventaja.

La seguridad de la información se discute en mayor detalle en otros tres folletos de esta serie:

- Prácticas de buena higiene para datos y computadoras personales
- ILa seguridad de la Información y las organizaciones
- Activismo de piratas informáticos, Ciberterrorismo y Ciberguerra

El efecto colateral de la rápida integración de Internet a casi todos los aspectos de las actividades humanas aumenta la vulnerabilidad de la sociedad moderna. Infraestructuras críticas, incluyendo las redes de suministro eléctrico, los sistemas de transporte, y los servicios de salud son todos parte de una red global potencialmente expuesta a ciberataques. Debido a que se sabe que los ataques a estos sistemas causan tras-

tornos severos y tienen un impacto financiero potencialmente alto, las infraestructuras críticas se constituyen en blancos frecuentes.

Los temas de seguridad en Internet pueden ser clasificados de acuerdo a tres criterios: tipo de acción, tipo de autor y tipo de objetivo.

Una clasificación basada en el tipo de acción incluiría: intercepción de datos, interferencia en los datos, acceso ilegal, software de espionaje y robo de identidad. Los posibles actores podrían ser piratas informáticos, cibercriminales, ciberguerreros o ciberterroristas.

Los objetivos potenciales son numerosos, desde individuos, empresas privadas e instituciones públicas hasta infraestructuras críticas, gobiernos y activos militares

### INICIATIVAS DE POLÍTICAS EN EL CAMPO DE SEGURIDAD EN INTERNET

Hay muchas iniciativas nacionales, regionales y globales enfocadas en la seguridad en Internet.

A nivel nacional se cuenta con un creciente número de legislación y jurisprudencia que trata con la seguridad en Internet. Las más prominentes son las iniciativas estadounidenses relacionadas con una más amplia autoridad gubernamental debido a su lucha contra el terrorismo. El Departamento de Seguridad Nacional es la principal institución encargada de los asuntos de seguridad en Internet. Es difícil encontrar algún país, principalmente desarrollado, que no cuente con alguna iniciativa enfocada hacia la seguridad en Internet.

A nivel internacional, las organizaciones más activas han sido la OCDE (Organización de Cooperación y Desarrollo Económico), que produjo sus Pautas sobre Seguridad en Internet, y la UIT, que ha producido un gran número de marcos de seguridad, arquitecturas y estándares, incluyendo X.509, el cual brinda la base para la infraestructura de llave pública (PKI), utilizada por ejemplo en la versión segura de http (https).

El Grupo de los Ocho (G-8) también ha propuesto unas cuantas iniciativas en el campo de la seguridad en Internet, como por ejemplo mejorar la cooperación entre las agencias de seguridad. El G8 también constituyó un Subgrupo dedicado a los Crímenes de Alta Tecnología encargado de establecer comunicaciones 24x7 entre los diferentes centros de ciberseguridad y los estados miembros, de capacitar al personal, y de mejorar los sistemas legales en las naciones con el fin de combatir el ciberdelito y

promover la cooperación entre la industria de tecnología de infocomunicaciones y las agencias de seguridad.

La Asamblea General de las Naciones Unidas ha aprobado varias resoluciones anuales sobre "Avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional", específicamente las resoluciones 53/70 de 1998, 54/49 de 1999, 55/28 de 2000, 56/19 de 2001, 57/239 de 2002 y 58/199 de 2003. Desde 1998, las resoluciones han venido presentando contenidos similares sin aportar mejoras significativas. No se percibe un reflejo de los cambios considerables que han tenido lugar en el campo de la seguridad en Internet desde 1998.

Un instrumento legal importante relacionado con la seguridad en Internet es la Convención sobre Ciberdelito del Consejo de Europa que entró en vigencia el 1 de julio de 2004.

Algunos países han establecido acuerdos bilaterales. Los Estados Unidos cuenta con acuerdos bilaterales de cooperación legal en asuntos criminales con más de 20 países. Estos acuerdos también se utilizan en casos de ciberdelito.

Un intento de los académicos y de las partes interesadas no estatales de redactar un acuerdo internacional es el Proyecto de Stanford para la Convención sobre la Protección contra el Ciberdelito y el Terrorismo . Este proyecto recomienda el establecimiento de un organismo internacional llamado la Agencia para la Protección de la Infraestructura de la Información (AIIP por sus siglas en inglés)

## LOS ASUNTOS

### La Arquitectura de Internet y la Seguridad

La naturaleza misma de la organización de Internet afecta su seguridad. ¿Debemos continuar el enfoque actual de desarrollar la seguridad sobre una base preexistente no segura o debemos modificar algo en la base de la infraestructura de Internet? ¿De qué manera afectaría este cambio las demás características de Internet, especialmente su apertura y transparencia? La mayor parte del desarrollo previo de los estándares de Internet estaba dirigido a mejorar el desempeño e introducir nuevas aplicaciones. La seguridad no ha sido nunca una prioridad.

No queda claro si el IETF podrá cambiar los estándares de correo electrónico y brindar autenticación lo que en último término reduciría el uso incorrecto de Internet (p. ej. correo electrónico indeseado y ciber-

delito). Dada la controversia que rodea cualquier cambio en los estándares básicos de Internet, es probable que las mejoras relacionadas con la seguridad del Protocolo de Internet básico sean graduales y lentas. El sector comercial y otras partes interesadas en obtener soluciones más rápidas podrían empezar a desarrollar nuevas capas, "Internet Inteligente", que facilitarían, entre otras cosas, comunicaciones más seguras en Internet.

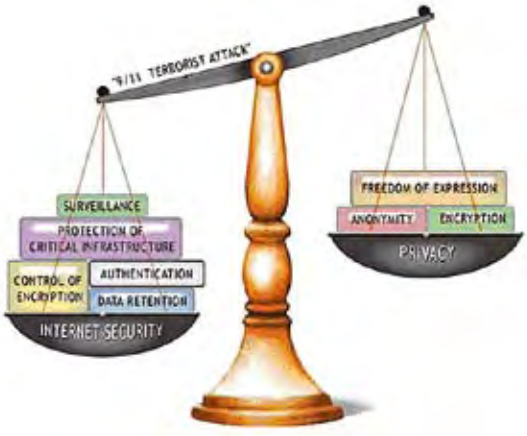
### Comercio Electrónico y Seguridad en Internet

La seguridad es mencionada a menudo como una de las condiciones básicas para un crecimiento más acelerado del comercio electrónico. Sin seguridad y confiabilidad en Internet, los clientes continuarán renuentes a brindar información confidencial en línea, como sus números de tarjetas de crédito. Lo mismo aplica para la banca en línea y el uso de dinero electrónico.

### Privacidad y Seguridad en Internet

Otro tema debatido es la relación entre seguridad y derechos humanos. ¿El aumento en la seguridad de Internet implica una pérdida en la privacidad? ¿Cómo debe regularse el uso del software de codificación, el cual puede ser utilizado tanto para la protección legítima de la privacidad en las comunicaciones como para la protección de comunicaciones ilegales de terroristas y criminales? Este equilibrio entre seguridad en Internet y derechos humanos cambia constantemente.

En el periodo subsiguiente al "9/11", la seguridad se convirtió en una prioridad en los Estados Unidos, lo cual se vio reflejado en la adopción de diferentes leyes nacionales que prescribían, entre otras cosas, mayores niveles de vigilancia en Internet. La reacción de la sociedad civil se enfoca en los riesgos para la privacidad y el concepto de libertad de expresión.




La cuestión del equilibrio entre la seguridad informá-

tica y la privacidad fue resaltado durante discusiones sobre la posibilidad de extender a nivel global el Consejo de la Convención Europea sobre Ciberdelito. La principal objeción de los activistas de derechos humanos es que la convención enfrenta los temas de seguridad de Internet a expensas de la protección de la privacidad y otros derechos humanos.


## CODIFICACIÓN

Uno de los puntos centrales de discusión sobre seguridad en Internet es la codificación, es decir la utilización de herramientas para proteger las comunicaciones de datos.

El software de codificación mezcla las comunicaciones electrónicas (correos electrónicos, imágenes) y las convierte en texto ilegible utilizando algoritmos matemáticos. El equilibrio entre la necesidad de los particulares de mantener algunas comunicaciones en confidencia y la de los gobiernos y agencias de inteligencia de monitorear actividades potencialmente criminales y terroristas sigue siendo tema de controversia.

Los aspectos internacionales de la política de codificación son relevantes para la discusión sobre Gobernanza de Internet ya que la regulación sobre la codificación debe ser global o al menos involucrar a aquellos países capaces de producir herramientas para la misma.

Por ejemplo, la política estadounidense de control de exportaciones de software de codificación no resultó muy exitosa debido a que no podía controlar la distribución internacional del mismo. Las empresas de software en los Estados Unidos iniciaron una campaña de cabildeo argumentando que los controles a la exportación no aumentan la seguridad nacional sino que socavan los intereses comerciales del país.

### REGÍMENES INTERNACIONALES PARA LAS HERRAMIENTAS DE CODIFICACIÓN

La codificación ha sido abordada en dos contextos: el Acuerdo Wassenaar y la OCDE. El Acuerdo Wassenaar es un régimen internacional adoptado por 33 países industrializados para restringir la exportación de armas convencionales y tecnologías de "uso dual" a países en guerra

o "estados paria". El acuerdo establece su secretaría en Viena. El cabildeo llevado a cabo en los Estados Unidos junto con el Grupo Wassenaar tenía como propósito extender la "Iniciativa Clipper" a nivel internacional, controlando el software de codificación por medio de un depósito de claves. Esto fue rechazado por muchos países, especialmente Japón y las naciones escandinavas.

En 1998 se alcanzó un acuerdo al introducir directrices de criptografía que incluían en la lista de productos de uso dual los productos de hardware y software de criptografía de más de 56 bits. Esta extensión incluyó herramientas de Internet como los navegadores web y el correo electrónico. Es interesante resaltar que esta iniciativa no cubre transferencias "intangibles" como las descargas. La incapacidad de introducir una versión internacional de "Clipper" contribuyó al retiro de esta propuesta a nivel interno en los Estados Unidos. En este ejemplo de la relación entre el ámbito nacional e internacional, los desarrolladores internacionales tuvieron un impacto decisivo sobre los nacionales.

OCDE fue otro foro de cooperación internacional en el campo de la codificación. Aunque OCDE no produce documentos legalmente vinculantes, sus directrices en diferentes temas son altamente respetadas debido a que son el resultado de un enfoque experto y un proceso de toma de decisiones por consenso. La mayoría de sus directrices son eventualmente incorporadas en leyes a nivel nacional. El tema de la codificación fue sumamente controversial dentro de las actividades de OCDE. Fue traído a colación en 1996 como resultado de una propuesta de los Estados Unidos de adoptar un depósito de claves como estándar internacional. De modo similar a Wassenaar, las negociaciones relacionadas con la propuesta estadounidense de adoptar un depósito de claves con estándares internacionales enfrentaron una fuerte oposición de parte de Japón y los países escandinavos. El resultado fue una especificación de compromiso sobre los principales elementos de las políticas de codificación.

Algunas tentativas de desarrollar un régimen internacional de codificación, principalmente dentro del contexto del Acuerdo Wassenaar, no dieron como resultado el desarrollo de un régimen internacional efectivo. Aun es posible obtener en Internet software de codificación sumamente poderoso.


## CORREO ELECTRÓNICO INDESEADO (SPAM)

### LA SITUACIÓN ACTUAL

El spam o correo electrónico indeseado es usualmente definido como correo electrónico no solicitado enviado a un gran número de usuarios de Internet. El correo electrónico indeseado es utilizado principalmente para la promoción comercial. Algunos otros usos incluyen: activismo social, campañas políticas, y la distribución de materiales pornográficos. El correo electrónico indeseado está incluido en la canasta de infraestructura ya que impide el funcionamiento normal de Internet al impactar una de su aplicaciones clave: el correo electrónico. Es uno de los temas de Gobernanza de Internet que afecta a casi todas las personas que se conectan a Internet. De acuerdo con las estadísticas más recientes, de cada 13 mensajes de correo electrónico, aproximadamente 10 pueden ser categorizados como correo electrónico indeseado. Dejando de lado el hecho de que es molesto, el correo electrónico indeseado provoca además pérdidas económicas considerables, tanto en términos del ancho de banda utilizado como del tiempo perdido revisándolo/borrándolo. Un estudio sobre el correo electrónico indeseado comisionado recientemente por la Unión Europea reportó que solamente la pérdida anual en términos de capacidad de ancho de banda representa unos €10,000 millones.

El correo electrónico indeseado puede ser combatido tanto por medios técnicos como legales. En la parte técnica, existen muchas aplicaciones para filtrar mensajes y detectar correo electrónico indeseado. El principal problema con los sistemas de filtrado es que se sabe que también borran mensajes deseados. La industria que combate el correo indeseado es un sector creciente que ofrece aplicaciones cada vez más sofisticadas capaces de distinguir correo electrónico indeseado de mensajes regulares. Los métodos técnicos solamente tienen un impacto limitado y deben ser complementados con medidas legales específicas.

En la parte legal, muchas naciones han reaccionado introduciendo legislación antispam. En los Estados Unidos, la Ley Can-Spam establece un delicado balance entre permitir correos electrónicos promocionales y la prevención del correo electrónico indeseado. A pesar de que la ley prescribe condenas severas para la distribución de correo electrónico indeseado, incluyendo penas de prisión de hasta cinco años; según los críticos algunas de estas disposiciones toleran o pueden incluso motivar el envío del mismo. La posición inicial por defecto establecida en la legislación es que el correo electrónico no solicitado es permitido hasta que el receptor del mismo pida que se detenga (por medio de una cláusula de retiro). Desde la aprobación de la ley en diciembre 2003, las estadísticas no evidencian una disminución en el número de mensajes de correo electrónico indeseados.

En julio 2003, la Unión Europea introdujo su propia legislación para combatir el correo indeseado como parte de su directiva sobre privacidad y comunicaciones electrónicas. A pesar de que la unión europea solicitó a sus estados miembros implementar esta ley para combatir el correo indeseado antes del final de 2003, nueve estados miembros decidieron no respetar la fecha límite. La legislación de la unión europea motiva la autorregulación y las iniciativas del sector privado que puedan conducir a la reducción del correo electrónico indeseado.

## LA RESPUESTA INTERNACIONAL

Tanto las leyes para combatir el correo indeseado adoptadas en los Estados Unidos como en la Unión Europea tienen una debilidad: la falta de previsión para la prevención del correo electrónico indeseado enviado desde otros países. Este tema es particularmente relevante para algunos países como Canadá, el cual según las últimas estadísticas recibe 19 de cada 20 mensajes indeseados de otros países. El Ministro de Industria Canadiense, Lucienne Robillard, declaró recientemente que el problema no puede ser resuelto "país por país". Una conclusión similar fue presentada por un estudio sobre la legislación contra el correo electrónico indeseado (realizado por el Instituto de Derecho de la Información de la Universidad de Ámsterdam: "El simple hecho de que la mayor parte del correo electrónico indeseado provenga de países externos a la Unión Europea, restringe considerablemente la efectividad de las Directivas que esta emita. Se requiere una solución global, implementada por medio de tratados internacionales u otros mecanismos similares.

Un Memorando de Entendimiento firmado por Australia, Corea, y el Reino Unido es uno de los primeros ejemplos de cooperación internacional en la campaña para combatir el correo indeseado.

OCDE estableció una Fuerza de Tareas para correo electrónico no deseado y preparó un conjunto de herramientas para combatir el correo indeseado. La UIT también ha sido proactiva al organizar la Reunión Temática para Combatir el Correo Indeseado (7-9 de julio de 2004) y considerar diferentes posibilidades para establecer el Memorando Global de Entendimiento para Combatir el Correo Electrónico Indeseado. A nivel regional, la Unión Europea estableció la Red de Agencias de Seguridad para Combatir el Correo Indeseado y la Cooperación Económica del Asia Pacífico preparó un conjunto de Guías para el Consumidor.

El Correo Electrónico Indeseado y el Desarrollo

Spam is causing serious, but still manageaEs correo indeseado está causando dificultades serias, aunque aún manejables, en los países en desarrollo, y además paraliza la infraestructura de Internet en muchos de ellos. Debido a que la infraestructura de Internet es de baja velocidad y se encuentra subdesarrollada, el correo indeseado amenaza el acceso básico a Internet de muchos usuarios en los países en desarrollo. Estos países usualmente no cuentan con los recursos técnicos y la pericia requeridos para combatir el correo indeseado. Consecuentemente, el correo indeseado aumenta la brecha digital entre los países desarrollados y en desarrollo.

Otro enfoque posible para combatir el correo electrónico indeseado fue asumido por las principales empresas de Internet dedicadas a hospedar cuentas de correo electrónico: America Online, British Telecomm, Comcast, EarthLink, Microsoft, y Yahoo!. Estas establecieron la Alianza Técnica Contra el Correo Electrónico Indeseado (ASTA por sus siglas en inglés) cuya tarea principal es coordinar actividades técnicas y políticas en la lucha contra el correo indeseado.

## LOS ASUNTOS

### Diferentes Definiciones de Correo Electrónico Indeseado

Las diferentes perspectivas en el concepto de correo electrónico indeseado afectan las campañas para combatirlo. En los Estados Unidos, la preocupación generalizada por la protección de la libertad de expresión y la Primera Enmienda de la Constitución afecta también la campaña contra el correo electrónico indeseado. Los legisladores en los Estados Unidos consideran el correo electrónico indeseado como "correo electrónico comercial no solicitado" dejando por fuera otros tipos como el activismo

político y la pornografía. En muchos otros países, el correo electrónico indeseado es cualquier "envío masivo de correo electrónico no solicitado" sin importar su contenido. Debido a que la mayor parte del correo electrónico indeseado proviene de los Estados Unidos, esta diferencia en las definiciones limita seriamente cualquier posibilidad de introducir mecanismos internacionales efectivos para combatirlo.

### Correo Electrónico Indeseado y Autenticación de Correo Electrónico

Uno de los generadores estructurales de correo indeseado es la posibilidad de enviar mensajes de correo electrónico utilizando una dirección falsa de envío. Existe una solución técnica posible para este problema, la cual requeriría cambios en los estándares actuales de Internet. El IETF está trabajando en la introducción de cambios en su protocolo de correo electrónico con el fin de garantizar la autenticación del mismo. Este es un ejemplo de cómo los aspecto técnicos (estándares) pueden afectar una política. Un posible beneficio que podría generar la introducción de autenticación de e-mail sería poner un freno al anonimato en Internet.

### La Necesidad de Implementar Acción a Nivel Global

Como indicamos anteriormente, la mayor parte del correo electrónico indeseado proviene de otros países. Se trata de un problema global que requiere una solución global. Existen varias iniciativas que podrían conducir a una mejor cooperación global. Ya hemos mencionado algunas de ellas, como los Memorandos de Entendimiento Bilaterales (MOUs por sus siglas en inglés). Otras incluyen acciones como el desarrollo de capacidades y el intercambio de información. Una solución más integral involucraría algún tipo de instrumento global para combatir el correo indeseado. Algunos participantes en la última reunión de UIT propusieron la adopción de un MOU multilateral o la adopción de un instrumento en el contexto de la CMSI. Hasta el momento, los países desarrollados prefieren fortalecer su legislación nacional con campañas bilaterales o regionales. Dada su posición desventajosa al ser receptores de "un mal público global" que se origina principalmente en los países desarrollados, la mayor parte de los países en desarrollo están interesados en producir una respuesta global ante el problema del correo electrónico indeseado.

SECTION 3

# La Canasta Legal

## LA CANASTA LEGAL

Prácticamente todos los aspectos relacionados con la Gobernanza de Internet incluyen algún componente legal, sin embargo, la preparación de una respuesta legal ante el rápido desarrollo de Internet aún se encuentra dando sus primeros pasos. Los dos enfoques más frecuentes ante los aspectos legales de Internet son:

a) El enfoque del derecho "real" en el cual Internet recibe básicamente el mismo trato que otras tecnologías de telecomunicaciones, desde las señales de humo hasta el teléfono. A pesar de que Internet es un medio de comunicación más rápido e integral, continua comunicando individuos a distancia. Por este motivo, es factible aplicar a Internet las normas legales existentes.
b) El enfoque de "ciberlegislación" se basa en el supuesto de que Internet introduce nuevos tipos de relaciones sociales en el ciberespacio. Consecuentemente, existe una necesidad de formular nuevas "ciberleyes" para el ciberespacio. Un argumento a favor de este enfoque es que la sola velocidad y volumen de las comunicaciones internacionales facilitadas por Internet dificulta la aplicación de las normas legales existentes.

