

CAPITULO III. HETERORREGULACIÓN: DIVERSAS MODALIDADES

***La realidad supera en dureza a la ficción:
los Gobiernos resultan necesarios para proteger la libertad,
incluso a pesar de bastarse por sí solos para destruirla²⁸⁷.***

Parece evidente tras el análisis efectuado en el capítulo anterior que la regulación más acorde con el Ciberespacio exige la combinación de diversos modelos normativos. A pesar de ello, y de momento, vamos a centrarnos en el análisis individualizado de la heterorregulación y de las diversas modalidades desde las que este sistema puede hacerse presente en la red. Soy consciente de que las alternativas de heterorregulación ofrecidas para el Ciberespacio pueden ser tan numerosas como autores aborden el estudio del tema, no obstante, se va a limitar el examen al estudio de la tipología más comúnmente aceptada o, al menos, más utilizada en los últimos tiempos. Los modelos heterorregulados que van a ser examinados a continuación son los siguientes:

1. Aplicación de la soberanía de los Estados nacionales. Esta opción trata de aplicar al Ciberespacio las leyes y las normas que regulan la vida de los ciudadanos dentro de cada Estado con el mismo rigor empleado en el mundo estrictamente físico. Este tipo conduce claramente al problema de la territorialidad de las normas.

287. LESSIG, L., *El código y otras leyes del Ciberespacio*, op. cit., p. 13.

2. Regulación mediante la creación de una legislación universal única para ordenar la totalidad de la red. Esta opción incluiría la creación de un Organismo Internacional único que se ocupara tanto de canalizar los nuevos procedimientos como de dictar y aplicar la normativa Internacional del Ciberespacio.

3. Regulación parcial de la red por medio de Tratados Internacionales, en los cuales se regulen de forma específica los problemas característicos de la red, como son el cibercrimen, la transmisión de datos internacionales, etc. Esta modalidad implica la renuncia de la soberanía nacional a favor del ejercicio de una soberanía compartida.

4. Por último serán considerados otros mecanismos de ordenación como la ordenación mediante la centralización de todos los proveedores de servicios de telecomunicaciones por una conexión central donde se procede a un minucioso control. Otra solución similar radica en actuar sobre los servidores y los proveedores de servicios de Internet, en la medida en que jurídicamente quepa y técnicamente sea posible responsabilizar a los unos y a los otros. Se examinarán, asimismo, otros medios menos reconocidos por su difícil aplicación práctica.

III.1. APLICACIÓN DE LA SOBERANÍA NACIONAL DE LOS ESTADOS A LA RED

Según este modelo cada Estado soberano tiene libertad y poder para regular Internet en la medida en que lo estimen necesario, eso sí, siempre en la parcela territorial y competencial sobre la que tiene poder soberano en el mundo físico. Éste ha sido el modelo adoptado por muchos Estados porque, se afirma, *no hay, actualmente, nada mejor para sustituirlo*²⁸⁸.

La mayor parte de los Gobiernos se están esforzando en poner orden en Internet. Ninguno de ellos se resigna a no hacer uso de su poder de crear normas aunque éstas resulten poco útiles o de cumplimiento com-

288. HICKS, B.D., *Choice of law issues in cyberspace*, Texas Tech University, Texas, 1996. Se puede acceder on line: www.geocities.com/athens/Academy/5090

plejo. Gracias a la acumulación de titulares relativos a la pornografía infantil, a virus informativos destructivos y a guerras electrónicas, los derechos fundamentales intocables en las sociedades democráticas se encuentran debilitados en Internet. Los Gobiernos hallan en este tipo de noticias, muchas veces marginales y con escasa entidad, justificación suficiente para comenzar a extender sus redes de poder de regulación sobre el territorio, hasta entonces más o menos virgen, del Ciberespacio.

La información es poder, y la información circula libremente por la red. El Estado que consiga imponer su ordenamiento y su poder en el Ciberespacio habrá obtenido un avance incalculable en la fuerza que le respalda. No obstante, la aplicación de las normas y del poder de los Estados nacionales a la parte de red que supuestamente se encuentra dentro de sus fronteras, a través de la regulación de los ciudadanos de ese país que se conectan a Internet en el territorio nacional, o a través de la regulación de los servidores radicados igualmente en ese país, no es una tarea fácil ni efectiva. La pérdida de significado de las fronteras estatales en este marco contrasta con el alcance típicamente territorial, vinculado a la noción de soberanía de las normas de los ordenamientos jurídicos estatales.

Internet constituye una tecnología de vocación mundial, universal sin fronteras físicas, entonces, ¿Cómo aplicar las fronteras legislativas a esta red de redes? No puede concebirse eficacia en el cumplimiento de unas normas estatales que pueden sortearse fácilmente. La comunicación y el suministro de servicios por las infovías es un fenómeno que sobrepasa las fronteras de los Estados y que, por tanto, no puede ser regulado, en lo necesario, solamente desde el nivel territorial. Es loable la justificación dada por los Estados para acometer la regulación de la red, más la protección de los derechos fundamentales de los internautas requiere el establecimiento de fórmulas de actuación que necesitan superar el ámbito de un solo Estado.

No obstante, parece que la falta de aplicabilidad práctica y la escasa eficacia que se presume tendrán las normas, no ha sido obstáculo ni ha persuadido a los Estados en su lucha por Internet. Los ejemplos sobre los intentos, y los logros, de aplicar la normativa nacional a la red han sido y siguen siendo múltiples. Un desarrollo completo a través de los diferentes países de la aplicación de este modelo lo encontramos en

la obra de HICKS. En ella se estudia este modelo aplicado por Estados Unidos, China, Singapur, Unión Europea, Reino Unido y Sudáfrica²⁸⁹.

A pesar de que la mayoría de los países ya han elaborado normas aplicables al Ciberespacio y han efectuado actos que tratan de regular abiertamente la red de redes, quizá el supuesto más trascendental de aplicación de una legislación nacional en la red ha sido el caso Yahoo!. Esta Sentencia ha sido mencionada anteriormente. No obstante, las incalculables consecuencias que provocó en el ámbito de la regulación de la red, aconsejan un examen exhaustivo de la misma en este lugar de la exposición. Para ello vamos a seguir el interesante desarrollo de los autores DE LA TORRE FORCADELL y COTINO HUESO²⁹⁰.

En su gama de servicios el buscador y portal Yahoo! pone a disposición de sus usuarios un canal de subastas (auctions.Yahoo.com) servicio que era abiertamente utilizado por simpatizantes y coleccionistas de objetos evocativos de la Alemania Nazi (hay que aclarar que en Francia la venta de este tipo de artículos está prohibido mientras en Estados Unidos no hay obstáculo legal para ello) Esta situación dio pie a que la LICRA (Liga contra el racismo y el antisemitismo) y la UEJF (Unión de los Estudiantes Judíos en Francia) demandasen al inicio del año 2000 a la empresa norteamericana Yahoo! Inc -con sede en California- y a su filial francesa Yahoo! fr ante el Tribunal *de Grande Instance de Paris*.

Frente a las alegaciones de los demandantes la Compañía americana Yahoo! Inc. presentó las siguientes pautas de defensa:

- La incompetencia territorial de la jurisdicción francesa para conocer del litigio, dado que los hechos encausados se cometieron desde el territorio de los Estados Unidos.
- El hecho de que la compañía había tenido un papel totalmente pasivo respecto al contenido de las subastas y que su función se limitaba a la transferencia de información.

289. *Ibid.*

290. COTINO HUESO, L. y DE LA TORRE FORCADELL, S., "El caso de los contenidos nazis en Yahoo! ante la jurisdicción francesa: un nuevo ejemplo de la problemática de los derechos fundamentales u de la territorialidad en Internet", *op. cit.*, pp. 904-916.

- La imposibilidad técnica que se producía de hecho para identificar territorialmente a los internautas que visitaban el servicio de subastas.

Tales alegaciones no tuvieron ningún eco en el mandamiento judicial dictado por el Juez Jean Jacques Gómez. En mayo de 2000 dictaminó la atracción de la jurisdicción a Francia, ya que permitir la visualización en ese país de tales objetos y la participación eventual de un internauta instalado en Francia supone la comisión de una falta en territorio francés. De igual modo dictó sentencia a favor de los demandantes. El texto de la resolución aplica directamente el Derecho natural ya que la motivación se encuentra más cercana a la búsqueda de la justicia universal que a la aplicación del Derecho positivo. En este sentido sorprende la falta de cobertura legal que tiene la persecución de los hechos denunciados en este asunto.

La Sentencia de 22 de Mayo de 2000 determinaba los siguientes aspectos:

- La obligación de destruir todo dato informático almacenado directa o indirectamente en su servidor y de cesar de albergar y poner a disposición sobre el territorio de la Republica Francesa, desde el servido Yahoo.com, de textos, imágenes o cualquier otro objeto prohibido en dicho territorio.
- La supresión en todas las guías de navegación accesibles desde Francia del descriptor *negacionista* y de todo enlace a cualquier hipertexto relacionado con el holocausto. No deja de sorprender el hecho de que se obligue a Yahoo! a retirar enlaces que siguen existiendo en otras páginas web en la red.
- La condena a Yahoo! Inc. y a Yahoo! fr. a pagar a la UEJF la suma de 10.000 francos y a Yahoo! Inc. a pagar a la LICRA la suma de 10.000 francos.
- La imposición a Yahoo! fr. de la obligación de incluir una advertencia para todo internauta que consultase Yahoo! fr. Dicha advertencia debía figurar antes de que pudiese activarse el enlace para continuar la búsqueda en el servidor de

Yahoo.com. El mensaje debería informar de los riesgos legales que asumiría el usuario si continuaba la consulta en esos sitios, páginas o foros cuyo título o contenidos estén estrictamente prohibidos por las leyes francesas.

- La inclusión en la página de inicio, tanto de Yahoo! fr como de Yahoo.com, de un extracto de la sentencia.