Aunque ambos enfoques ofrecen elementos válidos, el enfoque del derecho real está predominando tanto en el análisis teórico como en las políticas. El pensamiento general es que una parte considerable de la legislación existente puede ser aplicada a Internet. Sin embargo, en casos como la protección de las marcas registradas, la legislación real tendría que ser adaptada de manera que cubra el mundo cibernético. Otros casos, como el correo electrónico indeseado o spam, deberán ser regulados por leyes nuevas ya que la analogía más cercana al spam en el mundo físico, es decir el correo chatarra, no es ilegal.

Esta discusión sobre las inquietudes legales se divide en dos partes: mecanismos legales y asuntos legales.

## MECANISMOS LEGALES

Los siguientes mecanismos legales ya han sido aplicados o podrían ser aplicados a la Gobernanza de Internet:

- Legislación;
- Normas Sociales (costumbres);
- Autorregulación;
- Regulación por medio de código (solución de software) [p. 22];
- Jurisprudencia (decisiones de los tribunales de justicia);
- Derecho internacional.

### Legislación

Todas las disposiciones legales están compuestas por reglas y sanciones. Las reglas establecen ciertos comportamientos aceptados (no cometer un crimen, pagar impuestos) y las sanciones especifican las consecuencias en caso de que las reglas no sean respetadas (p. ej. multas, penas de prisión, pena capital).

Sin importar cuál enfoque sea más apropiado, el "real" o el "cibernético", el principio general sigue siendo que las leyes no impiden el comportamiento prohibido, solamente lo castigan. El hecho de que el fraude esté prohibido tanto en el mundo "cibernético" como en el "real" no significa que el fraude será automáticamente erradicado. Esta distinción es relevante ya que uno de los argumentos frecuentes para establecer regulaciones independientes para el ciberespacio es que el comportamiento prohibido (fraude, crimen, etc.) es de por sí frecuente en este medio y que el derecho "real" no podría ser implementado con eficiencia.

Las actividades legislativas se han intensificado progresivamente en el campo de Internet. Esto sucede principalmente en los países de la OCDE, en los cuales las infocomunicaciones se han extendido ampliamente y tienen un alto grado de impacto en las relaciones económicas y sociales. Hasta el momento, las áreas prioritarias para las regulaciones legislativas han sido la privacidad, la protección de datos, la propiedad intelectual, las cargas fiscales y el cibercrimen.

Sin embargo, las relaciones sociales son demasiado complejas para ser reguladas únicamente por legisladores. La sociedad es dinámica y la legislación siempre va a la zaga del cambio. Esto es particularmente notable hoy en día, ya que el desarrollo tecnológico está dando nueva forma a la realidad social a un ritmo más acelerado que las reacciones de los legisladores. Algunas veces las reglas se vuelven obsoletas incluso antes de haber sido adoptadas. El

riesgo de la obsolescencia legal constituye una consideración importante en la regulación de Internet.

Gobernanza de la Sociedad de la Información

El derecho siempre va a la zaga de la tecnología

**Normas Sociales (Costumbres)**

Al igual que la legislación, las normas sociales prescriben ciertos comportamientos. A diferencia de la legislación, ningún poder estatal impone estas normas. Estas son impuestas por la comunidad a través de la presión de los pares. En los primeros días, el uso de Internet estaba regulado por un conjunto de normas sociales llamadas "netiquette" o etiqueta en la red, cuyas principales sanciones eran la presión de los pares y la exclusión. Durante este periodo, en el cual Internet era utilizada principalmente por comunidades relativamente pequeñas y principalmente académicas, las reglas sociales eran ampliamente respetadas. El crecimiento de Internet ha hecho que estas reglas se vuelvan ineficientes. Sin embargo, este tipo de regulación todavía puede ser utilizada dentro de grupos restringidos y con fuertes lazos comunitarios.

**Autorregulación**

El Libro Blanco sobre Gobernanza de Internet (1998) publicado por el gobierno de los Estados Unidos propone la autorregulación como mecanismo principal de regulación en Internet. La autorregulación comparte algunos elementos con las normas sociales descritas anteriormente. La principal diferencia es que en contraste con las normas sociales, las cuales típicamente involucran un sistema regulador difuso, la autorregulación se basa en un enfoque intencional y bien organizado. Las reglas de la autorregulación usualmente se codifican en códigos de práctica o buena conducta.

La tendencia hacia la autorregulación es particularmente notable entre los Proveedores de Servicios de Internet (ISPs). En muchos países, los ISPs están recibiendo cada vez más presión por parte de las autoridades

gubernamentales para imponer reglas relacionadas con políticas de contenido. Los ISPs cada vez recurren con mayor frecuencia a la autorregulación como método para imponer ciertos estándares de comportamiento y, en última instancia, prevenir la interferencia gubernamental en sus actividades.

Aunque la autorregulación puede ser una técnica reguladora provechosa, todavía presenta algunos riesgos en la regulación de áreas de alto interés público, como las políticas de contenido. Queda por ver hasta qué punto los ISPs podrán regular el contenido alojado en sus sitios Web. ¿Podrán tomar decisiones en sustitución de las autoridades legales? ¿Podrán los ISPs juzgar qué tipo de contenido es aceptable? También es necesario referirse a otros temas como la libertad de expresión y la privacidad.

### Jurisprudencia

La jurisprudencia (decisiones de los tribunales de justicia) constituye un elemento importante en el sistema legal estadounidense, el primero en tratar asuntos legales relacionados con Internet. En este sistema, los precedentes constituyen la ley, especialmente en casos que involucran la regulación de asuntos nuevos, como es el caso de Internet. Los jueces deben decidir los casos incluso si no cuentan con las herramientas necesarias, es decir las normas legales.

La primera herramienta legal que utilizan los jueces es la analogía legal, en la cual algo nuevo es relacionado con algo conocido. La mayoría de los casos legales relacionados con Internet se resuelven por medio de analogías. En las páginas 23 a 26 se presenta una lista de analogías para Internet.

### Regulación Internacional

Una perspectiva común sobre la Gobernanza de Internet es que su naturaleza global requiere una regulación global. La necesidad de contar con un enfoque global es a menudo confirmada por la falta de efectividad de las medidas nacionales para combatir el spam, el cibercrimen y otras actividades indeseadas. El régimen de aviación civil es usualmente mencionado como ejemplo de un régimen universal exitoso en la lucha contra el crimen. "Desde la adopción de los tratados de aviación civil, el sabotaje y los actos de interferencia ilícita han declinado consistentemente". Una de las principales razones es que con la cobertura legal universal de la aviación civil, los criminales ya no pueden encontrar un "refugio seguro". Sin em-

bargo, la importancia de un enfoque global no quiere decir que algunos asuntos no puedan o deban ser regulados a nivel nacional o regional.

La regulación global requiere de consenso universal, y este solamente puede ser alcanzado por medio de largos procesos de negociación, los cuales no siempre producen los frutos esperados. Diferentes mecanismos legales internacionales pueden ser utilizados en el desarrollo de un régimen de Gobernanza de Internet. Según el Estatuto de la Corte Internacional de Justicia, los recursos legales internacionales se dividen en tratados, costumbres y principios generales. Por encima de estos se encuentra la "legislación blanda", un recurso de creciente importancia en el derecho internacional.

**Los Tratados.** Actualmente, la única convención que se enfoca directamente en asuntos relacionados con Internet es la Convención sobre Cibercrimen del Consejo de Europa. Otras convenciones y tratados se aplican solo parcialmente a Internet. Un ejemplo es el corpus de las convenciones sobre derechos humanos. La libertad de expresión se encuentra protegida en el Artículo 19 del Pacto Internacional sobre Derechos Civiles y Políticos. Otros derechos relacionados con Internet, como la privacidad y el derecho a la información han sido regulados por medio de instrumentos globales y regionales de derechos humanos. En el campo de la resolución de disputas, uno de los principales instrumentos es la Convención de Nueva York sobre Arbitraje.

El enfoque imperante sobre la Gobernanza de Internet (nacional vrs. internacional, legislación blanda vrs. dura) finalmente influenciará el tipo y la forma de la convención sobre Gobernanza de Internet, en caso de alcanzarse alguna. Algunos discuten que Internet requerirá un instrumento legal integral similar a la Convención sobre el Derecho del Mar. Esta analogía no es apropiada, debido a que la negociación del Derecho del Mar involucraba la codificación del derecho consuetudinario histórico y la integración de cuatro convenciones existentes.

En Internet, no existe derecho consuetudinario. Está siendo formado constantemente y muchos enfoques y experimentos de prueba y error han sido intentados. En lugar de un tratado integral de Internet, es más probable que varios instrumentos independientes sean adoptados.

**Derecho consuetudinario.** El desarrollo del derecho consuetudinario usualmente requiere un lapso mayor para la cristalización de algunas prácticas legalmente vinculantes. Esto era posible en el pasado. Sin embargo, el desarrollo tecnológico posterior a la Segunda Guerra Mundial

requirió el rápido desarrollo de marcos reguladores internacionales dadas las profundas consecuencias económicas y políticas producidas por estos cambios en un periodo muy corto de tiempo. Internet es un buen ejemplo de esta tendencia. Es poco probable que el derecho consuetudinario juegue un rol dominante en el régimen emergente de Gobernanza de Internet.

**Legislación "Blanda".** La legislación blanda usualmente se relaciona con diferentes documentos políticos como declaraciones, directrices y legislaciones modelo. El criterio lingüístico para identificar una legislación "blanda" es el frecuente uso de la palabra "debería" en lugar de "deberá", que usualmente se asocia con un enfoque de mayor vinculación legal codificado en una legislación "dura" (tratados).

Diferentes instancias de legislación blanda han sido respetadas por los estados participantes. Algunas de ellas han obtenido considerable importancia, como el Pacto de Helsinki de 1975 por medio del cual se estableció un marco para las relaciones entre Oriente y Occidente. La legislación blanda es utilizada por los estados por diferentes motivos, tales como aumentar la mutua confianza, estimular el desarrollo en progreso, e introducir nuevos mecanismos legales y gubernamentales. La legislación blanda puede ser una técnica legal potencialmente aplicable a la Gobernanza de Internet.


## JURISDICCIÓN

### INTRODUCCIÓN

La jurisdicción es el tema relacionado con Gobernanza de Internet que requiere atención inmediata. La cantidad de disputas relacionadas con Internet ha venido aumentando consistentemente. La confusión sobre la jurisdicción podría tener dos consecuencias inmediatas:

- la incapacidad del estado de ejercer su poder legal como entidad responsable de regular las relaciones sociales dentro de su territorio o la incapacidad de los individuos y entidades legales de ejercer su derecho a la justicia (denegación de justicia).

Otras consecuencias potenciales de una jurisdicción ambigua pueden ser:

- inseguridad legal en Internet;
- más lento desarrollo del comercio electrónico;
- compartimentación de Internet en zonas legalmente seguras.

### ¿Cuál es la relación entre jurisdicción e Internet?

La jurisdicción se basa principalmente en la división geográfica del mundo en territorios nacionales. Cada estado tiene el derecho soberano de ejercer jurisdicción sobre su territorio. Sin embargo, Internet facilita intercambios considerables entre países, los cuales son difíciles (mas no imposibles) de monitorear utilizando mecanismos gubernamentales tradicionales. La cuestión de la jurisdicción en Internet expone uno de los principales dilemas asociados con la Gobernanza de este medio: ¿cómo se puede "anclar" a Internet dentro de la geografía legal y política existente?

### Jurisdicción – Técnicas Básicas

Existen tres aspectos principales en el tema de la jurisdicción:

- ¿Cuál tribunal o autoridad estatal cuenta con la autoridad apropiada? (jurisdicción procesal);
- ¿Cuáles reglas deben ser aplicadas? (jurisdicción sustantiva);
- ¿Cómo pueden ser implementadas las decisiones de los tribunales? (jurisdicción exequátur).

Los siguientes criterios principales se utilizan para establecer jurisdicción en casos particulares:

- Vínculo Territorial – el derecho del estado de regir a las personas y propiedades dentro de su territorio;
- Vínculo Personal – el derecho de un estado de regir sobre sus ciudadanos sin importar dónde se encuentren;
- Vínculo de Efectos – el derecho del estado de regir sobre los efectos económicos y legales en un territorio en particular, producto de actividades conducidas en un lugar diferente.

Otro principio importante del derecho internacional moderno es el principio de jurisdicción universal en casos que involucran el incumplimiento de normas legales internacionales principales (ius cogens) como por ejemplo genocidio y piratería.

## LA SITUACIÓN ACTUAL

Los problemas con la jurisdicción surgen cuando las disputas involucran un componente extraterritorial (p. ej. involucra individuos de diferentes nacionalidades o transacciones internacionales). Cuando se publica contenido en Web, es difícil determinar cuál es la legislación nacional que se estaría violando, de existir alguna. Todo el contenido de Internet puede ser visto desde cualquier parte del mundo. Dentro de este contexto, prácticamente todas las actividades en Internet tienen un aspecto internacional que podría involucrar múltiples jurisdicciones o provocar el llamado efecto indirecto.

Los dos casos más ilustrativos y frecuentemente citados que ejemplifican el problema de la jurisdicción son el Caso CompuServe de Alemania en 1996 y el Caso Yahoo! de Francia en 2001.

En el Caso de CompuServe, un tribunal alemán solicitó a CompuServe prohibir el acceso a materiales pornográficos. Con el fin de cumplir la ley alemana, CompuServe tuvo que remover materiales de su servidor web central localizado en los Estados Unidos. Como resultado, desactivó el acceso incluso para ciudadanos que residían en otros países (p. ej. los Estados Unidos) en los cuales el acceso a materiales pornográficos no está prohibido por ley. CompuServe tuvo que apegarse a la legislación más restrictiva en este campo. Este caso desencadenó el temor de que la totalidad de Internet tuviera que ajustarse a la legislación más restrictiva (el principio del mínimo común denominador).

Algunos casos recientes, incluyendo el Caso Yahoo! interpuesto en los tribunales franceses, reiteran la alta relevancia del problema de las múltiples jurisdicciones. El Caso Yahoo! fue provocado por el incumplimiento de la legislación francesa sobre distribución de materiales de contenido nazista. Estas leyes le prohibieron a cualquier persona en Francia tener acceso a un sitio Web de Yahoo! que contenga objetos de interés nazista, a pesar de que el sitio era hospedado en los Estados Unidos, donde la exhibición de estos materiales era, y aún es, legal.

El enfoque del derecho real discute que ninguna nueva lección puede ser aprendida en casos como el de CompuServe, ya que muchos ejemplos del efecto indirecto se presentan en el mundo externo a Internet. Un ejemplo bien conocido es el establecimiento de condiciones estrictas por parte de la Comisión de la Unión Europea para la fusión Boeing-McDonnell Douglas ya aprobada por los Estados Unidos. A pesar de que ninguna de las compañías contaba con instalaciones de fabricación en Europa, aún así

tuvieron que respetar la legislación sobre competencia de la Unión Europea para poder vender sus aviones en ese territorio.

Aunque el razonamiento del derecho "real" es en principio sólido, aún así presenta serias imperfecciones en el sentido práctico, las cuales limitan la aplicabilidad a Internet de la legislación existente. El principal problema es la simple magnitud de los casos potencialmente relacionados con Internet, ya que prácticamente todos los sitios y servicios Web están expuestos a acciones legales potenciales desde cualquier parte en el mundo. Por lo tanto, el aspecto cuantitativo (el número de casos) podría desafiar el principio legal y promover nuevas soluciones.

## SOLUCIONES POTENCIALES

Es posible encontrar soluciones potenciales para el problema de la jurisdicción múltiple con relación a Internet en:

- la modernización del derecho internacional privado;
- la armonización de leyes nacionales, que harían que la cuestión de la jurisdicción fuera menos relevante;
- la utilización del arbitraje;
- la utilización de soluciones técnicas para identificar el origen de los usuarios (principalmente software de localización geográfica).

### La modernización del Derecho Internacional Privado

Dentro de los procedimientos legales tradicionales, los tribunales nacionales deciden si les es posible juzgar un caso en particular y cuáles reglas deben aplicar. Las decisiones que involucran tanto la jurisdicción procesal como sustantiva se basan en el derecho internacional privado ("conflicto de leyes" en los sistemas legales anglosajones). Estas reglas especifican los criterios para establecer la jurisdicción, tales como el vínculo entre el individuo y la jurisdicción nacional (p. ej. nacionalidad, domicilio) o el vínculo entre una transacción particular y la jurisdicción nacional (p. ej. el lugar donde se firmó el contrato, el lugar donde se llevó a cabo el intercambio). Internet hace que la aplicación de estos criterios sea más compleja que en los casos tradicionales, mas no imposible.

El enfoque tradicional se utiliza en raras ocasiones en la resolución de disputas relacionadas con Internet debido a su complejidad, lentitud y alto costo. Además no calza con el modus operandi de Internet, el cual es rápido, simple y pragmático. Los principales mecanismos del derecho interna-

cional privado fueron desarrollados en una época en que la interacción entre países era menos frecuente e intensiva. Proporcionalmente, una menor cantidad de casos involucraban a individuos y entidades de diferentes jurisdicciones. Con el advenimiento de Internet, la interacción entre países se convirtió en algo común. Las comunicaciones, intercambios y disputas entre instituciones e individuos de diferentes países son mucho más frecuentes e intensas que hasta ahora.

Una solución potencial podría ser la modernización del derecho internacional privado con el fin de contar con un proceso rápido y de bajo costo para la asignación de jurisdicciones nacionales en casos relacionados con Internet. Algunas de las mejoras podrían incluir procedimientos simplificados para la identificación de jurisdicciones apropiadas, la opción de llevar a cabo deliberaciones en línea y el establecimiento de acuerdos flexibles de asesoría legal.

A nivel regional, la Unión Europea ha adoptado la Convención de Bruselas, la cual simplifica el proceso de determinación de la jurisdicción y favorece la protección de los clientes en casos de comercio electrónico.

A nivel global, la principal jurisdicción para el desarrollo del derecho internacional privado es la Conferencia de la Haya. Hasta el presente las negociaciones han sido dominadas por los Estados Unidos. En 1992, los Estados Unidos inició negociaciones sobre jurisdicción con el objetivo principal de fortalecer la protección de la propiedad intelectual imponiendo a nivel global las decisiones de los tribunales estadounidenses. Desde 1992, el crecimiento de Internet y el comercio electrónico han modificado el panorama de las negociaciones. Cada vez es más riesgoso para las compañías estadounidenses de Internet operar en un ambiente de múltiples jurisdicciones. Los casos de CompuServe (Alemania) y Yahoo! (Francia) han demostrado cómo el contenido albergado en los Estados Unidos puede desencadenar procesos en los tribunales de otros países.

"Banderas de Conveniencia" en Internet

Otra consecuencia potencial de la falta de armonización sería la migración de "datos" y materiales web a países con menores niveles de control sobre el contenido. Utilizando la analogía del Derecho del Mar, algunos países podrían convertirse en "banderas de conveniencia" o en los centros "off-shore" del mundo de Internet.

Si la propuesta inicial de la Convención de la Haya fuera adoptada, plantearía un considerable desafío al sistema legal de los Estados Unidos. Los tribunales de los Estados Unidos tendrían que hacer cumplir las decisiones de los tribunales extranjeros, lo que involucraría el contenido de los sitios web albergados en su país, lo que a su vez desafiaría la libertad de

expresión consagrada en la Primera Enmienda de la Constitución. La consecuencia involuntaria de la iniciativa fue un cambio en la posición estadounidense, reduciendo sus ambiciones de reformar el sistema de derecho internacional privado. La falta de progreso en la modernización del derecho internacional privado a nivel global podría fortalecer otras opciones para la resolución de conflictos.

### La Armonización de las Legislaciones Nacionales

La armonización de las legislaciones nacionales debería producir como resultado el establecimiento de un conjunto de normas equivalentes a nivel global. Al contar con normas idénticas, la cuestión de la jurisdicción se vuelve menos relevante. La armonización puede ser lograda en áreas donde ya existe un alto nivel de consenso global, por ejemplo en lo relacionado con pornografía infantil, piratería, esclavitud, terrorismo y cibercrimen. Las perspectivas también convergen en otros temas como el correo electrónico indeseado y la seguridad en Internet. Sin embargo, en algunos campos, incluyendo las políticas de contenido, es poco probable que se alcance un consenso global sobre normas básicas.

Otra opción para resolver el problema de la jurisdicción es el arbitraje, el cual se discute a continuación.