Esta Sentencia supuso el recrudescimiento del debate sobre la posibilidad de material de los Estados para regular la parte de red que, supuestamente, se encuentra bajo su jurisdicción. Si Internet constituye una tecnología de vocación mundial, universal, sin fronteras físicas, entonces, no es posible que se apliquen las fronteras legislativas a esta red de redes. Si esta jurisprudencia se generaliza, todos los propietarios de páginas y sitios web tendrían que respetar, no solo la ley francesa, sino todas aquellas leyes de cada uno de los Estados en los que operen. Como consecuencia, cada portal tendría que adaptarse a la legislación de cada país si no quiere tener problemas, pero es una labor muy compleja, dado el gran número de legislaciones existentes y la diversidad de las mismas.

Esta decisión ha planteado la duda de cómo puede una jurisdicción decidir lo que se puede o no mostrar en la red mundial. En otros casos recientes jueces alemanes e italianos han llegado a soluciones similares, y han declarado que las fronteras nacionales son tan válidas en el mundo virtual como lo son en el mundo físico. Se tiene la ingenua idea de que Internet lo cambia todo, sin embargo, afirma Ronald Katz, abogado del caso Yahoo! no lo cambia todo, no cambia las leyes de Francia. De repente Internet sin fronteras está chocando con fronteras de verdad. La imposición de leyes jurisdiccionales en Internet supondría que bien los editores en la red deciden mantener cierto tipo de material fuera de Internet por miedo a demandas civiles o penales en determinados países o bien que en diferentes regiones permiten solamente el acceso a determinados usuarios instalando puertas electrónicas y puntos de control alrededor de los sitios²⁹¹.

La empresa Yahoo! Inc. no acató tal decisión y poco después, el 21 de Diciembre de 2000, emprendía acciones legales ante la jurisdic-

291. En *The N.Y Times News*. Recogido por *Ciberp@is*, nº 12, junio 2001, p. 39.

ción norteamericana, por medio de una demanda ante un Juez californiano de S. José. A pesar de que el 03 de Enero de 2001, la empresa Yahoo! Inc anunció su decisión voluntaria de suprimir los sitios de subastas nazis, el procedimiento siguió adelante. Yahoo! Inc. alegaba que la sentencia del Tribunal Francés violaba la libertad de expresión, y lo que es más importante a nuestros efectos, había sido dictada sin observar los principios de jurisdicción.

El 9 de Noviembre de 2001, el juez californiano dictaminó que Yahoo! Inc. no tenía obligación alguna de acatar un fallo de un tribunal galo. El nuevo dictamen del juez estadounidense sienta un precedente en el sentido de que tanto empresas como individuos de ese país podrán invocar la ley estadounidense y el derecho a la libertad de expresión, con lo que los jueces extranjeros no podrán exigir que sitios estadounidenses eliminen contenido o servicios que son legales en los Estados Unidos. El juez determinó que la libertad de expresión amparaba este comercio en su país y un tribunal extranjero no podía interferirlo.

Parece pues que los conceptos de jurisdicción y competencia no encajan bien en el Ciberespacio. No podemos pretender aplicar las normas nacionales sobre el Ciberespacio, ya que en él, por mucho que se intente, no se puede ordenar tomando como referencia las fronteras nacionales. Si se tiende a imitar la actuación francesa, corremos el peligro de que la red no vuelva a ser lo que ha sido hasta ahora, no se puede someter el Ciberespacio a la suma de las distintas legislaciones nacionales ya que, de esta forma, por ejemplo, un país islámico podría demandar a todos los sitios que vendan productos derivados del cerdo o aquellos que defiendan los derechos de los homosexuales. Si Internet se convirtiese en la suma de todas las legislaciones mundiales, si se produjesen las nefastas consecuencias que preveían los internautas de primera generación, la red se estancaría y dejaría de desarrollarse, pues es imposible tratar de hacer cumplir todas y cada una de las normas que se han desarrollado en los distintos países.

La sentencia de Yahoo! ha demostrado la dificultad de aplicar el Derecho nacional a la red, una red que sobrepasa las fronteras. Si un Estado aplica sus normas, todos los Estados tendrán derecho a imi-

tarle. *Pensar en una red multiregulada por la suma de todas las legislaciones nacionales es absurdo. Los abandonos de soberanía son buenos: dicha renuncia ha de aplicarse a la libertad de expresión. Para combatir a los propagandistas de ideas u opiniones racistas o xenóforas, Reporteros sin Fronteras y Transfert.net consideran que no sirve de nada erigir un arsenal legislativo cada vez más draconiano. La libertad de expresión es evidentemente peligrosa, pero los obstáculos a dicha libertad son más peligrosos aún. Ninguna autoridad local debe otorgarse el derecho a definir las fronteras de lo que es política o moralmente aceptable*²⁹².

Como se observa los problemas de la imposición de este tipo de modelo son importantes y variados. La eficacia de las leyes nacionales que se intentan aplicar en el Ciberespacio no es muy elevada y el problema de la jurisdicción no parece sencillo de resolver. El porqué la jurisdicción se torna en un problema tan grande dentro de los límites del Ciberespacio es algo que solo lo podemos entender dentro de los límites de la red, navegando. Ya hemos visto que el Ciberespacio es un lugar donde las fronteras no son totalmente diferentes a las del mundo real, aunque eso no quiere decir que en el mundo virtual no encontramos ninguna frontera en absoluto. La mayoría de la red es accesible a todos los usuarios de Internet, sin tener en cuenta donde puedan encontrarse. La idea de jurisdicción que nosotros tenemos relaciona perfectamente un país soberano con sus límites geográficos. El Ciberespacio desatiende estos límites totalmente. De hecho, el usuario puede acceder a docenas de sitios web de diferentes países en cuestión de segundos, sin saber, generalmente, de qué país proviene la información.

Por lo tanto, sería ilusorio aplicar el sistema jurídico de un país al conjunto de Internet, y ni siquiera se puede aplicar correctamente el sistema jurídico de un país a la parte de Ciberespacio que, en teoría, se encuentra bajo su soberanía. La escasa eficacia de la normativa nacional aplicada sobre el espacio de su soberanía no es obstáculo para los Estados, los cuales, en la mayoría de los supuestos, ya han dictado normas reguladoras del Ciberespacio. Tratar de evitar el cibercrimen, garantizar la seguridad nacional, controlar la eficacia de los

292. IRIARTE, CARLOS M. En www.chez.com/cmi

mercados electrónicos o proteger la intimidad y otros derechos fundamentales en red son los motivos básicos que respaldan la creación de normas estatales. Ya hemos visto como, en nuestro país, la regulación del comercio electrónico y de los servicios de la sociedad de la información, así como de la firma electrónica (Ley 34/2002, de 11 de Julio, de servicios de la sociedad de la información y de comercio electrónico; Ley 59/2003, de 19 de Noviembre, de Firma electrónica) ha supuesto el comienzo de la actuación nacional sobre la red.

A pesar de todo ello, es necesario observar que *regular Internet a nivel nacional puede tener sus éxitos concretos, pero no puede funcionar debido a la naturaleza global de Internet*²⁹³. Cuando hablamos del poder para gobernar el Ciberespacio, debemos entender que ningún Gobierno tiene la energía o la autoridad de gobernar el conjunto del mismo. La autoridad para gobernar el conjunto de la red se puede ejercitar solamente en una escala global, porque solamente en una escala global tal poder existe. Si un país desea gobernar Internet, debe aceptar que no puede procurar aplicar sus reglas al conjunto del mismo, y que la eficacia de las normas que cree va a estar limitada por la supra-territorialidad que impera en la red. Los nacionales de cualquier país fácilmente escapan a las normas soberanas impuestas por su Estado mediante el acceso a la red a través de proveedores extranjeros.

Todo lo anteriormente señalado nos muestra como en ningún caso vamos a asistir a una regulación nacional, de Internet. Las propias características de la red de redes, su complejidad, sus enormes posibilidades, el hecho indudable de que actúa en muchos países con distintas legislaciones, culturas, necesidades, dará lugar a una regulación también plural, compleja y en permanente desarrollo, que sugestivamente compara MUÑOZ MACHADO como una estructura de malla, con la misma *imagen física de la gran telaraña que trata de ordenarse*²⁹⁴. En esta malla regulatoria son muy diversas las entidades que tendrán un destacado papel. El Estado, ya lo hemos visto, tendrá un papel sin duda fundamental y particularmente difícil, en la búsqueda de un equilibrio entre regulación necesaria y justa en cada momento y el exceso sobrerregulatorio. Pero no será el único.

293. HICKS, B.D., *Choice of law issues in cyberspace*, op. cit.

294. MUÑOZ MACHADO, S., *La regulación de la red*, op. cit., p. 41.

A pesar de todos los inconvenientes señalados, es importante determinar cómo, conforme avanzan los días, la posibilidad de regular Internet desde la soberanía nacional va teniendo más esperanzas de eficacia. La globalidad de Internet, su ingobernabilidad y su inmunidad al control de la soberanía de los Estados está empezando a convertirse en un sueño lejano.

III.2. LEGISLACIÓN UNIVERSAL

Si lo analizásemos exclusivamente desde el punto de vista del deber ser, es obvio que la solución más acertada para ordenar Internet pasaría por el establecimiento de una legislación única y universal, válida en todos los países del mundo que permitan o posean acceso a Internet²⁹⁵. Sin embargo, desde el plano del ser no pasa inadvertido que regular de forma unitaria Internet es complicado, por no decir imposible, pues supondría unificar todos los criterios legales de los países en una sola legislación o marco legal.

Según la mayoría de la doctrina, deberíamos buscar un núcleo duro de Derecho que fuese común a todos los países. Por lo tanto, el primer paso sería hallar el mínimo común denominador de todas las legislaciones a fin de, sobre la base de este resultado, comenzar a construir una legislación adecuada para el Ciberespacio donde se recoja la normativa básica y comúnmente aceptada por todas las naciones que pueblan la tierra.