## ARBITRAJE

El arbitraje es un mecanismo alterno para la resolución de disputas que puede ser utilizado en lugar de los usualmente lentos y complejos procesos judiciales. En los arbitrajes, las decisiones las toman uno o más individuos independientes elegidos por los disputantes. El arbitraje internacional en el sector comercial cuenta ya con una larga tradición. Es común que los contratos privados establezcan un mecanismo de arbitraje por medio del cual las partes acuerdan resolver cualquier disputa por medio de arbitraje. Existe una gran variedad de contratos de arbitraje que especifican aspectos como el lugar del arbitraje, los procedimientos y la escogencia de la legislación.

Una de las principales ventajas del arbitraje sobre los tribunales tradicionales es que elimina el problema de tener que elegir la jurisdicción procesal y sustantiva ya que ambas son elegidas de antemano por los disputantes.

Los arbitrajes en línea se utilizan no solo para resolver problemas en Internet, sino también disputas comerciales regulares. El arbitraje en línea es conducido enteramente por Internet, incluyendo la presentación de evidencia y las resoluciones.

El arbitraje ofrece ventajas particulares cuando se trata de una de las más difíciles tareas en un proceso judicial, es decir, la ejecución de las decisiones (sentencias). La ejecución de las sentencias de arbitraje se encuentra regulada por la Convención de Nueva York sobre el Reconocimiento y Ejecución de las Sentencias Arbitrales Extranjeras, firmada por la mayoría de los países. Según esta convención, los tribunales nacionales están obligados a ejecutar las sentencias arbitrales. Es más simple ejecutar las sentencias arbitrales que los fallos de los tribunales extranjeros.

El arbitraje ha sido utilizado ampliamente para superar la brecha producida por la incapacidad del derecho internacional privado actual de resolver los casos de Internet. Un ejemplo particular del uso de arbitraje en casos de Internet es la Política Uniforme de Resolución de Disputas de Nombres de Dominio (UDRP por sus siglas en inglés). La UDRP fue desarrollada por la Organización Mundial de la Propiedad Intelectual (OMPI) e implementada por ICANN como el procedimiento clave para la resolución de disputas. La UDRP se establece de antemano como el mecanismo de resolución de disputas en todos los contratos que involucren el registro de gTLDs (.com, .edu, .org, .net). Su característica singular es que las sentencias arbitrales se aplican directamente a cambios en el Sistema de Nombres de Dominio sin recurrir a la ejecución por medio de tribunales nacionales.

En general, el arbitraje ofrece un método rápido, simple y económico para la resolución de disputas. Sin embargo, el uso del arbitraje como mecanismo principal de resolución de disputas en Internet presenta algunas limitaciones importantes.

*Primero,* debido a que el arbitraje se establece usualmente por acuerdo previo, no cubre una amplia gama de aspectos en lo cuales no es posible obtener consenso previo (difamación, diferentes tipos de responsabilidades, cibercrimen).

*Segundo,* muchos ven la práctica actual de adjuntar una cláusula de arbitraje a los contratos regulares como una desventaja para la parte más débil en la contratación (usualmente el usuario de Internet o el cliente del comercio electrónico).

*Tercero,* a algunas personas les preocupa que el arbitraje extienda globalmente el derecho basado en precedentes y que gradualmente suprima otros sistemas legales nacionales. En el caso del derecho mercantil esto podría resultar más aceptable, debido al alto nivel de unificación actual entre las normas sustantivas. Sin embargo, sería una propuesta mucho más delicada cuando se trate de aspectos de contenido y socioculturales, en los cuales un sistema legal refleja contenido cultura específico.

*Cuarto,* la jurisprudencia relacionada con Internet existente actualmente indica que los arbitrajes, como los que se basan en UDRP, han sido más receptivos a los intereses del sector comercial que a los de los individuos. A continuación presentamos un ejemplo que trata dos casos similares. Primero, un tribunal ordinario de Francia resolvió en contra de la compañía francesa "Danone" y a favor del empleado descontento que registró el dominio "jeboycottedanone.com" (Yo boicoteo a Danone). Sin embargo, en un segundo caso, el arbitraje de la OMPI (basado en UDRP) aceptó la solicitud de remover el sitio web "vivendiuniversalsucks.com" (Vivendi Universal apesta). En ambos casos, nombres de dominio fueron utilizados como medios de protesta o criticismo. Un tribunal ordinario de Francia aceptó este tipo de protesta, mientras que el arbitraje de la OMPI no.

## DERECHOS DE PROPIEDAD INTELECTUAL

El conocimiento y las ideas son los recursos clave de la economía global. Su protección, por medio de los Derechos de Propiedad Intelectual, se está convirtiendo en uno de los asuntos más importantes relacionados con Internet, el cual además presenta consecuencias legales y políticas considerables. Las cuestiones sobre derechos de propiedad intelectual reflejan varios aspectos de la Gobernanza de Internet. Debido a que el conocimiento y las ideas son parte importante de la herencia cultural y de la interacción social, estos conservan un valor especial para muchas sociedades. Los derechos de propiedad intelectual también se encuentran en el corazón del debate sobre desarrollo. Los derechos de propiedad intelectual relacionados con Internet incluyen marcas registradas, derechos de autor y patentes.


## MARCAS REGISTRADAS

La relevancia de las marcas registradas en Internet se relaciona con el registro de nombres de dominio. Durante la fase inicial del desarrollo de Internet, el registro de los nombres de dominio siguió el principio de "prioridad según el orden de llegada". Esto condujo a la ciberokupación, es decir la práctica de registrar nombres de empresas comerciales para luego venderlos a un precio más alto. Con la creciente importancia de Internet, esta práctica se convirtió en un serio problema, debido a que las empresas estaban expuestas a una falsa representación en Internet. Los recursos legales por medio de los tribunales regulares no resultaban muy prácticos ya que los plazos para resolver eran sumamente prolongados.

Esta situación obligó al sector comercial a colocar la cuestión de la protección de las marcas registradas en el centro de la reforma de Gobernanza de Internet, lo que condujo al establecimiento de ICANN en 1998. En el Libro Blanco de ICANN, el gobierno de los Estados Unidos solicitó que ICANN desarrollara e implementara un mecanismo para la protección de marcas registradas en el campo de los nombres de dominio. Poco tiempo después de su constitución, ICANN introdujo la Política Uniforme de Resolución de Disputas de Nombres de Dominio (UDRP por sus siglas en inglés) desarrollada por la OMPI.

El uso de la UDRP como mecanismo de resolución de disputas se convirtió en una condición obligatoria en todos los contratos de registro para dominios en el nivel superior, como los .com, .org, y .net. Los poseedores de marcas registradas alentaron la extensión de la UDRP a los dominios de país.

Las marcas registradas también son abordadas en este folleto:


- Sistema de Nombres de Dominio (DNS) en la página 41;
- Política Uniforme de Resolución de Disputas de Nombres de Dominio (UDRP) en la página 79.

## DERECHOS DE AUTOR

El concepto tradicional de derechos de autor o copyright ha sido desafiado de múltiples formas por los desarrollos en Internet. Desde simples funciones como "cortar y pegar" textos contenidos en sitios web hasta actividades mucho más complejas como la distribución de archivos de música y vídeo por medio de la red. Los materiales pueden ser copiados y distribuidos a nivel mundial utilizando Internet sin que esto represente costos significativos.

Estos desarrollos ponen en peligro el delicado balance entre los intereses de los autores de materiales protegidos y los intereses públicos de aumentar la creatividad, el conocimiento público y el bienestar general. Evitar la copia ilimitada de materiales y a la vez, resguardar el acceso a los mismos por medio de Internet es una de las interrogantes que debe tratar la Gobernanza de Internet. Hasta el momento, los poseedores de derechos de autor, representados por las principales compañías discográficas y de multimedios, han sido más proactivos en la protección de sus intereses. El interés público ha sido percibido vagamente y no ha sido suficientemente protegido.

> Los derechos de Copyright solamente protegen la expresión de una idea tal y como se materializa en diversas formas, como un libro, un disco compacto un archivo de computadora, etc. La idea como tal no se encuentra protegida por los derechos de autor.

Uno de los desarrollos decisivos en el campo del copyright y que ha disparado una activa respuesta por parte de los poseedores de los derechos de autor, ha sido el intercambio de música utilizando redes entre pares. Se estima que Napster, el primer ejemplo, produjo pérdidas de US$ 4,300 millones para la industria de la grabación musical. La reacción de la industria de la música sacó a la luz los muchos riesgos, analogías erróneas e insuficiencias del sistema legal actual. Además ilustra la situación actual de la protección de derechos de autor en Internet y la cantidad de asuntos pendientes de resolución.

## LA SITUACIÓN ACTUAL

### Protección más Estricta del Copyright a Nivel Nacional e Internacional

Las industrias de la música y el entretenimiento han venido cabildeando intensivamente a nivel nacional e internacional para fortalecer la protección de los derechos de autor. En los Estados Unidos, una protección más estricta de los derechos de autor fue introducida por medio de la Ley de Derechos de Autor del Milenio Digital de los Estados Unidos (DMCA) de 1998. A nivel internacional, la protección de los artefactos digitales fue introducida en el Tratado sobre Derechos de Autor de la OMPI en 1996. Este tratado también establece previsiones para fortalecer el régimen de protección de derechos de autor, tales como previsiones más estrictas para las limitaciones de los derechos exclusivos de autor, la prohibición de burlar las protecciones tecnológicas para los derechos de autor y otras medidas relacionadas.

### El Creciente Número de Casos en los Tribunales

Solamente en 2004 se emitieron aproximadamente 1000 citatorios fundamentados en DMCA contra ISPs, en los cuales se les solicitaba que detuvieran actividades de intercambio de archivos entre sus abonados, y fueron planteadas más de 500 demandas contra individuos.

Un caso particularmente relevante para el futuro de los derechos de autor en Internet es el caso contra Grokster y StreamCast, dos empresas que producen software para el intercambio de archivos entre pares (P2P). De conformidad con las previsiones de la DMCA, la Asociación Discográfica de los Estados Unidos solicitó a estas empresas detener el desarrollo de tecnologías para el intercambio de archivos ya que contribuyen a la violación del copyright. Inicialmente, los tribunales de los Estados Unidos eligieron no achacar a empresas de software como Grokster y StreamCast la responsabilidad por la posible violación de los derechos de autor bajo circunstancias razonables. Sin embargo, en Junio de 2005, la Corte Suprema de los Estados Unidos dictaminó que los desarrolladores de software eran responsables por cualquier posible abuso de su software.

### Software contra la Violación del Copyright

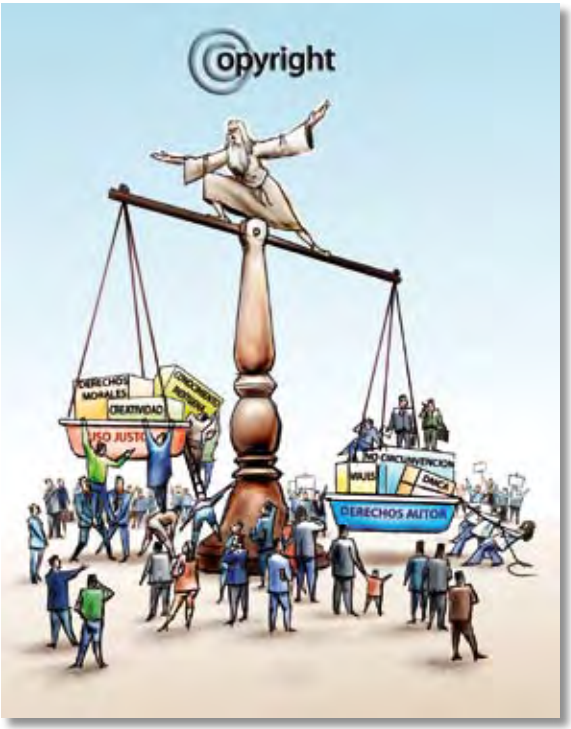
Las herramientas utilizadas por los infractores también pueden ser utilizadas por los protectores. Tradicionalmente las autoridades y em-

presas estatales llevaban a cabo sus responsabilidades por medio de mecanismos legales. Sin embargo, está aumentando el uso de herramientas alternas de software por parte del sector comercial contra los infractores de los derechos de autor.

Un artículo publicado por el diario International Herald Tribune contenía una lista con las siguientes tácticas de software utilizadas por las empresas discográficas y de entretenimiento para proteger su copyright.

- un "Caballo Troyano" que redirige a los usuarios a sitios donde pueden adquirir legítimamente la canción que estaban tratando de descargar;
- software "congelador" que bloquea las computadoras por un periodo de tiempo y despliega advertencias sobre la descarga de música pirateada;
- "El Silencio", método por medio del cual se escanea los discos duros y se intenta eliminar los archivos pirateados encontrados;
- "La interdicción", en la cual se impide el acceso a la red a quienes traten de descargar música pirateada.

El Profesor Lawrence Lessig, de la Escuela de Derecho de Stanford, advierte que estas medidas podrían ser ilegales. Indica que las medidas indicadas anteriormente no se incluyen entre las aprobadas para tratar el problema de la violación del copyright. ¿Estarán las empresas que utilizan estas medidas de autoprotección violando la ley?



### Tecnologías para la Gestión de los Derechos Digitales

Dentro de un enfoque más estructural y de más largo plazo, el sector comercial introdujo varias tecnologías para manejar el acceso a materiales protegidos con derechos de autor. Microsoft introdujo el software Digital Rights Management para manejar la descarga de archivos de sonido, películas y otros materiales con copyright. Sistemas similares fueron desarrollados por Xerox (ContentGuard) Philips y Sony (InterTrust).

El uso de herramientas tecnológicas para la protección del copyright recibe apoyo tanto a nivel internacional (Tratado de la OMPI sobre Derechos de Autor) como en la Ley DMCA. Lo que es más, la Ley DMCA convirtió en crimen las actividades dirigidas a burlar la protección tecnológica de los materiales con derechos de autor.

## LOS ASUNTOS

### ¿Enmendar los Mecanismos de Copyright o Desarrollar unos Nuevos?

¿De qué manera deben ser ajustados los mecanismos de copyright para reflejar los profundos cambios introducidos por las tecnologías de infocomunicaciones y los desarrollos en Internet? Una respuesta sugerida por el gobierno de los Estados Unidos en el Libro Blanco sobre Propiedad Intelectual y la Infraestructura Nacional de Información es que solamente se requieren cambios menores, principalmente por medio de la "desmaterialización" de los conceptos de copyright de "fijación", "distribución", "transmisión" y "publicación". Este enfoque fue adoptado por los principales tratados internacionales sobre derechos de autor, incluyendo ADPIC y las Convenciones sobre Derechos de Autor de OMPI.

Sin embargo, una perspectiva opuesta discute que los cambios en el sistema legal deben ser profundos, ya que copyright en la era digital ya no se refiere únicamente al "derecho de evitar la reproducción" sino también al derecho de "evitar el acceso". En última instancia, tomando en cuenta las crecientes posibilidades técnicas para restringir el acceso a los materiales digitales, uno podría preguntarse si la protección del copyright es realmente necesaria. Queda por ver de qué manera se protegerá el interés público, la segunda parte dentro de la ecuación del copyright.

### Protección del Interés Público – el "Uso Justo" de los Materiales con Copyright

El derecho de reproducción o Copyright fue inicialmente diseñado para motivar la creatividad y la invención. Por este motivo combina dos elementos: la protección de los derechos de los autores y la protección del interés público. El principal desafío fue estipular la manera en que el público podría tener acceso a materiales sujetos a copyright con el fin de aumentar la creatividad, el conocimiento y el bienestar global. Operativamente hablando, el interés público se protege por medio del concepto de "uso justo" de los materiales protegidos. El uso justo usualmente se define como el uso para la investigación académica y otros fines no comerciales.

### Copyright y Desarrollo

Cualquier restricción en el uso justo podría debilitar la posición de los países en desarrollo. Internet ofrece a los investigadores, estudiantes y otras personas en países en desarrollo, una poderosa herramienta para participar en los intercambios académicos y científicos a nivel global. Un régimen de copyright restrictivo podría tener un impacto negativo en el desarrollo de capacidades de los países en desarrollo.

Otro aspecto es la creciente digitalización de los oficios culturales y artísticos en los países desarrollados. Paradójicamente, los países en desarrollo pueden terminar teniendo que pagar por su propia herencia cultural y artística una vez que esta sea digitalizada, reempacada y protegida por empresas extranjeras de entretenimiento y medios.

### OMPI y ADPIC

Existen dos regímenes internacionales para la protección de los derechos de autor. La Organización Mundial de la Propiedad Intelectual (OMPI) maneja el régimen tradicional de protección de derechos de propiedad intelectual basándose en las convenciones de Berna y París. Otro régimen emergente es manejado por la OMC y se basa en el Acuerdo sobre Aspectos de Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC). El cambio en la coordinación internacional de los derechos de propiedad intelectual de la OMPI a la OMC fue realizado para fortalecer la protección de los derechos, especialmente en el campo de la aplicación. Esta fue una de las principales ganancias de los países desarrollados durante la Ronda de Negociaciones de la OMC en Uruguay.

Muchos países en vías de desarrollo están preocupados por este desarrollo. Los estrictos mecanismos de aplicación de la OMC podrían reducir el espacio para las maniobras de los países en desarrollo y la posibilidad de balancear las necesidades de desarrollo con la protección de los derechos internacionales de propiedad intelectual, principalmente basados en los Estados Unidos. Hasta el momento, la OMC y ADPIC se han enfocado principalmente en varias interpretaciones de los derechos de propiedad intelectual de productos farmacéuticos. Es muy probable que las discusiones futuras se extiendan a los derechos de propiedad intelectual e Internet.

#### La Responsabilidad de los ISPs en la Violación del Copyright

Los mecanismos internacionales de coacción en el campo de la propiedad intelectual han sido reforzados al responsabilizar a los ISPs por albergar materiales que violen los derechos de autor si el material no es removido una vez notificada la violación. Esto ha provocado que el régimen de derechos de propiedad intelectual previamente ambiguo sea directamente aplicable en el campo de Internet.


## LAS PATENTES

Tradicionalmente, una patente protege un nuevo proceso o producto de naturaleza principalmente técnica o productiva. Hasta épocas recientes se empezó a otorgar patentes sobre el software. El aumento en los registros de patentes genera un mayor número de procesos judiciales entre empresas de software de los Estados Unidos, los cuales involucran inmensas cantidades de dinero.

Para la Gobernanza de Internet, el principal desarrollo ha sido el otorgamiento flexible de protección a nivel de patente para los procesos de negocios en Internet, como el procedimiento "1-Click" utilizado por Amazon.com. La principal crítica a esta decisión es que Amazon protegió únicamente la idea (el uso de un solo clic), no un proceso de negocios en particular.

El registro exitoso de la patente de "1-Click" desencadenó una ola de registros, incluyendo algunas propuestas ridículas como una patente para

las descargas de Internet. Otro caso controversial es la solicitud de British Telecom de cobrar derechos de licencia por el uso del los enlaces de hipertexto que patentó en la década de 1980. Si British Telecom gana este caso, los usuarios de Internet tendrán que pagar un derecho por cada enlace de hipertexto creado o utilizado. De otra manera, pasará a la historia junto con otros casos como el de quien pretendía patentar la rueda.

Es importante enfatizar que la práctica de otorgar patentes al software y a los procedimientos relacionados con Internet no recibe apoyo en Europa y en la mayoría de los demás países.


## CIBERCRIMEN

La tecnología se desarrolla para ser utilizada, pero a menudo también se utiliza incorrectamente e incluso se abusa de ella. En general, el cibercrimen se refiere al abuso de las tecnologías de información y comunicación. Aunque la parte "crimen" del término ha sido claramente definida (p. ej. robo, pornografía infantil), abundan las opiniones sobre la parte "ciber".

Existe una dicotomía entre el derecho "real" y el "cibernético" en la discusión sobre cibercrimen. El enfoque del derecho real hace hincapié en que el cibercrimen no es más que crimen fuera de línea cometido por medio del uso de computadoras. El crimen es el mismo, solo cambian las herramientas. El enfoque del derecho cibernético enfatiza que los elementos únicos del cibercrimen requieren de un tratamiento especial, sobre todo en lo que se refiere a la coacción y la prevención.

Los encargados de escribir el borrador de la Convención sobre Cibercrimen del Consejo de Europa se acercaron más al enfoque del derecho real, estableciendo que el único aspecto específico del cibercrimen es el uso de tecnologías de infocomunicaciones como medio para cometer un crimen. La convención, que entró en vigencia el 1 de julio de 2004, es el principal instrumento internacional en este campo.

La convención regula el fraude relacionado con las computadoras, la violación del copyright, la pornografía infantil y la seguridad de redes. El

protocolo de la convención recientemente adoptado suma la distribución de contenido racista o xenófobo a los demás crímenes regulados.

La convención establece varios mecanismos procesales para las actividades anticrimen de los estados, como el intercambio de datos relacionados con cibercrimen, incluyendo bitácoras de tráfico en Internet. A los proveedores de servicios de Internet se les asigna responsabilidades especiales en este régimen de cibercrimen, incluyendo la obligación de preservar las bitácoras de Internet de los usuarios y facilitar la intercepción legal para apoyar la recolección de evidencia. Queda por ver si la convención será ratificada por el Congreso de los Estados Unidos, ya que esto constituiría un paso importante para la cobertura global de la convención.

Además del Consejo de Europa, el G-8 adoptó un Plan de Acción que especifica tareas coordinadas para los siguientes crímenes relacionados con Internet: pedofilia y explotación sexual, tráfico de drogas, lavado de dinero, fraude electrónico, así como espionaje industrial y gubernamental.

En 2003, la OECD produjo pautas para ayudar a los gobiernos a combatir el fraude relacionado con Internet. La Unión Europea inició un proceso para adoptar la Decisión Marco sobre Cibercrimen, fortaleciendo así las medidas prácticas y la cooperación en este campo.

## LOS ASUNTOS

### Definición de Cibercrimen

La definición de cibercrimen es uno de los principales temas de impacto legal práctico. Muchas diferencias importantes se presentan en la interpretación del cibercrimen y esto podría tener un impacto directo sobre la efectividad del régimen internacional de cibercrimen.

Por ejemplo, si el enfoque de las definiciones de cibercrimen se centra en el método – como el acceso no autorizado a sistemas seguros de computación – entonces existe el riesgo potencial de confundir el cibercrimen con el "hacktivismo" (desobediencia civil digital).

### Cibercrimen vrs. Derechos Humanos

La Convención sobre Cibercrimen refuerza la discusión sobre el balance entre seguridad y derechos humanos. Han surgido muchas preocupacio-

nes, articuladas principalmente por la sociedad civil, sobre el hecho de que la convención otorga a las autoridades estatales un poder demasiado amplio, incluyendo el derecho de revisar las computadoras de los piratas informáticos o hackers, la vigilancia de las comunicaciones, y otros. Esta amplitud de potestades podría poner en peligro algunos derechos humanos, particularmente la privacidad y la libertad de expresión.

### Recolección y Preservación de Evidencia

Uno de los principales desafíos en la lucha contra el cibercrimen es la recolección de evidencia para los procesos judiciales. La velocidad de las comunicaciones modernas requiere una rápida respuesta de parte de las autoridades. Una posibilidad para preservar la evidencia se encuentra en las bitácoras de red que contienen información sobre quién y cuándo ingresó a recursos particulares de Internet. La Convención sobre Cibercrimen establece algunas previsiones para tratar con este tema.


## FIRMAS DIGITALES

A grandes rasgos podría decirse que las firmas digitales están ligadas a la autenticación de los individuos en Internet lo que a su vez tiene un impacto sobre muchos otros aspectos, incluyendo la jurisdicción, el cibercrimen y el comercio electrónico. El uso de firmas digitales debería contribuir al desarrollo de confianza en Internet.

La autenticación digital en general forma parte del marco del comercio electrónico. Debería facilitar las transacciones de comercio electrónico pactando contratos electrónicos. Por ejemplo ¿es válido o vinculante un acuerdo si ha sido formalizado por e-mail o en un sitio web? En muchos países la legislación requiere que los contratos sean realizados "por escrito" o que estén "firmados". ¿Qué significa esto en términos de Internet?

Al enfrentar estos dilemas y bajo la presión de establecer un ambiente posibilitador para el comercio electrónico, muchos gobiernos empezaron a adoptar legislación sobre firmas digitales. El principal desafío es que los gobiernos no están regulando un problema existente, como el cibercrimen o el copyright, sino creando un nuevo ambiente en el que no tienen experiencia práctica. Esto ha producido una variedad de soluciones y una vaguedad general en las disposiciones sobre firmas digitales. .

Han surgido tres enfoques principales para la regulación de las firmas digitales. El primero es el enfoque "minimalista", el cual especifica que las firmas electrónicas no pueden ser negadas alegando que se encuentran en formato electrónico. Este enfoque especifica un muy amplio uso de las firmas digitales y ha sido adoptado en países de derecho consuetudinario: Estados Unidos, Canadá, Australia y Nueva Zelanda.

El segundo enfoque es el "maximalista", que especifica el marco y los procedimientos para las firmas digitales, incluyendo la criptografía y el uso de identificadores de llave pública. Este enfoque usualmente especifica el establecimiento de autoridades certificadoras dedicadas que puedan legitimar a los usuarios futuros de las firmas digitales. Este enfoque prevalece en la legislación de países europeos como Alemania e Italia.

El tercer enfoque, adoptado por la Directiva sobre Firma Digital de la Comisión Europea combina los dos enfoques anteriormente indicados. Contiene una disposición minimalista para el reconocimiento de las firmas enviadas por un medio electrónico. El enfoque maximalista también es reconocido al establecer que "las firmas electrónicas avanzadas" tendrán un efecto legal más fuerte en el sistema legal (p. ej. es más fácil probar estas firmas en procesos judiciales).

La regulación de la Unión Europea sobre firmas digitales fue una de las respuestas a nivel multilateral. Aunque ha sido adoptada en todos los países miembros de la Unión Europea, aún se conserva una diferencia en el estatus legal de las firmas digitales. Solamente ocho países han implementado los requerimientos establecidos en la directiva para que las firmas digitales sean tratadas de igual manera que las firmas regulares.

A nivel global, en 2001 la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) adoptó la Ley Modelo sobre Firmas Electrónicas. La ley modelo otorga el mismo estatus a las firmas digitales que a las manuales, en el tanto se cumplan algunos requerimientos legales.

La Cámara de Comercio Internacional (CCI) publicó el documento "Uso General en el Comercio Internacional Garantizado Digitalmente" (GUIDEC por sus siglas en inglés), que contiene un estudio sobre las mejores prácticas, regulaciones y temas de certificación.

Directamente relacionadas con las firmas digitales se encuentran las iniciativas de Infraestructura de Llave Pública (PKI por sus siglas en inglés). Dos organizaciones, la UIT y la IETF, se encuentran involucradas en la estandarización de la PKI.

### LOS ASUNTOS

#### Necesidad de Contar con Estándares Detallados para la Implementación

Aunque muchos países desarrollados han adoptado legislación amplia en el área de las firmas digitales, esta a menudo carece de estándares y procedimientos de implementación. Dada la novedad de estos temas, muchos países están esperando ver en qué sentido se desarrollan los estándares concretos. Las iniciativas de estandarización se presentan a varios niveles e incluyen organizaciones internacionales (la UIT) así como asociaciones profesionales (IETF).

#### Riesgo de Incompatibilidad

La variedad de enfoques y estándares en el campo de las firmas digitales podría conducir hacia la incompatibilidad entre diferentes sistemas nacionales. Las soluciones poco sistemáticas podrían restringir el desarrollo del comercio electrónico a nivel global. La armonización necesaria debe provenir de las organizaciones regionales y globales.

## LEGISLACIÓN LABORAL

Frecuentemente se dice que Internet está cambiando "la manera en que trabajamos". Aunque este fenómeno requiere una mayor elaboración, los siguientes aspectos son de relevancia directa para la Gobernanza de Internet:

- Internet introdujo una gran cantidad de trabajadores temporales y de corto plazo. El término "permatemp" fue acuñado por los empl-

eados que se mantienen durante largos periodos con contratos de corto plazo revisados periódicamente. Esto introduce un menor nivel de protección social para la fuerza laboral.

- El teletrabajo se está volviendo cada vez más relevante gracias al continuo desarrollo de las telecomunicaciones, específicamente con el acceso de banda ancha a Internet.
- La subcontratación extranjera en el sector de servicios de infocomunicaciones, como los centros de llamadas y las unidades de procesamiento de datos, se encuentra en aumento. Una cantidad considerable de estas actividades ya han sido transferidas a países de bajo costo, principalmente en Asia y América Latina.


Las infocomunicaciones han desdibujado la rutina tradicional de trabajo, tiempo libre y sueño (8+8+8 horas). Cada vez resulta más difícil distinguir dónde empieza y dónde termina el trabajo. Estos cambios en los patrones de trabajo pueden requerir una nueva legislación laboral que trate temas como las horas de trabajo, la protección de los intereses laborales y la remuneración.

En el campo del derecho laboral, un tema importante es la cuestión de la privacidad en el lugar de trabajo. ¿Puede un empleador monitorear el uso de Internet por parte de sus empleados (como el contenido de los mensajes de correo electrónico o el acceso a sitios web)? La jurisprudencia en este campo se está desarrollando gradualmente con una variedad de soluciones de donde escoger.

En Francia, Portugal, y Gran Bretaña, las pautas legales y algunos casos específicos han tendido a restringir la vigilancia sobre el correo electrónico de los empleados. El empleador debe ofrecer notificación previa sobre cualquier actividad de monitoreo. En Dinamarca, los tribunales consideraron un caso que involucraba el despido de un empleado por enviar correos electrónicos privados y acceder a salas de charla sobre temas sexuales. La corte dictaminó que el despido no era legítimo ya que al empleado no se le había entregado una política de uso de Internet que prohibiera la utilización no oficial de este recurso. Otro motivo argumentado por el tribunal Danés fue el hecho de que el uso de Internet por parte del empleado no afectaba su desempeño laboral.

El derecho laboral ha sido tradicionalmente un tema nacional. Sin embargo, la globalización en general e Internet en particular han producido la internacionalización de los temas laborales. Con el creciente número de individuos trabajando para entidades extranjeras e interactuando con equipos de trabajo de base global, surge la creciente necesidad de contar con mecanismos reguladores internacionales apropiados. Este aspecto fue reconocido en la declaración de la CMSI, la cual en el párrafo 47 pide el respeto de todas las normas internacionales relevantes en el campo del mercado laboral de tecnologías de infocomunicaciones.


## PRIVACIDAD Y PROTECCIÓN DE DATOS

La privacidad y la protección de datos se encuentran íntimamente ligados con los asuntos de Gobernanza de Internet. La protección de datos es un mecanismo legal que garantiza la privacidad.

¿En qué consiste la privacidad? La definición de privacidad depende de las perspectivas individuales. A algunos individuos no les importa revelar algunos datos privados, mientras que otros protegen su privacidad con mayor celo. La privacidad también es determinada por las diferentes culturas nacionales. Aunque este tema de la privacidad es importante en las sociedades occidentales, podría tener menos importancia en otras culturas.

Sin embargo, teniendo estas salvedades en mente, la privacidad debe ser definida antes de poder ser utilizada como concepto legal. Las definiciones varían ampliamente. Una definición tradicional describe la privacidad como "el derecho a que lo dejen a uno en paz". Las definiciones modernas de la privacidad se enfocan en la privacidad de las comunicaciones (comunicaciones libres de vigilancia) y de la información (información individual libre de manipulación por parte de terceros). Tradicionalmente, la privacidad ha estado ligada principalmente a la relación entre ciudadanos (individuos) y el estado. Sin embargo, hoy en día el marco de privacidad ha sido extendido y ahora incluye al sector comercial, tal y como lo refleja la ilustración de la página siguiente.

### Protección de la Privacidad: Individuos y Estados

La información ha sido siempre una mercancía esencial para que las autoridades estatales supervisen su territorio y población. Esto puede deducirse a partir de los registros escritos más antiguos, los cuales en su mayoría tratan con las funciones estatales. Las tecnologías de información han mejorado enormemente la capacidad del estado de recolectar y analizar información. Esto incluye tanto la información administrada por los departamentos gubernamentales (impuestos, seguridad social, salud, propiedad, registros criminales) como la de las empresas autorizadas por los gobiernos a brindar servicios esenciales (electricidad, agua, telecomunicaciones).


Toda esta información es recolectada con la aprobación implícita mas involuntaria de los ciudadanos, ya que no les es posible desafiliarse a estos esquemas, salvo que emigren a otro país, donde encontrarían el mismo problema de todas maneras.

Tecnologías, como los almacenes de datos, son utilizadas para acumular y relacionar datos provenientes de muchos sistemas individuales (por ejemplo el régimen tributario, registros de vivienda o propiedad de vehículos) con el fin de llevar a cabo análisis sofisticados, búsquedas de pa-

trones, inconsistencias, patrones inusuales y otros descubrimientos. Estos podrían tener un impacto dramático en la sociedad, y en la mayoría de los casos, lograr mantenerse dentro de los parámetros de la Declaración Universal de Derechos Humanos.

El terrorismo, el espionaje y otras actividades contra el estado han dado pie a un aumento en la vigilancia de los individuos sospechosos (sean nacionales o no). Los defensores de las libertades civiles advierten sobre la gradual erosión de la privacidad personal ante la introducción de medidas de seguridad nacional más rigurosas.

Hace algunos años, la propuesta de equipar las computadoras personales con un microprocesador que les otorgara una identidad única (el "Clipper"), y que casualmente (o no) también podría ser utilizado como puerta trasera para la vigilancia estatal, provocó un escándalo público. La batalla contra el Clipper la ganaron los libertarios, sin embargo el péndulo se acerca de nuevo al fortalecimiento de la seguridad nacional.

Después del 9/11 la Ley Patriota de los Estados Unidos y algunas leyes comparables de otros países, introdujeron un marco para un control más estricto de las comunicaciones electrónicas, incluyendo una disposición para la Intercepción Legítima. El concepto de Intercepción Legítima como apoyo a la recolección de evidencia también fue incluido en la Convención sobre Cibercrimen del Consejo de Europa de 2001 (Artículos 20 y 21).

Herramientas de vigilancia más poderosas surgirán al ir evolucionando la tecnología, lo que podría fortalecer aún más el rol estatal reduciendo a su vez la privacidad individual.

### Protección de la Privacidad: Individuos y Empresas

En este triángulo de la privacidad, la segunda relación que se encuentra en pleno crecimiento es la de los individuos y el sector comercial. En una economía de información, los datos de los clientes, incluyendo sus preferencias y perfiles de compras, se convierten en una importante mercancía para el mercado. La venta de los datos de los clientes es un negocio muy lucrativo en Internet.

Existe un tipo diferente de "vigilancia" entre los individuos y las empresas, particularmente en el caso del comercio electrónico.

En este caso, millones de individuos revelan voluntariamente cantidades considerables de información personal a empresas y organizaciones: nú-

meros de tarjetas de crédito, direcciones detalladas y otros datos que, de ser utilizados inadecuadamente podrían ocasionar serias consecuencias como fraude o suplantación.

El éxito y la sostenibilidad del comercio electrónico, tanto entre empresas y clientes como entre las mismas empresas, depende del desarrollo de una gran confianza en las políticas de privacidad de las empresas y en las medidas de seguridad establecidas por estas para proteger la información confidencial de sus clientes contra el robo y el abuso.

Las organizaciones comerciales también explotan las tecnologías de almacenes de datos para desarrollar apreciaciones sobre los hábitos y preferencias de sus clientes. Los supermercados utilizan los esquemas de las tarjetas de cliente frecuente para dar seguimiento a los hábitos de compra de sus clientes, determinar qué día de la semana o a qué hora del día prefieren comprar, cuánto gastan o cuáles productos compran (ya que el almacén de datos también se encuentra conectado al equipo de punto de venta).

Los resultados de estos análisis se utilizan más adelante para enfocar iniciativas de mercadeo personalizadas para los hogares individuales.Si no existe una legislación para la protección de los datos, la información de los individuos recolectada por las empresas podría ser vendida y utilizada en otros contextos.

#### Protección de la Privacidad: Estado y Empresas

Este tercer lado del triángulo es el que recibe la menor cantidad de publicidad y sin embargo podría ser el más relevante. Ambas partes, el estado y las empresas, recolectan cantidades considerables de datos sobre los individuos. Ha sido reportado que algunos de estos datos fueron intercambiados dentro del contexto de actividades antiterroristas. Sin embargo, en algunos casos, como el de la Directiva Europea para la Protección de Datos, el estado supervisa y protege los datos de los individuos que se encuentran en manos de las empresas comerciales.

#### Protección de la Privacidad: Entre Individuos

El último aspecto de la protección de la privacidad que no aparece dentro del esquema del triángulo, es el riesgo potencial de violación de la privacidad de los individuos por parte de otros individuos. Hoy en día, la tecnología ha conferido a los individuos herramientas poderosas de vigilancia. Incluso un simple teléfono móvil con cámara puede convertirse en una he-

rramienta de vigilancia. Hoy en día es posible adquirir cámaras miniatura y micrófonos muy sofisticados a precios asequibles. La tecnología ha "democratizado la vigilancia", al decir de la revista The Economist. Muchas instancias de invasión de privacidad han sido documentadas, desde el simple voyeurismo hasta el uso más sofisticado de cámaras para grabar números de tarjetas en los bancos y llevar a cabo espionaje electrónico.

El problema principal es que la mayor parte de la legislación se enfoca en los riesgos para la privacidad que plantea el estado. Al enfrentarse con la nueva realidad, algunos gobiernos han dado pasos iniciales. El Congreso de los Estados Unidos adoptó la "Ley de Prevención del Voyeurismo por Vídeo" que prohíbe tomar fotografías de personas desnudas sin su previa aprobación. Leyes similares de privacidad para impedir la vigilancia individual también fueron adoptadas en Alemania y unos cuantos países.

### La Regulación Internacional de la Privacidad y la Protección de Datos

El principal documento internacional sobre privacidad y protección de datos contiene las "Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales" de la OCDE y fue publicado en 1980. Estas directrices y el trabajo subsiguiente de OCDE han inspirado muchas regulaciones internacionales y regionales en este campo. Los principios propuestos en las directrices de la OCDE han sido ampliamente aceptados. Las principales diferencias descansan en la forma en que los principios son implementados.

Un enfoque utilizado en los Estados Unidos se basa en la autorregulación y en este las políticas de privacidad son establecidas por las empresas comerciales. Las políticas de privacidad quedan a discreción de las empresas y de los mismos individuos. La principal crítica a este enfoque es que los individuos se encuentran en una posición comparativamente más débil.

El segundo enfoque, promovido por la Unión Europea, indica que la protección de la privacidad debe ser garantizada por las autoridades públicas. Este enfoque sobre la privacidad, promovido en 1995 por la Directiva Europea de Protección de Datos (95/46/EC), cubre la protección de los individuos en lo relacionado al procesamiento de datos personales y el libre movimiento de los mismos. Además de la Directiva Europea, la cual es el principal mecanismo, el enfoque europeo hacia la privacidad y la

protección de los datos se encuentra constituido por otros instrumentos regionales, como la Convención del Consejo de Europa para la Protección de los Individuos en lo relacionado al Procesamiento Automático de Datos Personales (1981).

Estos dos enfoques sobre la protección de la privacidad – el de los Estados Unidos y el de la Unión Europea – han entrado en conflicto. El principal problema surge del uso de los datos personales por parte de las empresas comerciales. ¿Cómo puede la Unión Europea imponer sus regulaciones sobre, por ejemplo, una empresa de software basada en los Estados Unidos? ¿Cómo puede la Unión Europea garantizar que los datos de sus ciudadanos estén protegidos de conformidad con las reglas especificadas en su Directiva de Protección de Datos? ¿Según cuáles normas (de la Unión Europea o de los Estados Unidos) se manejan los datos transferidos a través de la red de una empresa desde la Unión Europea a los Estados Unidos? La Unión Europea amenaza con bloquear la transferencia de datos hacia cualquier país que no garantice el mismo nivel de protección a la privacidad que ofrece su directiva. Esta solicitud inevitablemente produjo un choque con el enfoque de autorregulación en la protección de la privacidad propuesto por los Estados Unidos.

Esta arraigada diferencia dificultó aún más el establecimiento de cualquier acuerdo. Por otra parte, no hubiera sido posible ajustar la legislación de los Estados Unidos a la Directiva de la Unión Europea ya que hubiera requerido la modificación de algunos principios importantes del sistema legal estadounidense. El gran adelanto en el impasse se presentó cuando el embajador estadounidense Aaron sugirió una fórmula de "Puerto Seguro". Esto reencuadra todo el asunto y ofrece una salida al punto muerto en que se encontraban las negociaciones.