Algunos autores mantienen que *es necesario trabajar para alcanzar un consenso mundial sobre las medias legislativas necesarias para la armonización de determinados aspectos de Internet, prohibiendo el comportamiento injusto sin imponer ningún tipo de comportamiento, pues debe prevalecer la libertad de expresión y de contenidos frente a*

295. En el año 2002 Corea del Norte era el único país del mundo donde no existía Internet. No había ni servidor ni posibilidad de conexión. En la actualidad existen limitadas conexiones, las cuales vienen de conexiones satélites provistas por empresas de Corea del Sur y por líneas terrestres de China. Asimismo, cuentan con pocos sitios webs (la mayoría casinos on line)

*cualquier intento de regular y controlar, pero partiendo del principio básico de que no puede permitirse en la red lo que está prohibido en la calle, por lo que los Estados Miembros deben aplicar la legislación existente que pueda sancionar esas conductas ilícitas*²⁹⁶. Esta solución parece eficaz y factible, no obstante adolece de un gran inconveniente: ¿Quién decide que comportamientos son injustos? ¿Qué se entiende exactamente con lo prohibido en la calle? ¿Prohibido por qué países? Esta perfecta, pero a la par ilusoria solución, materializa un gran problema pues si hay tantas legislaciones como Estados, es utópico tratar de encontrar un consenso acerca de las conductas que son injustas, y aun más en las conductas que son ilícitas. No hay que investigar demasiado para observar que lo que es ilícito en un país, en el vecino puede estar absolutamente permitido. En ese caso, ¿cuál de las normativas ha prevalecer sobre las demás? ¿Acudiremos nuevamente a la ley del más fuerte, a la ley de los países que dominan geográfica y económicamente el Ciberespacio? NO-LOUIS CABALLERO indica que *no podemos hacer más que confiar en la leal colaboración de los pueblos, Gobiernos y Estados, en el sentido de mantener siempre los ideales de Libertad, Igualdad, Justicia y Solidaridad que conforman nuestras vidas, para poder encontrar soluciones armónicas, coherentes y proporcionales*²⁹⁷.

El director del Master sobre Internet en Santiago de Compostela T. DE PASERVAL, no deja lugar a la duda sobre el fracaso de una regulación universal de Internet, según este autor, la idea parece un imposible a estas alturas de desarrollo legislativo. Este autor afirma que *la idea de legislar globalmente Internet será una utopía durante mucho tiempo. Es muy difícil regular Internet, sobre todo por el problema de la globalización. Las legislaciones de los distintos países o culturas constituyen unos marcos jurídicos basados en unas mentalidades, en unos fondos de pensamiento muy contrapuestos. Estos aspectos son los que constituyen el verdadero handicap para llegar a contar con*

296. CARRASCOSA LÓPEZ, V. “¿Es necesaria una legislación mundial para Internet?”, *op. cit.*, p. 176.

297. NO-LOUIS Y CABALLERO, E., “Internet, germen de la sociedad de la información”, XV años de encuentros sobre Informática y Derecho, (1987-2002) DAVARA RODRÍGUEZ, M. A.(Coordinador), Universidad Pontificia Comillas de Madrid, Facultad de Derecho, Instituto de Informática Jurídica, Madrid, 2002, p. 372.

una ley de Internet a nivel global (...) Hay muchas trabas todavía para que la legislación se aplique porque Internet no tiene fronteras. Ahora es imposible regular Internet, igual dentro de 30 años hay un consenso para llegar a unos acuerdos que permitan un libre mercado absoluto dentro del mundo de las nuevas tecnologías e igual si es posible llegar a un acuerdo, esa regulación constituye una autentica utopía²⁹⁸. La misma opinión es compartida por MUÑOZ MACHADO cuando afirma que la solución más simple es la universalización. Si una nueva ley ha de regir en el mundo entero, que la dicte una autoridad mundial. La armonización implica que exista una única norma a escala regional o universal. Pero ello es imposible. Los Estados no lo permitirán y no es necesario²⁹⁹.

Lógicamente, este modelo de regulación exigiría la constitución de una Organización Internacional-Mundial cuya función fuese la de gobernar y legislar, de manera exclusiva y excluyente, la Red de redes. Desde este punto de vista, la Organización Internacional tendría competencia absoluta e ilimitada para tomar cualquier decisión relacionada con Internet. Una Organización similar requiere la participación de la totalidad de los países del globo y el acuerdo general de todos ellos en la construcción y organización de tal entidad, lo cual, de momento, parece imposible. En este sentido POST establece que *es difícil establecer cómo una organización internacional va a gobernar la red y a imponer sus normas a países que no forman parte de ella porque no la han aceptado. En ese caso es muy dudoso el derecho que asiste a esta organización para imponer sus normas. Muchas son las dudas que esta alternativa presenta, por las cuales varios autores rechazan la posibilidad de llevarla a la práctica³⁰⁰*. Para otros autores, este problema se resolvería desde *el momento en que la Organización Internacional obtenga el acuerdo general sustancial de la mayoría de los países del mundo³⁰¹*. En este sentido el problema de la representatividad mundial de la Organización se resolvería mediante la crea-

298. DE PASERVAL, T., en *El Correo Gallego*, Miércoles 28 de Noviembre de 2001.

299. MUÑOZ MACHADO, S., entrevista en *Ciberp@is semanal*, 18 de Enero de 2001, p. 17.

300. POST, D.G., *Anarchy, State and the Internet: an essay on law-making in cyberspace*, 1995, on line: www.wm.edu/law/publications/jol/articles/post.shtml

301. HICKS, B.D., *Choice of law issues in cyberspace*, op. cit.

ción de la misma de forma apropiada: mediante un tratado multilateral en el que participan un número sustancial de países.