Se obtuvo una solución en la cual las regulaciones de la Unión Europea pueden ser aplicadas a empresas estadounidenses dentro de un "Puerto Seguro" legal. Las empresas estadounidenses que manejan datos de ciudadanos de la Unión Europea pueden voluntariamente respetar los requerimientos de protección de la privacidad de la Unión Europea. Una vez que los han aceptado, las empresas deben respetar los mecanismos formales de aplicación acordados entre la Unión Europea y los Estados Unidos.

Las perspectivas conflictivas en cuanto a la protección de la privacidad electrónica entre la Unión Europea y los Estados Unidos confir-

man que la creciente interdependencia provocada por el comercio electrónico puede desafiar algunos principios básicos afianzados en sus respectivas historias sociales y culturales. La globalización provocará que este asunto reaparezca al integrar la participación de otras sociedades. El "Acuerdo de Puerto Seguro" debe verse como un valioso precedente y como una herramienta útil en la formulación de acuerdos similares entre la Unión Europea y otros países, incluyendo Canadá y Australia.

SECTION 4

# La Canasta Económica

## LA CANASTA ECONÓMICA

La importancia del aspecto económico de la Gobernanza de Internet se ilustra con el título del documento que inició la reforma de la Gobernanza de Internet y provocó el establecimiento de ICANN: "Marco para el Comercio Electrónico Global" (1997). El Marco establece que el "sector privado debería liderar" el proceso de Gobernanza de Internet y que la función principal de esta gobernanza sería "aplicar un ambiente legal predecible, minimalista, consistente y simple para el comercio electrónico". Estos principios son el cimiento del régimen de Internet basado en ICANN.

Diversos mecanismos políticos y reguladores de alta importancia para el comercio electrónico se clasifican en otras canastas.

### LA CANASTA DE INFRAESTRUCTURA Y ESTANDARIZACIÓN:

- La introducción del acceso de banda ancha y la calidad de servicio constituyen una condición previa para acelerar el crecimiento del comercio electrónico en el campo de los multimedios (p. ej. en la distribución de películas y canciones).
- La seguridad en Internet debería aumentar la confiabilidad y robustez del ambiente de comercio electrónico. También debería contribuir a desarrollar la confianza de los consumidores en el comercio electrónico.
- La codificación resulta crucial para la protección de las comunicaciones, especialmente en transacciones financieras.

.

### LA CANASTA LEGAL

- La jurisdicción es importante para la confiabilidad legal del comercio electrónico, en particular en lo relacionado con la protección del consumidor. La importancia de los derechos de propiedad intelectual para el comercio electrónico tiene que ver con el aumento en el volumen de las transacciones de productos intangibles.
- La firma digital facilita las transacciones en línea y resuelve el problema de la autenticación.
- Con una mayor cantidad de información individual recolectada por medio del comercio electrónico, la protección de los datos ofrece resguardo esencial a la privacidad de los individuos.


## COMERCIO ELECTRÓNICO

La selección de una definición para el comercio electrónico tiene muchas implicaciones prácticas y legales. Reglas específicas serán aplicadas dependiendo de si una transacción en particular es clasificada como comercio electrónico o no, como por ejemplo la regulación fiscal y aduanal.

Para el gobierno de los Estados Unidos, el elemento clave que distingue el comercio tradicional del comercio electrónico es "el compromiso en línea de vender bienes o servicios". Esto significa que cualquier negocio comercial pactado en línea debería ser considerado como una transacción de comercio electrónico, incluso si la realización del negocio involucra el envío físico. Por ejemplo, comprar un libro por medio de Amazon.com se considera una transacción de comercio electrónico aunque el libro sea usualmente entregado por correo tradicional. La OMC ofrece una definición más precisa de comercio electrónico: "la producción, distribución, mercadeo, venta o entrega de bienes y servicios por medios electrónicos".

**El comercio electrónico se presenta de muchas formas:**

- negocio a consumidor (B2C) – el tipo más común de comercio electrónico (p. ej. Amazon.com);
- negocio a negocio (B2B) – el más intensivo económicamente. En 2001, el volumen de transacciones B2B en los Estados Unidos alcanzó un total de US$ 995,000 millones, que representaba el 93.3% de todas las transacciones de comercio electrónico;
- negocio a gobierno (B2G) – de gran importancia en el área de políticas de proveeduría;
- consumidor a consumidor (C2C) – por ejemplo, las subastas de e-Bay.

Muchos países han venido desarrollando un ambiente regulador para el comercio electrónico. Leyes han sido adoptadas en los campos de firmas digitales, resolución de disputas, cibercrimen, protección del consumidor y cargas fiscales. A nivel internacional, un mayor número de iniciativas y regímenes se relacionan con el comercio electrónico.

## LA OMC Y EL COMERCIO ELECTRÓNICO

El jugador clave en la emisión de políticas para el comercio global de hoy, la Organización Mundial del Comercio (OMC), regula muchos de los aspectos relevantes del comercio electrónico, incluyendo la liberalización de las telecomunicaciones, los derechos de propiedad intelectual y algunos aspectos de los desarrollos de tecnologías de infocomunicaciones. La OMC trata el comercio electrónico directamente por medio de las siguientes iniciativas:

- Una moratoria temporal sobre los derechos de aduana en las transacciones electrónicas introducida en 1998. Ha permitido que todas las transacciones electrónicas a nivel global permanezcan libres del pago de derechos de aduana.
- El establecimiento del Programa de Trabajo de la OMC sobre Comercio Electrónico, que promueve las discusiones sobre comercio electrónico.

Aunque el comercio electrónico se ha mantenido en un segundo plano en las negociaciones diplomáticas de la OMC, han surgido varias iniciativas y una serie de asuntos clave han sido identificados. Dos de esos asuntos se mencionan aquí.

### ¿Deben las transacciones de comercio electrónico ser categorizadas como servicios (regulados por el Acuerdo General sobre el Comercio de Servicios - AGCS) o bienes (regulados por el Acuerdo General sobre Aranceles Aduaneros y Comercio - GATT)?

¿Cambia la categorización de la música de bien a servicio dependiendo de si es entregado en CD (tangible) o por Internet (intangible)? En última instancia, la misma canción podría tener diferentes categorías comerciales (y ser sujeta a diferentes derechos aduaneros e impuestos) dependiendo del medio de entrega. El tema de la categorización tiene implicaciones considerables debido a los diferentes mecanismos reguladores para bienes y servicios.

### ¿Cuál debería ser la relación entre ADPIC y la protección de los derechos de propiedad intelectual en Internet?

Debido a que ADPIC ofrece mecanismos de aplicación mucho más fuertes para los derechos de propiedad intelectual, los países desarrollados han tratado de extender la cobertura de ADPIC al comercio electrónico y a Internet utilizando dos enfoques. Primero, citando el principio de "neutralidad tecnológica" discuten que ADPIC, al igual que

otras normas de la OMC, debe extenderse a cualquier medio de telecomunicaciones, incluyendo Internet. Segundo, algunos países desarrollados solicitaron una mayor integración de los "tratados digitales" de la OMPI al sistema ADPIC. ADPIC ofrece mecanismos de aplicación más enérgicos que las convenciones de la OMPI. Ambos asuntos permanecen pendientes e irán tomando cada vez mayor importancia en las negociaciones futuras de la OMC.

No es muy probable que el comercio electrónico reciba atención prominente en la agenda de la OMC durante la etapa actual de negociaciones comerciales. La falta de acuerdos globales sobre comercio electrónico será parcialmente cubierta por algunas iniciativas específicas (relacionas por ejemplo con los contratos y las firmas) y varios acuerdos regionales, principalmente en la Unión Europea y Asia Pacífico.

## OTRAS INICIATIVAS INTERNACIONALES DE COMERCIO ELECTRÓNICO

Una de las iniciativas internacionales más exitosas y con mayor apoyo en el campo del comercio electrónico es la Ley Modelo de la CNUDMI sobre Comercio Electrónico. La Ley Modelo se enfoca en los mecanismos para la integración del comercio electrónico y el derecho mercantil tradicional (p. ej. el reconocimiento de la validez de los documentos electrónicos). La Ley Modelo ha sido utilizada como base para la regulación del comercio electrónico en muchos países.

Otra iniciativa diseñada para desarrollar el comercio electrónico fue la introducción de ebXML (Lenguaje Extensible de Marcas para negocios electrónicos) por parte del Centro de las Naciones Unidas para la Facilitación del Comercio y los Negocios Electrónicos (UN-CEFAT por sus siglas en inglés). De hecho, ebXML podría convertirse pronto en el principal estándar para el intercambio de documentos de comercio electrónico, remplazando el actual – Intercambio Electrónicos de Datos (EDI por sus siglas en inglés).

Las actividades de OCDE mencionan varios aspectos relacionados con el comercio electrónico, incluyendo la protección de los clientes y las firmas digitales. Por medio de sus recomendaciones y pautas, la OCDE enfatiza la promoción y la investigación del comercio electrónico. Otras organizaciones internacionales, como la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD) y la Fuerza de Tareas para Tecnologías de Infocomunicaciones de las Naciones Unidas también

conducen varias actividades de investigación y desarrollo de capacidades para el comercio electrónico.

En el sector comercial, las organizaciones internacionales más activas son la Cámara de Comercio Internacional, que produce una amplia gama de recomendaciones y análisis en el campo del comercio electrónico, y el Diálogo Global Empresarial, que promueve el comercio electrónico tanto en el contexto internacional como nacional.

### INICIATIVAS REGIONALES

La Unión Europea desarrolló una estrategia de comercio electrónico durante la llamada Cumbre "Punto Com" de líderes de la Unión Europea en Lisboa (Marzo 2000). A pesar de que adoptaba para el comercio electrónico un enfoque privado y centrado en el mercado, la Unión Europea también introdujo unas cuantas medidas correctivas dirigidas a proteger los intereses públicos y sociales (la promoción del acceso universal, una política de competencia que considera el interés público y una restricción en la distribución de contenido nocivo). La Unión Europea adoptó la "Directiva sobre Comercio Electrónico" así como un conjunto de directivas adicionales relacionadas con las firmas digitales, la protección de datos y las transacciones financieras electrónicas.

En la región Asia Pacífico, el punto focal de la cooperación sobre comercio electrónico es APEC (la Cooperación Económica de Asia Pacífico). APEC estableció el Grupo Director de Comercio Electrónico, que trata diferentes asuntos relacionados con el comercio electrónico, incluyendo la protección del consumidor, la protección de datos, el spam y la ciberseguridad. La última y más prominente iniciativa es el Plan de Acción Individual para el Comercio sin Papeles de APEC, la cual procura desarrollar el comercio total de bienes sin papeles en la región para el año 2010.

## PROTECCIÓN DEL CONSUMIDOR

La confianza del consumidor es una de las principales condiciones previas para el éxito del comercio electrónico. El comercio electrónico es aún relativamente nuevo y los consumidores no le tienen tanta confianza como a las compras en el mundo "real". La protección del consumidor

es un método legal importante para el desarrollo de confianza en el comercio electrónico.

La regulación del comercio electrónico debería proteger a los consumidores en varias áreas: el manejo en línea de información sobre tarjetas de pago, publicidad engañosa y el envío de productos defectuosos. Una nueva idiosincrasia del comercio electrónico es la internacionalización de la protección del consumidor, la cual no constituye un aspecto importante en el comercio regular. En el pasado, los consumidores casi nunca requerían protección internacional. Con el comercio electrónico, un mayor número de transacciones se llevan a cabo a través de las fronteras internacionales.

La jurisdicción es un asunto significativo que rodea la protección del consumidor. La jurisdicción involucra dos enfoques principales. El primero favorece al vendedor (principalmente negocios electrónicos) y se enfoca en el país de origen o es prescrito por el vendedor. En este escenario, las empresas de comercio electrónico tienen la ventaja de contar con un ambiente legal predecible y bien conocido. El otro enfoque, que favorece al consumidor, se basa en el país de destino. La principal desventaja para las empresas de comercio electrónico es la posibilidad de tener que exponerse a una amplia variedad de jurisdicciones. Una posible solución para este dilema sería una más intensa armonización de las normas de protección del consumidor, lo que haría que la cuestión de la jurisdicción fuera menos relevante.

Al igual que con otros asuntos de comercio electrónico, la OCDE tomo la delantera adoptando las Pautas para la Protección del Consumidor en el Contexto del Comercio Electrónico (2000) y las Pautas para la Protección de los Consumidores contra las Prácticas Fraudulentas y Engañosas de Origen Transfronterizo (2003). La OCDE estableció los principios fundamentales que han sido adoptados por algunas asociaciones comerciales, incluyendo la Cámara de Comercio Internacional y el Consejo de la Agencia para Mejores Negocios (BBB por sus siglas en inglés).

La Unión Europea ofrece un alto nivel de protección al consumidor en el comercio electrónico. Por ejemplo, el problema de la jurisdicción ha sido resuelto por medio de la Convención de Bruselas, la cual estipula que los consumidores siempre tendrán derecho a recurrir a la protección legal a nivel local.

A nivel global, ningún instrumento legal pertinente ha sido establecido. Uno de los más apropiados, la Convención de las Naciones Unidas sobre

A nivel global, ningún instrumento legal pertinente ha sido establecido. Uno de los más apropiados, la Convención de las Naciones Unidas sobre Contratos de Compraventa Internacional de Mercaderías (1980), no cubre los contratos directos con el consumidor ni la protección del mismo. El desarrollo futuro del comercio electrónico requerirá ya sea la armonización de las leyes nacionales o un nuevo régimen internacional para la protección del cliente en el comercio electrónico.


## CARGAS FISCALES

El dilema que se le plantea a la Gobernanza de Internet sobre si los asuntos cibernéticos deben ser tratados de manera distinta a los reales se refleja claramente en el tema de las cargas fiscales. Desde los primeros días, Estados Unidos ha procurado declarar a Internet como una zona libre de cargas fiscales. En 1998, el Congreso de los Estados Unidos adoptó la Ley para la Libertad Fiscal. La OCDE y la Unión Europea han promovido la perspectiva opuesta, es decir que Internet no debería recibir un tratamiento fiscal especial. Los Principios de Ottawa de la OCDE especifican que no existe ninguna diferencia entre las cargas fiscales tradicionales y las electrónicas que amerite regulaciones especiales. Muchos estados en los Estados Unidos discuten en el mismo sentido y solicitan la imposición de cargas fiscales a las transacciones en Internet.

Otro aspecto de las cargas fiscales que permanece sin resolución entre la Unión Europea y los Estados Unidos es la cuestión del emplazamiento fiscal. Los Principios de Ottawa introdujeron el concepto fiscal de "destino" en lugar de "origen". El gobierno de los Estados Unidos mantiene un fuerte interés en conservar el régimen fiscal en el punto de origen de las transacciones, ya que la mayor parte de las empresas de comercio electrónico se encuentran en ese país. En contraste, el interés de la Unión Europea de contar con un régimen fiscal en el punto de destino se inspira en el hecho de que la Unión Europea tiene más consumidores de comercio electrónico que vendedores.

## ADUANAS

Las aduanas se ven afectadas directamente por el comercio electrónico. El intercambio de mercancías digitales entre fronteras no puede ser controlado de la misma manera en que se controla las mercancías materiales. Es difícil, sino imposible, identificar cuáles paquetes en Internet contienen productos sujetos al pago de derechos de aduana. Esto plantea muchos asuntos relacionados con la aplicabilidad del concepto actual de controles aduaneros y la introducción de algunos procedimientos nuevos.

A nivel normativo, la principal iniciativa es la Moratoria de la OMC sobre los derechos de aduana de las transacciones de comercio electrónico (1998). La última extensión explícita de la moratoria fue realizada en Doha en 2001. Debido al fracaso de las Negociaciones de la OMC en Cancún (2003), el tema no fue oficialmente discutido, lo cual dejó amplio espacio para diferentes interpretaciones sobre si la moratoria global de aduanas se encuentra vigente o no. Desde el punto de vista práctico no hace mayor diferencia, ya que es prácticamente imposible imponer derechos aduaneros sobre bienes y servicios entregados por medio de Internet debido a la dificultad técnica de inspeccionarlos.


## PAGOS ELECTRÓNICOS: BANCA ELECTRÓNICA Y DINERO ELECTRÓNICO

El pago electrónico puede ser definido como la consumación de transacciones financieras dentro de un ambiente en línea utilizando diferentes instrumentos de pago en línea. La existencia de un sistema de pago electrónico es una condición previa para el exitoso desarrollo del comercio electrónico. El campo de los pagos electrónicos requiere establecer una distinción entre banca electrónica y dinero electrónico.

La banca electrónica involucra la utilización de una computadora e Internet para realizar transacciones bancarias convencionales tales como

pago de tarjetas o transferencias de fondos. La novedad esta únicamente en el medio, mientras que el servicio bancario permanece esencialmente sin variaciones. La banca electrónica ofrece ventajas a los clientes y reduce el costo de las transacciones. En términos de gobernanza, no presenta ningún problema específico más allá de los que ya han sido cubiertos, como la protección del consumidor a nivel internacional.

Por otro lado, el dinero electrónico introduce una innovación considerable. La Junta de la Reserva Federal de los Estados Unidos define el dinero electrónico como "dinero que se moviliza electrónicamente". El dinero electrónico se asocia usualmente con las llamadas "tarjetas inteligentes" emitidas por empresas como Mondex, Visa Cash y CyberCash. Todo el dinero electrónico responde a las siguientes características:

- Se almacena electrónicamente, típicamente en una tarjeta con un chip de microprocesador.
- Se transfiere electrónicamente. En la mayoría de los casos, esto ocurre entre consumidores y comerciantes. A veces es posible efectuar transferencias entre individuos.
- Sus transacciones involucran un sistema complejo que incluye al emisor del valor del dinero electrónico, al operador de redes y al compensador de las transacciones de dinero electrónico.

Hasta el momento, el dinero electrónico se encuentra en sus primeras etapas de desarrollo. No ha sido utilizado ampliamente debido a su limitada seguridad y la falta de privacidad. El dinero electrónico podría evolucionar en dos direcciones:

La primera sería un desarrollo evolutivo que incluiría métodos más sofisticados para las transacciones de base electrónica, incluyendo el desarrollo de micropagos eficientes. A la larga, todas esas transacciones estarían ancladas al sistema bancario y monetario existente.

La segunda sería un desarrollo revolucionario que sacaría el dinero electrónico del control de los bancos centrales. El Banco de Pagos Internacionales (BIS por sus siglas en inglés) ya ha identificado la disminución en el control sobre el flujo de capital y la oferta de dinero como riesgos asociados con el dinero electrónico. Conceptualmente, la emisión de dinero electrónico sería análoga a la impresión de dinero sin el control de una institución bancaria central. Un enfoque de este tipo permitiría a las instituciones privadas emitir dinero principalmente para el comercio electrónico. Como dijo un banquero prominente: "los sucesores de Bill Gates llevarán a la quiebra a los sucesores de Alan Greenspan". Un desarrollo

de este tipo tendría implicaciones considerables sobre el futuro del estado y las relaciones internacionales o, como indicó el mismo conferencista, "Las sociedades ya se las han arreglado sin bancos centrales en el pasado. También podrán hacerlo en el futuro". Otras posibilidades para el uso del dinero electrónico son aún especulativas.

**LOS ASUNTOS**

1. El uso continuado de la banca electrónica y el dinero electrónico podría generar cambios en el sistema bancario mundial, brindando a los clientes posibilidades adicionales y a la vez reduciendo los cargos bancarios. Los bancos de ladrillo y cemento enfrentarán serios desafíos debido a que la banca electrónica es más redituable.
2. Los sondeos sobre comercio electrónico listan la falta de métodos de pago (p. ej. tarjetas) como la tercer razón, después de la seguridad y la privacidad, para no utilizar el comercio electrónico. Actualmente, es prácticamente imposible llevar a cabo comercio electrónico sin tarjetas de crédito. Esto constituye un obstáculo importante para los países en desarrollo que no cuentan con un mercado maduro de tarjetas de crédito. Los gobiernos de estos países tendrían que aprobar los cambios legales necesarios para acelerar la introducción de los pagos con tarjetas.
3. Para promover el desarrollo del comercio electrónico, los gobiernos a nivel mundial tendrían que fomentar todo tipo de pago sin efectivo, incluyendo tarjetas de crédito y dinero electrónico. El aceleramiento en la introducción del dinero electrónico requerirá nuevas actividades reguladoras por parte del estado. La Unión Europea adoptó la Directiva sobre Dinero Electrónico en 2000, después de que Hong Kong introdujera la primera legislación integral sobre dinero electrónico. Los gobiernos se muestran reacios a la introducción del dinero electrónico debido a los riesgos potenciales que plantea a la autoridad del banco central. Opiniones como la del economista David Saxton incluyen serias advertencias: "El efectivo digital es una amenaza a todo gobierno en este planeta que desee seguir al mando de su propia moneda". A los gobiernos también les preocupa el uso potencial del dinero electrónico para el lavado de dinero.
4. Algunos analistas creen que la verdadera expansión del comercio electrónico se basa en la introducción de servicios efectivos y confiables para transacciones pequeñas. Por ejemplo, los usuarios de Internet todavía se muestran reacios a utilizar tarjetas de crédito para

pagos pequeños (de unos cuantos Euros/dólares), ya que usualmente se les cobra un monto adicional por acceder a artículos o servicios en Internet. Un esquema de micropagos basado en el dinero electrónico podría se la solución al problema. El Consorcio del World Wide Web (W3C), el principal organismo de estandarización en Internet, está involucrado en la creación de estándares para los sistemas de micropagos.

5. Debido a la naturaleza de Internet, es probable que el dinero electrónico se globalice – mayor razón para tratar este tema a nivel internacional. Un jugador potencial en el campo de la banca electrónica es el Grupo de Banca Electrónica del Comité de Basilea. Este grupo ha empezado a tratar temas clave para la introducción del dinero electrónico, como la autorización, los estándares prudenciales, la transparencia, la privacidad, el lavado de dinero y la supervisión transfronteriza.

6. Diferentes formas electrónicas de pago han sido desarrolladas, principalmente en las economías avanzadas. Los pagos electrónicos requieren un ambiente legal estable, seguro y funcional. Sin embargo, la mayoría de los países en desarrollo todavía cuentan con economías basadas en el efectivo. En los casos en que el uso de tarjetas es permitido, este depende de las firmas. Esta enorme discrepancia también afecta el desarrollo del comercio electrónico y aumenta la brecha digital entre el Norte rico y el Sur pobre. A diferencia de medidas como la compra de equipo, la introducción de pagos electrónicos requiere de muchos acuerdos institucionales y técnicos de introducción gradual. La confianza del usuario es un elemento esencial tanto para el comercio electrónico como para los pagos electrónicos y esta no se desarrolla con rapidez.

7. La más reciente solicitud enviada por el Fiscal General del Estado de Nueva York a PayPal y a Citibank pidiéndoles no ejecutar pagos a casinos en Internet establece un enlace directo entre el pago electrónico y la aplicación de la ley. Lo que las autoridades no pudieron lograr por medio de mecanismos legales, podría ser alcanzado por medio de controles sobre los pagos electrónicos.

SECTION 5

# La Canasta de Desarrollo

## LA CANASTA DE DESARROLLO

La tecnología no es nunca neutra. La historia de la sociedad humana ofrece múltiples ejemplos sobre la manera en que la tecnología otorgó poderes a ciertos individuos, grupos o naciones y excluyó a otros. Internet no presenta diferencia alguna en este sentido. Desde el nivel individual al global se ha presentado un cambio profundo en la distribución de riqueza y poder. El impacto de las TIC en la distribución de poder y desarrollo ha dado lugar a muchas interrogantes:

- ¿De qué manera afectarán los cambios acelerados por las TIC la brecha ya existente entre el Norte y el Sur? ¿Reducirán o ampliarán las TIC la brecha existente?
- ¿Cómo y cuándo podrán las naciones en desarrollo alcanzar los niveles de tecnologías de infocomunicaciones de países industrialmente más desarrollados?

La respuesta a estas y otras preguntas requiere analizar la relevancia del desarrollo dentro del contexto de la Gobernanza de Internet. Casi cualquier asunto relacionado con la Gobernanza de Internet presenta un aspecto de desarrollo. Por ejemplo:

- la existencia de una infraestructura de telecomunicaciones, la primera condición previa necesaria para superar la brecha digital;
- el modelo económico actual para el acceso a Internet, que coloca una carga desproporcionada en los países en desarrollo que deben financiar el acceso a las redes troncales instaladas en países desarrollados;
- el correo electrónico indeseado o spam, con un impacto negativo comparativamente mayor para los países en desarrollo debido a su limitado ancho de banda y la falta de capacidades para enfrentarlo;
- La regulación global de los derechos de propiedad intelectual que afecta directamente el desarrollo, debido a la reducida oportunidad de los países en desarrollo de acceder al conocimiento y a la información en línea.

El aspecto del desarrollo de la Cumbre Mundial de la Sociedad de la Información (CMSI) ha sido reiterado frecuentemente, empezando con la Resolución de la Asamblea General de la ONU sobre la CMSI, la cual recalcó que la CMSI debería estar "promoviendo el desarrollo, en particular en lo relacionado al acceso a la tecnología y su transferencia". La De-

claración de Ginebra y el Plan de Acción de la CMSI señalan el desarrollo como una prioridad y lo relacionan con la Resolución del Milenio y su promoción del "acceso de todos los países a la información, el conocimiento y las tecnologías de comunicación para el desarrollo".

Por medio de su enlace con los Objetivos del Milenio, la CMSI se encuentra fuertemente posicionada en el contexto del desarrollo.

Este capítulo se enfoca exclusivamente en los asuntos principales del desarrollo, como la brecha digital y el acceso universal, temas frecuentemente planteados en el debate sobre el desarrollo. Luego presentará un análisis sobre los principales factores influenciados por Internet y el desarrollo: infraestructura, asistencia económica, cuestiones normativas y aspectos socioculturales.

### ¿De qué manera afectan las TIC el Desarrollo de la Sociedad?

Los principales dilemas relacionados con las TIC y el desarrollo se resumen en un artículo publicado por la revista The Economist ("Falling through the Net?" – ¿Colándose por la Red? – del 21 de setiembre del 2000).

| Las TIC NO facilitan el desarrollo | Las TIC SI facilitan el desarrollo |
|---|---|
| • Los "factores exógenos a la red" ayudan a los primeros en llegar a establecer una posición dominante. Esto favorece a los gigantes estadounidenses y las firmas locales en economías emergentes serían efectivamente excluidas del comercio electrónico.<br>• La transferencia de poder del vendedor al comprador afectará a los países más pobres (Internet inevitablemente da origen al escenario del "proveedor alterno a solo un clic de distancia"). Afectará a los productores de materias primas principalmente en los países en desarrollo.<br>• El creciente interés en los títulos de alta tecnología de las economías ricas reducirá el interés de los inversionistas en los países en desarrollo. | • Las TIC reducen los costos de mano de obra; es más barato invertir en países en desarrollo.<br>• Las TIC se difunden rápidamente entre los países, a diferencia de las tecnologías anteriores. Tecnologías anteriores (ferrocarriles y electricidad) requería décadas para extenderse a los países en desarrollo, pero las TIC están avanzando a brincos y saltos.<br>• La oportunidad de adelantar las viejas tecnologías brincándose las etapas intermedias, como los cables de cobre y los teléfonos analógicos, estimulan el desarrollo.<br>• La propensión de las TIC a reducir el tamaño óptimo de una empresa en la mayoría de las industrias se acerca más a las necesidades de los países en desarrollo. |

## LA BRECHA DIGITAL

La brecha digital puede definirse como un distanciamiento entre quienes tienen acceso y capacidades para utilizar las TIC, por motivos políticos, sociales y económicos, y quienes no. Diferentes perspectivas han sido planteadas sobre el tamaño y relevancia de la brecha digital.

La brecha digital existe en diferentes niveles: dentro de los países y entre países, entre poblaciones rurales y urbanas, entre los jóvenes y los mayores, así como entre los hombres y las mujeres. Las brechas digitales no son fenómenos aislados. Reflejan las amplias desigualdades existentes en educación, atención de la salud, capital, habitación, empleo, agua potable y alimento. Esto fue claramente señalado por la Fuerza de Tareas para la Oportunidad Digital (DOT por sus siglas en inglés) del G-8: "No existe dicotomía entre la brecha digital y las brechas sociales y económicas más generales que deberían ser tratadas por el proceso de desarrollo; la brecha digital debe ser comprendida y tratada dentro del contexto de estas brechas más amplias".

### ¿Está Creciendo La Brecha Digital?

Los desarrollos de las tecnologías de infocomunicaciones dejan atrás al mundo en desarrollo mucho más rápido que los avances en otros campos (p. ej. técnicas agrícolas o médicas) y, como el mundo desarrollado cuenta con las herramientas necesarias para utilizar exitosamente estos avances tecnológicos, la brecha digital parece estar ampliándose rápida y continuamente. Esta es la perspectiva frecuentemente expresada en varios documentos muy respetados, como el Informe sobre Desarrollo Humano del PNUD o el Informe sobre Empleo en el Mundo de la OIT.

Algunas perspectivas opuestas discuten que las estadísticas sobre la brecha digital son a menudo engañosas y que la brecha digital no se está ampliando en lo absoluto. Según esta perspectiva, el enfoque tradicional sobre el número de computadoras, el número de sitios Web en Internet o el ancho de banda disponible debe ser remplazado por un enfoque sobre el impacto general de las TIC sobre las sociedades en los países en desarrollo. Algunos ejemplos citados frecuentemente son los éxitos digitales de la India y China.


## ACCESO UNIVERSAL

Además de la brecha digital, otro concepto mencionado frecuentemente en el debate de desarrollo es el acceso universal, es decir, acceso para todos. Aunque debería ser la piedra angular de cualquier política de desarrollo de tecnologías de infocomunicaciones, todavía existen diferentes percepciones y nociones sobre la naturaleza y el enfoque de este acceso universal. La referencia frecuente que se hace del acceso universal en los preámbulos de las declaraciones y resoluciones internacionales sin contar con el soporte político y financiero necesario lo convierten en un principio vago de poca relevancia práctica. La cuestión del acceso universal a nivel global continua siendo en gran parte un asunto normativo, que en última instancia depende de la disposición de los países desarrollados de invertir en la realización de esta meta.

A diferencia del acceso universal a nivel global, en algunos países el acceso universal es un concepto económico y legal bien desarrollado. Brindar acceso a las telecomunicaciones para todos los ciudadanos ha sido la base de la política de telecomunicaciones de los Estados Unidos. El resultado ha sido un sistema bien desarrollado con diferentes mecanismos normativos y financieros, cuyo propósito es subsidiar los altos costos de acceso de las zonas y regiones remotas. El subsidio es financiado por las regiones con bajos costos de conexión, principalmente las grandes ciudades. La Unión Europea también ha dado una serie de pasos concretos hacia la obtención del acceso universal.

## ESTRATEGIAS PARA SUPERAR LA BRECHA DIGITAL

La teoría del desarrollo centrada en la tecnología, que ha dominado los círculos normativos y académicos durante los últimos 50 años, discute que el desarrollo depende de la disponibilidad de la tecnología. A mayor tecnología, mayor desarrollo. Sin embargo, este enfoque fracasa en muchos países (principalmente países antiguamente socialistas) ya que resulta obvio que el desarrollo de la sociedad es un proceso mucho más complejo. La tecnología es una condición previa necesaria mas no sufi-

ciente para el desarrollo. Otros elementos incluyen un marco regulador, soporte económico, recursos humanos disponibles, y otras condiciones socioculturales. Incluso si todos estos ingredientes están presentes, el desafío clave sigue siendo cómo y cuándo deberían ser utilizados, combinados e interactuados.


### DESARROLLO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DE INTERNET

La posibilidad de establecer la conectividad es una condición previa para llevar a los individuos y a las instituciones a Internet y en última instancia superar la brecha digital. Existen diferentes opciones disponibles para brindar y mejorar la conectividad.

El rápido crecimiento de las comunicaciones inalámbricas ofrece una oportunidad para muchos países en desarrollo. Patrick Gelsinger de Intel ha recomendado a los países en desarrollo "decir no" a las infraestructuras de telecomunicaciones basadas en cobre y en su lugar utilizar infraestructuras inalámbricas para los bucles locales y fibra óptica para las troncales nacionales. Las comunicaciones inalámbricas pueden ser la solución al problema del desarrollo de infraestructuras de comunicaciones terrestres tradicionales (instalar cables a grandes distancias para cruzar de un lado a otro grandes territorios asiáticos y africanos). De esta manera se puede superar el problema de la última milla o del bucle local, uno de los principales obstáculos para un desarrollo más acelerado de Internet. Tradicionalmente, la Unión Internacional de Telecomunicaciones se ha enfocado en el aspecto de infraestructura de la brecha digital.

## APOYO ECONÓMICO

Los países desarrollados reciben soporte económico a través de diferentes canales, incluyendo agencias de desarrollo bilaterales o multilatera-

les como PNUD y el Banco Mundial, así como iniciativas de desarrollo regionales y bancos. Al aumentar la liberalización del mercado de las telecomunicaciones también ha aumentado la tendencia a desarrollar infraestructuras de telecomunicaciones por medio de inversión extranjera directa. Muchos países en desarrollo luchan continuamente para atraer inversión privada.

Actualmente, la mayoría de las empresas de telecomunicaciones occidentales se encuentran en una fase de consolidación debido a que acumularon deudas por sobreinversión durante la década de 1990. Aunque todavía se encuentran renuentes a invertir, muchos esperan que en el mediano plazo empiecen a invertir en países en desarrollo, ya que el mercado en los países desarrollados se encuentra sobresaturado con inmensas capacidades construidas a finales de la década de 1990.

La importancia del aspecto económico fue claramente reconocida durante la fase de Ginebra de la CMSI. Una idea propuesta durante la CMSI fue establecer un Fondo de Solidaridad Digital administrado por la ONU para ayudar a los países con desventajas tecnológicas a desarrollar sus infraestructuras de telecomunicaciones. El fondo dependería de contribuciones voluntarias. Algunos propusieron el establecimiento de un sistema de donaciones, como por ejemplo $1 por compra de computadora personal, equipo de red o paquete de software. Sin embargo, la propuesta de establecer un Fondo de Solidaridad Digital no cosechó el apoyo de los países desarrollados, los cuales favorecen la inversión directa en lugar del establecimiento de un fondo centralizado para el desarrollo. Con el fin de explorar las posibilidades de crear esquemas de financiamiento más flexibles y apropiados, se acordó establecer el Grupo de Trabajo sobre Financiamiento ICT4D el cual se reportará ante la CMSI 2005 en Tunes.

## ASPECTOS SOCIOCULTURALES

El aspecto sociocultural de las brechas digitales abarca una serie de temas, incluyendo el alfabetismo, las destrezas en tecnologías de infocomunicaciones, la capacitación, la educación, y la protección del leguaje.

Para los países en desarrollo, una de las cuestiones principales ha sido la "fuga de cerebros", descrita como el movimiento de mano de obra altamente calificada desde los países en desarrollo hacia los desarrollados. La fuga de cerebros provoca pérdidas en muchos sentidos para los países en desarrollo. La principal pérdida es en mano de obra calificada. Los

países en desarrollo también pierden la inversión de capacitar y educar la fuerza laboral que emigra. Es probable que la fuga de cerebros continúe, dados los diferentes esquemas de empleo/migración introducidos en los Estados Unidos, Alemania y otros países desarrollados para atraer mano de obra calificada principalmente en tecnologías de infocomunicaciones.

Un desarrollo que podría detener o en algunos casos incluso revertir la fuga de cerebros, sería el aumento en la subcontratación de tareas de TIC a los países en desarrollo. Los ejemplos más exitosos han sido los centros de la industria del software desarrollados en India, como por ejemplo el de Bangalore.

A nivel global, las Naciones Unidas inició la Red Digital de la Diáspora para promover el desarrollo en África a través de la movilización de las destrezas y recursos tecnológicos, empresariales y profesionales de las diásporas africanas en el campo de las TIC.

Las iniciativas de UNESCO son particularmente relevantes en el aspecto social de la brecha digital. UNESCO adoptó una convención para la protección de la diversidad cultural e incitó unos cuantos proyectos dirigidos a promover la diversidad lingüística y cultural en Internet.

## POLÍTICAS Y REGULACIONES PARA INTERNET

El desarrollo de políticas para telecomunicaciones se encuentra estrechamente relacionado con la superación de la brecha digital. Primero, los inversionistas privados y, cada vez más, los donantes públicos, no se encuentran dispuestos a invertir en los países sin contar con un ambiente institucional y legal para el desarrollo de Internet. Segundo, el desarrollo de los sectores nacionales de TIC depende de la creación de los marcos reguladores necesarios. Tercero, la existencia de monopolios nacionales de telecomunicaciones usualmente se menciona como una de las razones para los elevados costos de acceso a Internet.

La creación de un ambiente apto es una tarea demandante que involucra la desmonopolización gradual del mercado de las telecomunicaciones, la introducción de leyes relacionadas con Internet (que cubran los derechos de autor, la privacidad, el comercio electrónico, etc.) y el otorgamiento de acceso para todos sin restricciones políticas, religiosas o de otra índole.

El debate sobre el impacto que tiene la liberalización del mercado de las telecomunicaciones en el desarrollo se centra en dos puntos de vista do-

minantes. El primero es que la liberalización no ha beneficiado a los países en desarrollo. Con la pérdida de los monopolios de telecomunicaciones, los gobiernos del mundo en desarrollo han perdido una fuente importante de ingresos en sus presupuestos. La disminución en los presupuestos afecta los demás sectores de la vida social y económica. Según esta perspectiva, quienes pierden son los gobiernos en los países en desarrollo y quienes ganan son las empresas de telecomunicaciones del mundo desarrollado. La segunda perspectiva es que la apertura de los mercados de telecomunicaciones generó una mayor competencia que a su vez aumentó la calidad en el servicio y redujo los costos. En última instancia, esto conducirá a un sector de telecomunicaciones eficiente y asequible, una condición previa para el desarrollo general de la sociedad.

SECTION 6

# La Canasta Sociocultural

## LA CANASTA SOCIOCULTURAL

Las redes que conectan computadoras existen desde antes de la creación de Internet. Lo que hace a Internet diferente es que facilita las diferentes formas de comunicación y creatividad humanas. Los mayores adelantos están relacionados con la manera en que Internet se utiliza para desarrollar nuevos modos de comunicación (e-mail, Web, multimedios). En este contexto, algunos autores discuten que Internet es más un fenómeno social que tecnológico ya que complementa las comunicaciones tradicionales y además ofrece nuevas formas propias de comunicación (p. ej. las cibercomunidades). Estos acontecimientos han llevado al desarrollo de un aspecto sociocultural en Internet. La canasta sociocultural incluye algunos de los temas más controversiales en el campo de la Gobernanza de Internet, tales como la política de contenido y la multiplicidad de idiomas. Estos temas reflejan en particular las diferencias nacionales, religiosas y culturales más frecuentes hoy en día.

### POLÍTICA DE CONTENIDO

Uno de los principales asuntos socioculturales es la política de contenido, a menudo presentada desde el punto de vista de los derechos humanos (libertad de expresión y derecho a la comunicación), el gobierno (control de contenido), y la tecnología (herramientas para el control de contenido) por mencionar algunos.

Las discusiones sobre contenido usualmente se enfocan en tres grupos. El primer grupo es el contenido que cuenta con consenso global para su control. Se incluye aquí la pornografía infantil y algunos temas como la justificación del genocidio y el incitamiento u organización de actos terroristas, ya de por sí prohibidos por el derecho internacional (ius cogens). Aunque se ha alcanzado consenso para remover este contenido de la Red, aún existen diferentes interpretaciones. Por ejemplo ¿qué es exactamente un acto de apoyo al terrorismo?

El segundo grupo es el contenido que podría ser de carácter delicado para países, regiones o grupos étnicos en particular debido a sus valores

religiosos y culturales específicos. El alcance global y el aumento en la intensidad de las comunicaciones desafía los valores culturales y religiosos locales. La mayor parte de los procesos judiciales surgen a partir de este tipo de contenido. En el Caso de Yahoo!, un tribunal francés pidió a Yahoo.com (USA) prohibir a los ciudadanos franceses el acceso a partes de un sitio Web que vendía materiales y objetos de interés del nazismo. Alemania cuenta con jurisprudencia muy desarrollada y muchos procesos judiciales contra propietarios de sitios web que albergan materiales nazistas. La mayor parte del control de contenido que se ejerce en los países de Oriente Medio y Asia se justifica a nivel oficial como la protección de valores culturales específicos. Esto usualmente incluye bloquear el acceso a sitios Web que ofrecen pornografía y apuestas.

*El tercer grupo* se refiere al contenido que podría generar susceptibilidad política e ideológica. En esencia, esto se refiere a la censura de Internet. La organización Transparencia Internacional ha reportado una serie de prácticas de este tipo en China, Birmania y Arabia Saudita.