Si creamos una *Organización Internacional verdaderamente representativa para tratar de resolver los problemas que han surgido en la red, su contribución a la gobernación del Ciberespacio será importante*³⁰². Esto es cierto, no obstante, el problema radica en determinar qué consideramos por un apoyo sustancial de la mayoría de los países del mundo. En este supuesto correremos el mismo peligro que hemos designado a lo largo de todo el análisis del Ciberespacio. En el mundo real unos países cuentan más que otros, por lo que parece presumible que la creación de una Organización Internacional plasme la realidad del mundo físico. ¿Qué vamos a entender por un número sustancial de países? ¿Daremos por satisfecho este requisito cuando los países ricos manifiesten su apoyo? ¿Olvidaremos nuevamente que Internet es mundial y, por lo tanto, todos los países del mundo deberían tener voz y voto?

El mismo autor reconoce que el problema más grande es, sin ninguna duda, las diferencias ideológicas existentes entre los países. *Pueden tomarse los Estados Unidos y China como ejemplo. Considerando que los Estados Unidos creen en la libertad de expresión, China cree en la regulación de ideas e información. Con estos dos puntos de vista tan dispares parece casi imposible el que pongan de acuerdo en la creación de una Organización Internacional que regule la red. La Organización Internacional sólo debe fijar las normas mínimas -aun siendo en determinados aspectos de carácter detallista-. Se debe considerar la posibilidad de permitir a los países tener autoridad para intentar regular aspectos más concretos y no tan generales en su propio país. Por ejemplo, si el país soberano específico quiere prohibir la pornografía en total, él debe tener derecho para intentar regularlo*³⁰³. Para HICKS, uno de los principales inconvenientes de la regulación del Ciberespacio mediante Tratados Internacionales se encuentra en que éstos no pueden regular los pequeños detalles de Internet, ya que no podían responder a la rápida evolución tecnológica que impone Internet. Pues bien, el instrumento ideal para regular en detalle el Ciberespacio es, para este autor, las normas emanadas del Organismo

302. *Ibíd.*

303. *Ibíd.*

Internacional encargado de gobernar la red. Afirma, *creo que el establecimiento de una organización internacional es la respuesta a los problemas de los tratados multilaterales. Si podemos crear una organización internacional que sea aceptada por la mayoría de Estados en el mundo, puede regular más detalladamente las decisiones que afecten a Internet. Tal organización puede abordar y contestar rápidamente un nuevo problema acuciante, y puede hacerla cumplir las reglas porque tiene la autoridad que le han cedido los Estados soberanos*³⁰⁴.

Obviamente nos encontramos con grandes dificultades, ya que la elaboración de una legislación única y la creación de un Organismo Internacional-Mundial consensuado se muestran, de momento, como improbables. Además estos impedimentos aumentan desde el momento en que la falta de normativa mundial sobre determinados aspectos de Internet no es la excepción sino la regla general. Los problemas que se presentan en la red y que, por lo tanto, hay que resolver son mundiales, mientras que los mecanismos de solución están disgregados y descentralizados entre los diferentes países. Hoy por hoy resulta bastante utópico hacer realidad las soluciones que el Ciberespacio está demandando: un marco jurídico y policial mundial. Así las cosas, al menos a corto y medio plazo, el procedimiento alternativo más factible discurre por la vía de progresivos acuerdos entre los distintos Estados en los foros internacionales.

III.3. SOBERANÍA COMPARTIDA: TRATADOS INTERNACIONALES

De momento, y hasta que la elaboración de una legislación universal para la red y la creación de un Organismo Mundial superen la situación utópica actual, la forma más efectiva de regular la red implica el ejercicio de la soberanía compartida por parte de los Estados nacionales, mediante la elaboración de Tratados Internacionales que incidan sobre la ordenación parcial del Ciberespacio. Para muchos autores el Tratado Internacional es el mejor camino a seguir, por lo menos de momento. *El impacto mundial propio de las actividades en Internet y el alcance global de este medio, justifican la búsqueda de la coordinación internacio-*

304. *Ibíd.*

*nal, habida cuenta también de las limitaciones de los distintos Estados para garantizar la efectividad de ciertas sanciones relativas a las actividades que se desarrollan en el Ciberespacio*³⁰⁵.

Cuando los Gobiernos del mundo conocieron por fin el Ciberespacio, éste había evolucionado en magnitud y velocidad, así los Estados soberanos tenían que concretar ágilmente una estrategia de actuación. Se enfrentaron con algo que influenciaba nuestras vidas diarias y que, todavía estaba totalmente desreglado. Ésta debió ser la razón por la que los países se lanzaron a la aprobación de leyes nacionales para aplicarlas en el Ciberespacio. Pero ¿sería posible regular Internet por vía de un Tratado Multilateral? Y en ese caso, ¿ésta sería la ruta mejor para seguir? Firmar un tratado internacional parece la solución más sencilla para el Ciberespacio, sin embargo, también aquí se encuentran objeciones.