## ¿DE QUÉ MANERA SE PLANTEA LA POLÍTICA DE CONTENIDO?

Un menú a la carta de la política de contenido contiene las siguientes opciones legales y técnicas utilizadas en diferentes combinaciones.

### Filtrado Público del Contenido (a nivel gubernamental)

El elemento común para el filtrado gubernamental es un "Índice de Internet" que contiene los sitios Web cuyo acceso ha sido bloqueado para los ciudadanos. Si un sitio Web ha sido incluido en el "Índice" a los usuarios se les negará el acceso. Técnicamente hablando, el filtro típicamente utiliza bloqueo de IP basado en routers, servidores proxy y redirección a nivel de DNS. En muchos países se filtra el contenido. Además de los países usualmente asociados con estas prácticas (China, Arabia Saudita y Singapur), otros países lo implementan con creciente intensidad. Por ejemplo, Australia cuenta con un sistema de filtrado para páginas nacionales específicas. El estado alemán de Renania del Norte Westfalia solicitó a los ISPs filtrar el acceso, principal más no exclusivamente, a sitios neo-nazistas.

### Calificación Privada y Sistemas de Filtrado

Al enfrentarse al problema potencial de la desintegración de Internet por medio del desarrollo de diferentes barreras a nivel nacional (sistemas de

filtrado), el W3C y otras instituciones de ideas afines sugirieron la implementación de sistemas de calificación y filtrado controlados por los usuarios finales. Técnicamente hablando, los mecanismos de filtrado son integrados a los navegadores de Internet. La accesibilidad de cierto contenido en particular se indica por medio de una etiqueta que corresponde a un sitio web en particular. El uso de este tipo de filtros fue especialmente favorecido como un sistema para tener acceso exclusivo a sitios "inocuos para los niños".

### Software de Posicionamiento Geográfico

Otra solución técnica relacionada con el contenido es el software de posicionamiento geográfico, el cual filtra el acceso a cierto contenido Web dependiendo de la ubicación geográfica u origen nacional de los usuarios. El Caso Yahoo! fue importante en este sentido ya que el grupo de expertos involucrados, incluyendo a Vint Cerf, indicaron que en un 90% de los casos Yahoo! era capaz de determinar cuáles secciones de uno de sus sitios web eran visitadas desde Francia. Esta evaluación tecnológica ayudo al tribunal a desarrollar su veredicto. Las empresas productoras de software de posicionamiento geográfico dicen que pueden identificar el país de origen sin errores y la ciudad en el 85% de los casos, sobre todos si se trata de una ciudad grande. El software de posicionamiento geográfico puede ayudar a diferentes proveedores de contenido en Internet a filtrar el acceso según la ubicación de un usuario y por lo tanto evitar procesos judiciales en jurisdicciones extranjeras.

### Control de Contenido por medio de Motores de Búsqueda

Existe una diferencia importante entre disponibilidad y accesibilidad de los materiales en Internet. El hecho de que una página web o contenido específico se encuentre disponible en Internet, no significa que será visto por muchos usuarios. Por ejemplo, si un sitio Web en particular no aparece en Google, su relevancia se ve seriamente disminuida. El puente entre el usuario final y el contenido Web es usualmente un motor de búsqueda. Ha sido ampliamente publicitado que uno de los primeros ejemplos de control de contenido por medio de motores de búsqueda fue implementado por las autoridades chinas con el motor de búsqueda Google. Si los usuarios ingresan palabras prohibidas en sus búsquedas en Google, pierden su conexión IP durante algunos minutos. El departamento Chino de información declaró: "En Internet es muy corriente que a veces es posible ingresar a un sitio Web y a veces no. El ministerio no ha recibido información sobre bloqueos a Google".

Con el fin de ajustarse a la legislación local, Google decidió restringir algunos materiales en sus sitios web nacionales. Por ejemplo, en la versión Francesa y Alemana de Google, no es posible buscar ni encontrar sitios web con materiales nazistas. Esto indica un cierto nivel de autocensura de parte de Google con el fin de evitar posibles procesos judiciales.

### La Necesidad de Establecer un Marco Legal Apropiado

El vacío legal en el campo de las políticas de contenido que caracterizó el uso inicial de Internet, brindó a los gobiernos altos niveles de discreción en cuanto al control del contenido. Es necesario adoptar instrumentos legales debido a que la política de contenido es un tema sensible para todas las sociedades. La regulación nacional en el campo de las políticas de contenido podría brindar mejor protección a los derechos humanos y aclarar los roles a veces ambiguos de los proveedores de servicios de Internet, las autoridades y otros involucrados. En años recientes, muchos países han introducido legislación sobre políticas de contenido.

### Iniciativas Internacionales

A nivel internacional, las principales actividades están relacionadas con los países europeos que cuentan con legislaciones sólidas en el campo del discurso del odio, incluyendo el racismo y el antisemitismo. Las instituciones regionales europeas han venido tratando de imponer estas reglas en el ciberespacio. El instrumento legal clave en el tema del contenido es el Protocolo Adicional a la Convención sobre Cibercrimen del Consejo de Europa. El protocolo especifica diferentes tipos de discursos del odio que deberían ser prohibidos en Internet, incluyendo materiales racistas y xenófobos, así como justificaciones para el genocidio y los crímenes contra la humanidad.

La Organización para la Seguridad y la Cooperación de Europa (OSCE) se encuentra particularmente activa en este campo. En junio 2003, la Conferencia sobre la Libertad de los Medios de Comunicación en Internet de la OSCE adoptó las Recomendaciones de Ámsterdam sobre la Libertad de los Medios de Comunicación en Internet. Las recomendaciones promueven la libertad de expresión y procuran reducir la censura en Internet. En junio 2004, la OSCE organizó la Reunión sobre la Relación entre la Propaganda Racista, Xenófoba y Antisemítica en Internet y los Delitos Motivados por el Odio (París, 16 al 17 de junio de 2004). El evento se enfocó en los posibles abusos en el uso de Internet y la libertad de expresión. Los eventos de la OSCE ofrecieron una amplia variedad de

perspectivas académicas y normativas relacionadas con estos dos aspectos del control de contenido.

La Unión Europea ha llevado a cabo diversas iniciativas en el contexto del control de contenido, adoptando la Recomendación de la Comisión Europea contra el Racismo y la Intolerancia por Internet. A un nivel más práctico, la Unión Europea introdujo el Plan de Acción para una Internet más Segura, que incluye los siguientes puntos principales:

- establecer una red de líneas directas en Europa para reportar contenidos ilegales;
- motivar la autorregulación;
- desarrollar calificaciones, filtros y filtros con puntos de referencia (benchmarks) para el contenido;
- desarrollar software y contenido;
- aumentar la conciencia sobre el uso seguro de Internet.

## LOS ASUNTOS

### Control de Contenido vrs. Libertad de Expresión

Cuando se habla de control de contenido, el otro lado de la moneda es a menudo una restricción a la libertad de expresión. Esto resulta especialmente importante en los Estados Unidos, donde la Primera Enmienda de la Constitución garantiza una amplia libertad de expresión, incluso el derecho de publicar materiales nazistas y similares. Alcanzar un balance apropiado entre el control de contenido y la libertad de expresión constituye un desafío considerable. La mayor parte de los debates recientes sobre Gobernanza de Internet, incluyendo los procesos judiciales y la reglamentación legislativa, han estado relacionados con la búsqueda de este balance.

El Congreso de los Estados Unidos se ha inclinado hacia un control más estricto del contenido, mientras que la Corte Suprema busca proteger la Primera Enmienda (la Libertad de Expresión). El ejemplo más notable es la Ley sobre Decencia en las Comunicaciones del Congreso de los Estados Unidos (1996), que fue declarada inconstitucional por la Corte Suprema sustentándose en que violaba la Primera Enmienda.

La libertad de expresión da forma en gran parte a la posición de los Estados Unidos en el debate sobre Gobernanza de Internet. Por ejemplo, aunque Estados Unidos ha firmado la Convención sobre Cibercrimen, no puede firmar el Protocolo Adicional de la convención que trata sobre el

discurso del odio y el control de contenido. La cuestión de la libertad de expresión también fue presentada dentro del contexto del proceso judicial contra Yahoo!. Esta es la línea más allá de la cual Estados Unidos se niega a caminar en las negociaciones internacionales.

### "Ilegal Fuera de Línea - Ilegal en Línea"

Esto conduce la discusión sobre contenido hacia el dilema entre el mundo "real" y el "cibernético". Las normas existentes para el contenido pueden ser implementadas en Internet. Esto es frecuentemente destacado dentro del contexto europeo. La Decisión Marco del Consejo de Europa de Combatir el Racismo y la Xenofobia explícitamente indica que "lo que es ilegal fuera de línea es ilegal en línea". Uno de los argumentos del enfoque cibernético a la regulación de Internet es que la cantidad (intensidad de comunicación y número de mensajes) hace una diferencia cualitativa. Desde esta perspectiva, el problema del discurso del odio no es que no existen regulaciones en su contra, sino que la participación y amplitud de Internet lo convierte en un tipo diferente de problema legal. Una mayor cantidad de individuos están expuestos y resulta difícil aplicar las normas existentes. Por lo tanto, la diferencia que genera Internet está principalmente relacionada con los problemas de aplicación y no con las normas mismas.

### Efectividad del Control de Contenido

Dentro de las discusiones sobre políticas de Internet, uno de los argumentos es que la naturaleza descentralizada de Internet permite evadir la censura. Internet incluye muchas técnicas y tecnologías que pueden ofrecer un control efectivo, sin embargo, técnicamente hablando, los mecanismos de control pueden ser evadidos. --- En los países que cuentan con control de contenido dirigido por el gobierno, los usuarios talentosos han encontrado formas de evadirlo. No obstante, el control de contenido no está dirigido a este pequeño grupo de usuarios técnicamente talentosos, sino a la población en general. Lessing ofrece una declaración concisa sobre este problema: *"La regulación no requiere ser absolutamente efectiva para ser suficientemente efectiva".*

### ¿Quién Debería Responsabilizarse por la Política de Contenido?

Los gobiernos son los principales involucrados en el área de políticas de contenido. Los gobiernos indican qué debe ser controlado y cómo hacerlo. Algunos grupos de usuarios individuales, como los padres, demues-

tran su entusiasmo por introducir una política de control más eficiente en la protección de los niños. Varias iniciativas de calificación se dirigen a asistir a los padres a filtrar el contenido nocivo para los niños. La política de contenido también es aplicada por empresas privadas y universidades que desean restringir el acceso a ciertos materiales. En algunos casos, el contenido es controlado por medio de paquetes de software; por ejemplo, el movimiento de la Cientología ha distribuido entre sus miembros un paquete de software llamado Scienositter que limita el acceso a sitios que critican la Cientología.

Una iniciativa innovadora es la Fundación Internet Watch del Reino Unido, la cual busca combatir el abuso infantil en Internet. La fundación es una iniciativa de multisectorial establecida por el gobierno, proveedores de servicios de Internet y representantes de los usuarios.


## DERECHOS HUMANOS

Internet ha brindado a la sociedad nuevas formas de comunicación e interacción y en última instancia ha influenciado el concepto tradicional de los derechos humanos. Un conjunto básico de derechos humanos relacionados con Internet incluye la privacidad, la libertad de expresión, el derecho a la información, el derecho a la educación, así como diferentes derechos que protegen la diversidad cultural, lingüística y minoritaria. Durante la primera fase de la CMSI, muchos grupos de la sociedad civil propusieron la introducción de un derecho a comunicarse que va más allá de los derechos actualmente relacionados con Internet.

Los derechos humanos actuales que no han sido cubiertos en otras secciones de este folleto se tratan brevemente a continuación.

### La Libertad de Expresión y el Derecho a Buscar, Recibir e Impartir Información

This is one of the fundamental human rights, usually appearing in the Este es uno de los derechos humanos fundamentales que usualmente aparece en el foco de las discusiones sobre políticas de contenido y censura. En la Declaración de Derechos Humanos de la ONU, la libertad de expresión se contrapesa con el derecho del estado a limitar la libertad de

expresión para proteger la moralidad, el orden público y el bienestar general (Artículo 29). De este modo, tanto la discusión como la implementación del Artículo 19 deben colocase dentro del contexto del establecimiento de un balance apropiado entre ambas necesidades. Este régimen ambiguo abre muchas posibilidades para diferentes interpretaciones de las normas y en última instancia diferentes implementaciones.

### El Derecho a la Privacidad

El Derecho a la Privacidad se discute en la Canasta Legal (p. 69).

### Derechos de Propiedad Intelectual

Los derechos de propiedad intelectual le otorgan a cualquier persona el derecho de disfrutar de los intereses morales y materiales resultantes de las producciones científicas, literarias o artísticas. Este derecho se contrapesa con el derecho de todos a participar libremente en la vida cultural y a compartir los avances científicos. Alcanzar un balance entre estos dos derechos es uno de los principales desafíos de la Gobernanza de Internet.


## MULTIPLICIDAD LINGÜÍSTICA Y DIVERSIDAD CULTURAL

Desde sus primeros días, Internet se ha desarrollado predominantemente en el medio angloparlante. Según algunas estadísticas, aproximadamente el 80% del contenido web se encuentra en Inglés. La situación ha motivado a muchos países a tomar acciones concertadas para promover la multiplicidad lingüística y proteger la diversidad cultural. La promoción de la multiplicidad lingüística no solo es un tema cultural, sino que se relaciona directamente con la necesidad de continuar el desarrollo de Internet. Si se pretende que Internet sea utilizada por sectores más amplios de la sociedad y no únicamente las élites nacionales, entonces el contenido debe estar disponible en más idiomas.

### LOS ASUNTOS

Primero, la promoción de la multiplicidad lingüística requiere estándares técnicos que faciliten el uso de alfabetos no latinos. Una de las

primeras iniciativas relacionadas con la multiplicidad lingüística en el uso de las computadoras fue el Unicódigo. El Consorcio Unicódigo es una institución sin fines de lucro que desarrolla estándares que facilitan el uso de conjuntos de caracteres en diferentes idiomas. Recientemente ICANN e IETF dieron un importante paso al promover nombres de dominio internacionales escritos en Chino, Árabe y otros alfabetos no latinos.

Segundo, muchos esfuerzos han procurado mejorar la traducción mecánica. Dada su política de traducir todas las actividades oficiales a los idiomas de los estados miembros, la Unión Europea ha apoyado varias actividades de desarrollo en el campo de la traducción mecánica. Aunque algunos adelantos han sido alcanzados, todavía existen limitaciones.

Tercero, la promoción de la multiplicidad lingüística requiere marcos gubernamentales apropiados. El primer elemento de los regímenes de gobernanza ha sido aportado por organizaciones como la UNESCO. UNESCO ha incitado muchas iniciativas enfocadas en la multiplicidad lingüística, incluyendo la adopción de importantes documentos, como la Declaración Universal sobre la Diversidad Cultural. Otro promotor clave de la multiplicidad lingüística es la Unión Europea, ya que incorpora la multiplicidad lingüística como uno de sus principios políticos y operacionales básicos.


## BIEN PÚBLICO GLOBAL

El concepto del Bien Público Global puede ser relacionado con muchos aspectos de la Gobernanza de Internet. Las conexiones más directas se encuentran en las áreas de acceso a la infraestructura de Internet, la protección del conocimiento desarrollado a través de la interacción en Internet, la protección de los estándares técnicos públicos y el acceso a la educación en línea.

La infraestructura de Internet es administrada predominantemente por empresas privadas. Uno de los desafíos actuales es la armonización de la propiedad privada de la infraestructura de Internet con el estatus de Internet como bien público global. Las leyes nacionales ofrecen la posibili-

dad de introducir restricciones a la propiedad privada con algunos requerimientos públicos, incluyendo otorgar derechos equivalentes a todos los usuarios potenciales y no interferir en el transporte del contenido.

Una de las características clave de Internet es que a través de la interacción mundial de los usuarios se generan nuevos conocimientos e información. Cantidades considerables de conocimientos han sido generados por medio de intercambios en listas de correo, grupos de discusión y blogs. En muchos casos, no existen mecanismos legales internacionales para proteger ese conocimiento. Al quedar en el vacío legal, el conocimiento puede ser convertido en mercancía y comercializado por los individuos. Este acervo de conocimientos es una base importante de creatividad y se encuentra en riesgo de ser diezmado. Entre más se comercialice Internet, menos espontáneos serán los intercambios. Esto podría conducir a una reducción en la interacción creativa. El concepto de bienes públicos globales podría aportar soluciones que también protegieran el conocimiento común de Internet para las generaciones futuras.

En cuanto a la estandarización, se llevan a cabo esfuerzos prácticamente continuos para reemplazar los estándares públicos por estándares privados y patentados. Este fue el caso de Microsoft (con los navegadores y ASP) y Sun Microsystems (con Java). Los estándares de Internet (principalmente TCP/IP) son considerados abiertos y públicos. El régimen de Gobernanza de Internet debería garantizar la protección de los principales estándares de Internet como bienes públicos globales.

#### La Protección de Internet como Bien Público Global

Algunas soluciones basadas en el concepto de Internet como bien público global pueden ser desarrolladas a partir de conceptos económicos y globales existentes. Por ejemplo, la teoría económica cuenta con un concepto bien desarrollado de "bienes públicos", extendido a nivel internacional como "bienes públicos globales". Un bien público debe contar con dos propiedades críticas: no ser fungible (no ser susceptible de rivalidad) ni excluyente. Lo anterior estipula que el consumo por parte de un individuo no afecta el consumo por parte de otro; y que es difícil, sino imposible, excluir a un individuo del disfrute del bien. A nivel global, el Programa de las Naciones Unidas para el Desarrollo (PNUD) ha introducido el concepto de bienes públicos globales. Una solución potencial que ofrece el derecho internacional es el concepto res communis omnim (espacio como herencia común de la humanidad a ser regulado y cosechado por todas las naciones).

Será importante considerar cuáles de estos conceptos podrían ser aplicados a Internet y cuáles serían las consecuencias. Muchos están de acuerdo en que el modelo para el desarrollo futuro de Internet dependerá del establecimiento de un balance apropiado entre intereses privados y públicos.


## EDUCACIÓN

Internet ha abierto nuevas posibilidades para la educación. Varias iniciativas de "aprendizaje electrónico", "aprendizaje en línea" y "aprendizaje a distancia" han sido introducidas y su principal objetivo es utilizar Internet como medio de acceso a sus cursos. Aunque el aprendizaje en línea no puede remplazar la educación tradicional, este ofrece nuevas posibilidades para el aprendizaje, especialmente cuando las limitaciones de tiempo y espacio impiden a las personas asistir en persona a las clases. Algunos estimados pronostican que el mercado de aprendizaje en línea alcanzará aproximadamente US$10,000 millones para 2010.

El aprendizaje electrónico también ha intensificado la educación transfronteriza, con estudiantes participando en cursos en línea impartidos desde otros países. Esto ha introducido una dimensión de gobernanza internacional al sector educativo.

Tradicionalmente, la educación ha sido gobernada por las instituciones nacionales. La acreditación de las instituciones educativas, el reconocimiento de las calificaciones y el aseguramiento de la calidad son todos gobernados a nivel nacional. Sin embargo, la educación transfronteriza requiere del desarrollo de nuevos regímenes de gobernanza. Muchas iniciativas internacionales buscan cerrar la brecha de gobernanza, especialmente en áreas como aseguramiento de la calidad y reconocimiento de grados académicos.

### La OMC y la Educación

Un tema controversial en las negociaciones de la OMC es la interpretación de los Artículos 1 (3) (b) y (c) del Acuerdo General sobre el Comercio de Servicios, que especifica excepciones al régimen de libre comercio para los servicios brindados por el estado. Según una perspectiva,

apoyada principalmente por los Estados Unidos y el Reino Unido, estas excepciones deben ser tratadas restringidamente, posibilitando de facto el libre comercio en educación superior. Este punto de vista predominantemente gobernado por los intereses del sector educativo de los Estados Unidos y el Reino Unido de obtener cobertura global en el mercado educativo ha recibido considerable oposición por parte de muchos países.

El principal argumento contra esta perspectiva es que las universidades ofrecen bienes públicos y que juegan una importante función social y cultural en cada país, más allá de la simple transferencia de conocimiento e información. Según esta perspectiva, el mercado global libre en educación podría poner en peligro el futuro de las universidades en países pequeños y en desarrollo y generar el dominio educativo por parte de instituciones de los Estados Unidos y el Reino Unido, lo que reduciría considerablemente la diversidad cultural y privaría a muchas sociedades del rol universitario como catalizador en el desarrollo de cultura nacional. Otra crítica al libre comercio en educación es su potencial incompatibilidad con la implementación del derecho a la educación.