HICKS reconoce limitaciones a la labor de regulación de los Tratados Internacionales. Establece que *un Tratado Multilateral puede ser apropiado para colocar las reglas más fundamentales del Ciberespacio, como declararlo un espacio separado, similar a alta mar o al espacio exterior. Sin embargo, un tratado multilateral no puede convertirse en la herramienta apropiada a utilizar si deseamos colocar las reglas específicas detalladas del Ciberespacio. La razón hay que buscarla en que Internet en sí mismo está cambiando de un modo tan veloz que los mecanismos de modificación del Tratado o Tratados no podrían adaptarse a las nuevas necesidades*³⁰⁶.

LITAN Y NISKANEN determinan que *en algunos casos, puede ser necesaria la armonización de las normativas. Sin embargo, en muchas otras ocasiones, puede que alcanzar un consenso no sea ni deseable ni posible, considerando las claras diferencias que existen entre las actitudes sociales y políticas de los diferentes países y dentro de los Estados que conforman los Estados Unidos. En tales situaciones debe aspirarse a lograr un reconocimiento mutuo, a que las jurisdicciones se comprometan a respetar las normas de los demás*³⁰⁷.

305. MIGUEL ASENSIO, P. de, *Derecho privado de Internet*, op. cit., p. 24.

306. HICKS, B.D., *Choice of law issues in cyberspace*, op. cit.

307. LITAN, R. E. & NISKANEN, W. A., *El horizonte digital, manual de directrices para la era digital*, op. cit, p. 5.

Se analizó como los Estados aislados no pueden aplicar su poder individual sobre la red de modo efectivo. Es difícil que los Estados controlen la red de modo eficaz como si fuera parte de su territorio debido al carácter global del Ciberespacio. Por ello, la única opción válida y eficaz que existe en la actualidad, una vez descartada la viabilidad de una legislación universal, conlleva un esfuerzo concertado por parte de los Estados soberanos para actuar conjuntamente y crear un espacio nuevo y global de acción policial. *Como declaró el G 8 en su reunión de Washington de diciembre de 1997, es imposible para un país acabar con la delincuencia producida o distribuida por la red, por lo que se recomienda la cooperación internacional para actuar con eficacia en ese terreno*³⁰⁸. Al hacerlo perdieron soberanía, ya que se vieron obligados a renunciar a una parte de la misma para crear un organismo de soberanía compartida. *La soberanía compartida ha sido el precio que han tenido que pagar los Estados para retener, de modo colectivo, algún grado de control político*³⁰⁹.

La dimensión internacional de Internet, combinada con el desafío de la globalización, parece demandar una cooperación internacional adecuada, para evitar que la descentralización de los servidores vacíe de contenido las normativas nacionales. Por lo tanto, condicionada por la necesidad de adaptación al carácter transfronterizo y global de Internet, se refuerza la necesidad de cooperación internacional, en la que cada vez van adquiriendo mayor protagonismo las organizaciones intergubernamentales. Es necesario implementar mecanismos de cooperación transnacional para garantizar la efectividad de las legislaciones nacionales sobre el Ciberespacio, aunque sea mínimamente. *Los Estados que se rebelen contra esta alternativa y decidan no ceder ni un ápice de su soberanía devendrán más frágiles e inseguros en la red. No hay duda de que cuanto más se resiste un Estado a limitar su soberanía a favor de la internacional, más vulnerable se vuelve a los ciberataques*³¹⁰.

Vemos pues como se refuerza la necesidad de coordinación internacional en el Ciberespacio para superar la inseguridad jurídica existente. No obstante, cuando se analizan los Tratados Internacionales

308. VALLÉS COPEIRO DEL VILLAR, A., "Desafíos éticos de las nuevas tecnologías", *op. cit.*, p. 51.

309. CASTELLS, M., *La galaxia Internet*, *op. cit.*, p. 203.

310. *Ibíd.*, p. 204

aplicables a determinados ámbitos de la red, observamos que la heterogeneidad de los sistemas jurídicos que coexisten en el mundo suele restringir a determinados círculos de Estados la posibilidad de unificar sus normas de modo vinculante. Si bien la uniformización jurídica en círculos limitados de países suele alcanzar resultados mucho más efectivos, especialmente en el marco de integración política tan intenso como el europeo, el alcance global de Internet justifica también la participación estatal en foros de ámbito mundial.

Efectivamente, en el ámbito de la Unión Europea el desarrollo de la normativa ordenadora de la Red de redes ha empezado hace algún tiempo y parece, no obstante, imparable. A través de la normativa europea se están estableciendo unos criterios mínimos sobre contenidos y otros aspectos de Internet. Así, y tras la reglamentación en el ámbito europeo, los distintos Estados miembros han ido desarrollando normas internas que han servido para adaptar, en el ámbito nacional e interior, las directrices establecidas por las Directivas y demás normas comunitarias. Con ello se ha alcanzado un sistema más o menos homogéneo de regulación y protección de derechos y garantías sobre algunos aspectos específicos de la Red. La Directiva 2000/31/CE relativa a la regulación del comercio electrónico, *que pretende armonizar las disposiciones normativas de los miembros en relación con los servicios de la sociedad de información dentro del mercado interior*, supuso el estreno más contundente de una gran actividad productora de normas. Posteriormente se publicó la Directiva 2001/29/CE *relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información*. Asimismo, tras un largo proceso de tramitación, el 12 de Julio de 2002 se adoptó la Directiva 2002/58/CE del Parlamento y del Consejo, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones*³¹¹.