El próximo debate, que probablemente se desarrollará dentro del contexto de la OMC y otras organizaciones internacionales, se enfocará sobre el dilema de la educación como mercancía o como bien público. Si la educación es considerada como una mercancía, las normas de la OMC también se implementarían en este campo. Por otro lado, el enfoque del bien público preservaría el modelo actual de educación, en el cual las universidades privadas reciben un estatus especial como instituciones de importancia para la cultura nacional. El resultado de este debate tendrá un impacto considerable en el desarrollo del aprendizaje en línea.

### Aseguramiento de la Calidad

La disponibilidad de sistemas para ofrecer aprendizaje en línea y el fácil ingreso a este mercado ha planteado preguntas sobre el aseguramiento de la calidad. El enfoque sobre la entrega en línea podría pasar por alto la importancia de la calidad de los materiales y la didáctica. Una serie de dificultades factibles podrían poner en peligro la calidad de la educación. Una de ellas sería el fácil ingreso de instituciones nuevas con orientación principalmente comercial, las cuales a menudo cuentan con pocas de las capacidades académicas y didáctica necesarias. Otro problema del aseguramiento de la calidad es que la simple

transferencia de materiales ya impresos a un medio en línea no saca el máximo provecho del potencial didáctico del nuevo medio.

A nivel internacional se ha iniciado discusiones sobre el aprendizaje transnacional en general y el aprendizaje en línea en particular. Uno de los primeros intentos integrales por brindar aseguramiento de la calidad a los programas educativos transnacionales es el "Código de Buenas Prácticas en la Provisión de Educación Transnacional" de la UNESCO y el Consejo de Europa."

### El Reconocimiento de Grados Académicos y la Transferencia de Créditos

El reconocimiento de grados se ha vuelto particularmente relevante dentro del ambiente del aprendizaje en línea. Cuando se trata de aprendizaje en línea, el principal desafío es el reconocimiento de los grados más allá del contexto regional, principalmente a nivel global.

Una tendencia general hacia la movilidad estudiantil en la educación superior hace que sea posible estudiar en una serie de universidades. La Unión Europea, en particular, ha dado pasos en este campo a través de varias iniciativas como "SÓCRATES". La movilidad estudiantil requiere la transferencia de créditos entre universidades en diferentes países. Los marcos reguladores necesarios han empezado a ser desarrollados a nivel regional. La Unión Europea empezó a desarrollar el marco regulador con el Sistema Europeo de Transferencia y Acumulación de Créditos (ECTS por sus siglas en inglés). La región Asia-Pacífico sigue el liderazgo europeo al introducir su propio modelo regional para el intercambio de estudiantes y el sistema respectivo de créditos (UCTS).

### La Estandarización del Aprendizaje en Línea

La fase inicial de desarrollo del aprendizaje en línea estuvo caracterizada por el rápido desarrollo y la alta diversidad de los materiales, en el sentido de plataformas, contenido y didáctica. Sin embargo, existe la necesidad de desarrollar estándares comunes para facilitar el intercambio de cursos en línea e introducir un cierto estándar de calidad.

El primer estándar, AICC (Comité CBT de la Industria de Aviación) fue desarrollado por la asociación de la industria de la aviación con el objetivo principal de ofrecer interoperabilidad en los paquetes de aprendizaje en línea. El siguiente desarrollo importante fue la introducción del IMS (Sistema de Gestión de la Instrucción) el cual aportó una serie de

estándares para el aprendizaje en línea, incluyendo especificaciones de metadatos que podían ser compartidas por los cursos de aprendizaje en línea (una descripción del contenido, título del curso, autores, costo, taxonomía de aprendizaje, etc.). El IMS está basado en XML (Lenguaje Extensible de Marcas). Además, el Comité de Estándares para la Tecnología del Aprendizaje (LTSC) del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) ha establecido una cierta estandarización.

El Departamento de Defensa de los Estados Unidos inició el desarrollo más reciente en 1997. Al enfrentar las limitaciones de todos los estándares existentes, el Departamento de Defensa estableció la iniciativa de Aprendizaje Distribuido Avanzado (ADL por sus siglas en inglés), la cual produjo un nuevo estándar denominado Modelo de Referencia para Objetos de Contenido Intercambiable (SCORM por sus siglas en inglés). SCORM es el estándar más elaborado y de más amplia adopción entre los cursos en línea. Una de las razones para el éxito de SCORM es que se ha convertido en el estándar requerido para los cursos que se ofrecen al Departamento de Defensa (un mercado de US$ 700 millones anuales) y otros departamentos del gobierno de los Estados Unidos. SCORM también está obteniendo una amplia visibilidad y aceptación a nivel internacional.

La mayor parte del esfuerzo de estandarización es llevado a cabo por las instituciones privadas y profesionales de los Estados Unidos. Otras iniciativas, incluyendo algunas internacionales, se llevan a cabo a una escala mucho menor.

SECTION 7

# Anexos

# ANEXO I

## "LOS CIEGOS Y EL ELEFANTE"

<table>
<tr><td colspan="2">Había una vez seis hombres del Indostán<br>Muy inclinados al aprendizaje,<br>Que fueron a conocer al Elefante<br>(Pero todos ellos eran ciegos),<br>Para que cada uno por observación<br>Pudiera satisfacer su percepción.</td></tr>
<tr><td>El primero se acercó al Elefante,<br>Y cayendo accidentalmente<br>Contra el costado amplio y macizo,<br>Al instante empezó a vociferar:<br>"Qué Dios me ampare! pero el Elefante<br>¡Es ciertamente como una pared!"</td><td>El cuarto estiró una ansiosa mano,<br>Y palpó la rodilla.<br>"Que maravillosa es esta bestia<br>Es bastante simple", dijo él;<br>"Me queda muy claro que el Elefante<br>¡Es ciertamente como un árbol!"</td></tr>
<tr><td>El Segundo, palpando el colmillo,<br>Gritó, "¡ajajá! ¿Qué tenemos aquí<br>Tan redondo suave y puntiagudo?<br>A mi me queda totalmente claro<br>Esta maravilla de Elefante<br>Es ciertamente como una lanza!"</td><td>El quinto que alcanzó a tocar la oreja,<br>Dijo: "Hasta el más ciego de los hombres<br>Puede decir a qué se parece más;<br>¡Niégueme el que pueda,<br>Este prodigio de Elefante<br>Es ciertamente como un abanico!"</td></tr>
<tr><td>El Tercero se acercó al animal,<br>Y habiéndolo tomado<br>por el escurridizo moco con las manos,<br>audazmente habló;<br>"Veo", dijo él, "que el Elefante<br>Es ciertamente como una serpiente!"</td><td>El Sexto en cuanto a tientas<br>la bestia palpó,<br>tomó la cadenciosa cola<br>que a su alcance llegó,<br>"Veo", dijo él, "que el Elefante<br>Es ciertamente como una cuerda!"</td></tr>
<tr><td colspan="2">Y estos hombres del Indostán<br>Discutieron largo y tendido,<br>Cada uno con su propia opinión<br>Sumamente rígida y firme,<br>Y aunque todos tenían algo de verdad,<br>¡Todos estaban equivocados!<br>Moraleja: A menudo en las guerras teológicas<br>Los disputantes, digo yo,<br>Recriminan en total ignorancia<br>De lo que quiere decir el otro,<br>Y parlotean sobre un Elefante<br>¡Que ninguno de ellos ha visto!</td></tr>
<tr><td colspan="2">Poeta Estadounidense John Godfrey Saxe (1816-1887)</td></tr>
</table>

## ANEXO II – LA EVOLUCIÓN DE LA GOBERNANZA DE INTERNET

| Actor / Periodo | Estados Unidos | "Guardianes" de Internet | Organizaciones Internacionales | Sector Privado | Países | Sociedad Civil |
|---|---|---|---|---|---|---|
| | El Departamento de Defensa (DoD) corre el DNS | | | | | |
| 1986 | La Fundación Nacional de las Ciencias (NSF) asume después del DoD | | | | | |
| 1994 | | | | NSI firma un contrato con NSF para manejar el DNS de 1994-1998 | | |
| EL INICIO DE LA "GUERRA DEL DNS" Después que NSF subcontrata la administración del DNS a NSI (una empresa privada), la comunidad de Internet (principalmente ISOC) trata por muchos años de devolver la administración del DNS al dominio público. Tiene éxito después de 4 años. Este es un estudio de este proceso, que involucra una gran cantidad de técnicas diplomáticas, como: negociación, desarrollo de coalición, utilización de influencias, desarrollo de consenso, etc. | | | | | | |
| Junio 1996 | | IANA/ISOC – Plan para asumir después de NSI al finalizar su contrato; introducción de dominios adicionales; fuerte oposición del sector de marcas registradas contra nuevos dominios superiores; también fuerte oposición de la UIT. | | | | |
| Primavera 1997 | | Un Comité Internacional Ad Hoc (IAHC) Participantes en la Propuesta: 2 representantes de los grupos interesados de marcas registradas, OMPI, UIT y NSF; y 5 representantes de IETF. Conclusión de MoU para gTLD: DNS como "recurso público"; siete nuevos dominios; fuerte protección para marcas registradas". Establecimiento de CORE (Consejo de Registradores – ceremonia de firma Marzo 1997 en UIT, Ginebra); CORE colapsa inmediatamente. Fuerte oposición del gobierno de Estados Unidos, NSI y Unión Europea. | | | | |
| 1997 | El gobierno de los Estados Unidos transfiere la administración de DNS al Departamento de Comercio (DoC) | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Junio 1998 | Libro Blanco del DoC invita a los principales interesados a proponer sus propias soluciones | las propuestas se reciben de: IFDT (Foro Internacional sobre Libro Blanco), ORSC (Confederación Abierta de Servidor Raíz_ y BWG (Grupo de Trabajo de Boston) | | | | |
| | | En lugar de preparar un nuevo documento, ISOC se enfoca en: - Desarrollar una amplia coalición involucrando organizaciones internacionales (desde la iniciativa IAHC), el sector privado (IBM) y países clave (Unión Europea, Japón, Australia). - Crear una nueva organización | | | | |
| Segunda parte 1998 | | Setiembre 1998 – Acuerdo Borrador Conjunto ISOC-NSI Octubre 1998 – ISOC abandona acuerdos y crea ICANN | | | | |
| 15 Nov 1998 | DoC transfiere autoridad a ICANN | ICANN adquiere dos nuevas funciones cruciales: - Autoridad para acreditar registros para el gTLD – Manejo del rol autoritativo (el aspecto normativo se mantiene en el DoC) | | | | |
| Abril 1999 | | Acuerdo DoC – ICANN – NSI e introducción de "sistema compartido de registro"; NSI pierde su monopolio pero obtiene un acuerdo de transición favorable (administración de cuatro dominios, etc.) LA ESTRUCTURA Y FUNCIONAMIENTO DE ICANN | | | | |
| Junio 1998 | | Formación del PSO (Organización de Soporte del Protocolo) consistente de IETF, W3C y otros pioneros de Internet | Inicialización del Proceso de Nombres de Dominio de OMPI | ASO (Organización Soporte de Direcciones) creada para representar la asociación de registros DNS (ARN, RIPE, NCC) DNSO (Organización de Soporte Nombres de Dominio) – establecida para proteger los intereses comerciales y de marca registrada | 30 países establecen GAC para ganar mayor influencia al manejar dominios nacionales – ICANN reacciona estableciendo subcomité DNSO - ccTLDs | |
| FINAL DE LA "GUERRA DEL DNS" La "guerra" terminó por medio de un compromiso. ISOC logró obtener mayor control público en el manejo del DNS aunque los intereses comerciales siguen siendo muy fuertes. Por lo tanto, los intereses de las empresas privadas y las comunidades "guardianas" se encuentran protegidos apropiadamente. No sucedió así con la posición de los estados nacionales y la comunidad general de Internet. Estos son dos de los aspectos más débiles de la gobernanza de ICANN. | | | | | | |
| 2000-2003 | | | Surgimiento de un mayor enfoque sobre Internet en UIT, OMPI, UNESCO, OCDE, el Consejo de Europa y el Banco Mundial | Fuerte presión del sector privado para regular Internet (legislación copyright, comercio electrónico, etc.) | Desarrollo de legislación para Internet, procesos judiciales, etc. | Participación de ONGs en la brecha digital, derechos humanos, asuntos de género en Internet |
| | | | Iniciativas multisectoriales e iniciativas globales enfocadas en el desarrollo de Internet, gobernanza, etc.: Fuerza DOT G-8, Foro Económico Mundial, Fuerza Tareas TIC ONU, Cumbre Mundial de la Sociedad de la Información, Alianza para el Conocimiento Global | | | |

## ANEXO III - UN MAPA PARA UN VIAJE A TRAVÉS DE LA GOBERNANZA DE INTERNET

## ANEXO IV - EL CUBO DE GOBERNANZA DE INTERNET


| | |
|---|---|
| El eje del QUÉ se relaciona con los ASUNTOS de Gobernanza de Internet (ej. infraestructura, derechos de autor, privacidad). Transmite el aspecto multidisciplinario de este enfoque.<br><br>El eje del QUIÉN en este cubo se enfoca en los principales ACTORES (estados, organizaciones internacionales, sociedad civil, sector privado). Este es el enfoque multisectorial.<br><br>El eje del DÓNDE del cubo trata con el MARCO dentro del cual los asuntos de Internet deben ser tratados (autorregulador, local, nacional, regional, y global). Este es el enfoque de múltiples capas hacia la Gobernanza de Internet. | Cuando movemos piezas en nuestro cubo obtenemos la intersección – CÓMO. Esta es la sección del cubo que puede ayudarnos a ver la manera en que los asuntos particulares deben ser regulados, tanto en términos de técnicas cognitivas legales (p. ej. analogías) como en términos de instrumentos (p. ej. legislación blanda, tratados y declaraciones). Por ejemplo, una intersección específica puede ayudarnos a ver CÓMO los asuntos de privacidad (qué) deben ser tratados por la sociedad civil (quién) a nivel nacional (dónde).<br><br>Independientemente del Cubo de la Gobernanza de Internet existe un quinto componente – CUÁNDO |

# SOBRE LOS AUTORES

## Jovan Kurbalija

Jovan Kurbalija es el director fundador de DiploFoundation. Anteriormente fue diplomático con preparación profesional y académica en derecho internacional, diplomacia y tecnología de la información. Desde finales de la década de 1980 ha llevado a cabo investigaciones sobre las tecnologías de infocomunicaciones y el derecho. En 1992 estuvo a cargo de establecer la primera Unidad de TI y Diplomacia en la Academia Mediterránea de Estudios Diplomáticos en Malta. Después de más de diez años de empeño en los campos de la capacitación, la investigación y el mundo editorial, en 2003 la Unidad se convirtió en DiploFoundation

Jovan Kurbalija dirige cursos de aprendizaje en línea sobre TIC y diplomacia y da presentaciones académicas y de capacitación en instituciones en Suiza, los Estados Unidos, Austria, el Reino Unido, los Países Bajos y Malta. También fue miembro del Grupo Operacional de la ONU sobre Gobernanza de Internet.

Sus principales intereses investigativos incluyen: diplomacia y el desarrollo de un régimen internacional para Internet, el uso de hipertexto en la diplomacia, negociación en línea y derecho diplomático. .

**jovank@diplomacy.edu**

## Ed Gelbstein

Eduardo Gelbstein es Senior Special Fellow del Instituto de las Naciones Unidas para Formación Profesional e Investigaciones (UNITAR por sus siglas en inglés) y colaborador de la Fuerza de Tareas sobre Información y Telecomunicaciones (TIC) de las Naciones Unidas y del trabajo preparatorio para la Cumbre Mundial de la Sociedad de la Información. Anteriormente fue Director del Centro de Computación Internacional de las Naciones Unidas.

Además de su colaboración en las Naciones Unidas, es conferencista y charlista a nivel universitario reflejando sus 40 años de experiencia en la gestión de tecnologías de la información.

Ha trabajado en Argentina, los Países Bajos, el Reino Unido, Australia y después de integrarse a las Naciones Unidas en 1993, en Ginebra (Suiza) y Nueva York (Estados Unidos de América). Se graduó como ingeniero electrónico de la Universidad de Buenos Aires, Argentina en 1963 y cuenta con un grado de maestría obtenido en los Países Bajos y un grado de doctorado del Reino Unido.

gelbstein@diplomacy.edu

## BIBLIOTECA DE LA SOCIEDAD DE LA INFORMACIÓN

Existe un amplia variedad de textos sobre todos los temas relacionados con la gestión de la información y la tecnología de la información. Este folleto se suma a esta amplia colección y pretende cumplir con los siguientes objetivos:

- ofrecer a los lectores legos una perspectiva interna sobre los pocos principios importantes y razonablemente estables;
- presentar el materia dentro de un contexto relevante para la labor de aquellos involucrados en las relaciones internacionales;
- despertar la curiosidad de los lectores de manera que deseen ir un paso más allá de lo que se presenta en este folleto y deseen investigar y experimentar, desarrollando de esta manera el conocimiento y llevando a cabo acciones que satisfagan sus necesidades particulares.

El formato de estos folletos y sus contenidos surgen de los cursos impartidos por los autores durante los últimos años en diferentes ambientes, así como la retroalimentación de los participantes. Las opiniones de los lectores de estos folletos serían altamente valoradas por los autores y contribuirían a mejorar las futuras ediciones. Los datos de contacto de los autores se indican al final de este folleto.

## OTROS TÍTULOS DE LA BIBLIOTECA DE LA SOCIEDAD DE LA INFORMACIÓN

**Internet Basics** • Preguntas frecuentes, factores de juicio y problemas frecuentes

**Finding Information in Cyberspace** • De la irritación a la inspiración

**Good Hygiene for Data and Personal Computers** • Por qué y cómo proteger los datos y las computadoras personales

**Appropriate Use** • Pautas y mejores prácticas para correo electrónico y otros servicios en Internet

**Information Security and Organisations** • Guía para legos sobre los actores, las ofensas y las defensas efectivas

**Hacktivism, Cyber-terrorism and Cyberwar** • Las actividades de la sociedad incivil en el ciberespacio

**Online Learning for Professionals in Full Time Work** • A guide to what works and what does not

**Yellow Pages for the Information Society Library** • Un directorio de URLs recomendados

## SERIE CONOCIMIENTO PARA EL DESARROLLO

Esta publicación es parte de la serie Conocimiento para el Desarrollo de la Sociedad para el Conocimiento Mundial (GKP por sus siglas en inglés), un esfuerzo general para aumentar la disponibilidad de información y conocimientos sobre diferentes temas en el área de tecnologías de infocomunicaciones para el desarrollo (ICT4D).

## OTROS TÍTULOS DE LA SERIE CONOCIMIENTO PARA EL DESARROLLO

**Media and the Information Society**

**Multi-Stakeholder Partnerships**

**ICT for Development Success Stories**

**ICT for Poverty Reduction in Asia**

www.diplomacy.edu

Diplo *es una organización sin fines de lucro que brinda asistencia a todos los países, particularmente a aquellos con limitaciones de recursos, para que puedan participar de manera significativa en las relaciones internacionales. Diplo promueve un enfoque multisectorial que involucra la participación de organizaciones internacionales, la sociedad civil y otros actores en asuntos internacionales. Las actividades de Diplo incluyen programas de educación y capacitación, investigación y el desarrollo de tecnologías de información y comunicación para actividades diplomáticas.*

www.globalknowledge.org

La Sociedad para el Conocimiento Mundial (GKP) *es una red global comprometida a aprovechar el potencial de las tecnologías de información y comunicación (TICs) para el desarrollo sostenible y equitativo. La visión de GKP es la de un mundo con igualdad de oportunidades dentro del cual todas las personas tengan acceso y puedan utilizar el conocimiento y la información para mejorar sus vidas. La red permite el intercambio de información, experiencias y recursos para facultar a las personas y ayudar a reducir la pobreza.*

www.sdc.admin.ch

La Agencia Suiza para el Desarrollo y la Cooperación (COSUDE) *es la entidad encargada de la cooperación internacional dentro del Departamento Federal de Asuntos Exteriores (DFAE). Con otras oficinas de la Confederación, la COSUDE es responsable de la coordinación general de la cooperación para el desarrollo y de la cooperación con los Países del Este, así también como de los programas de ayuda humanitaria suizos.*

ISBN 99932-53-11-1