La seguridad en la red es una objetivo primordial para la Unión Europea, así nos encontramos, entre otras, con la Resolución del Consejo de 18 de Febrero de 2003 *sobre un enfoque europeo orientado hacia una cultura de seguridad de las redes y de la información*; Decisión nº 1151/2003/CE del Parlamento Europeo y del Consejo, de 16

311. Disponible on line: www.aepsi.org/documentos

de Junio de 2003, que modifica la Decisión nº 276/1999/CE *por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales*. Recientemente se ha aprobado el Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de Marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información. De la misma forma son destacables, entre otras, en el ámbito comunitario, la Directiva 2002/19/CE del Parlamento y del Consejo, de 7 de Marzo, *relativa al acceso a redes de comunicación electrónica y recursos asociados, y a su interconexión*; la Directiva 2002/20/CE del Parlamento y del Consejo, de 7 de Marzo, *relativa a la autorización de redes y servicios de comunicaciones electrónicas*, la Directiva 2002/21/CE del Parlamento y del Consejo, de 7 de Marzo, *relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas*; la Directiva 2002/22/CE del Parlamento y del Consejo, de 7 de Marzo, *relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicación electrónica* y la Directiva 2002/77/CE de la Comisión, de 16 de Septiembre, *relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas*.

La Unión Europea, de la misma forma, procedió a incrementar la confianza en Internet y a impulsar el desarrollo de la sociedad de la información a través de la iniciativa eEurope: *Una sociedad de la información para todos*. E-Europe es una iniciativa política dirigida a asegurar que la Unión Europea obtenga el máximo provecho de los cambios que está produciendo la sociedad de la información. Esta iniciativa se plasmó inicialmente en el plan eEurope 2002³¹², completada y renovada por el plan eEurope 2005³¹³ y por el marco i2010³¹⁴. Asimismo, el

312. *Comunicación de la Comisión de 13 de marzo de 2001: eEurope 2002: Impacto y prioridades Comunicación al Consejo Europeo de primavera de Estocolmo del 23 y 24 de marzo de 2001 [COM (2001) 140 final - no publicada en el Diario Oficial]*

313. *Comunicación de la Comisión al Consejo de 28 de mayo de 2002: eEurope 2005: Una sociedad de la información para todos [COM (2002) 263 final - no publicada en el Diario Oficial].*

314. *Comunicación de la Comisión de 1 de junio de 2005: i2010 - Una sociedad de la información europea para el crecimiento y el empleo [COM (2005) 229 final - no publicada en el Diario Oficial].*

plan de acción *Safer Internet*³¹⁵ (199-2005) y el programa *Safer Internet Plus*³¹⁶ (2005-2008) establecen mecanismos que garanticen un empleo seguro de Internet. Mediante todos ellos se ha pretendido acrecentar, complementar y asegurar el marco regulatorio de Internet.

La iniciativa eEurope fue lanzada el 08 de diciembre de 1999 con la adopción por parte de la Comisión de la Comunicación “eEurope - una sociedad de la Información para todos” (Comisión Europea 1999). El Consejo Europeo ha respaldado el Plan de Acción Global eEurope 2002. El Consejo Europeo fijó como objetivo convertir a Europa en la economía más competitiva y dinámica del mundo y ha convertido las cuestiones relativas a la Sociedad de la Información y a la nueva economía en una de las prioridades de las instituciones comunitarias. Aprobado por el Consejo Europeo en Sevilla en Junio de 2002, eEurope 2005 se inscribe en la estrategia de Lisboa encaminada a convertir a la Unión Europea en una economía basada en el conocimiento, más competitiva y dinámica, con avances en materia de empleo y de cohesión social, para el 2010³¹⁷. Este plan propone básicamente:

315. *Decisión n° 276/1999/CE del Parlamento Europeo y del Consejo, de 25 de enero de 1999, por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. Prorrogado hasta el 2005 por la Decisión n° 1151/2003/CE del Parlamento Europeo y del Consejo, de 16 de junio de 2003, que modifica la Decisión n° 276/1999/CE por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales.*

316. *Decisión n° 854/2005/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, por la que se crea un programa comunitario plurianual para el fomento de un uso más seguro de Internet y las nuevas tecnologías en línea.*

317. *Las conclusiones del Consejo Europeo de la Unión celebrado en Lisboa en Marzo de 2000 establecían, como requisitos necesarios para la preparación del paso a una economía competitiva, dinámica y basada en el conocimiento, el que las empresas y los ciudadanos tuvieran acceso a una infraestructura de comunicaciones mundial, barata y con ello a un amplio abanico de servicios. Igualmente se ponía de manifiesto que todo ciudadano debería poseer los conocimientos necesarios para vivir y trabajar en la nueva sociedad de la información, evitando toda exclusión y reforzándose la lucha contra el analfabetismo y restando atención especial a las personas discapacitadas. Se señalaba finalmente que las tecnologías de la información habrían de utilizarse ►*

camente estimular el desarrollo de servicios, aplicaciones y contenidos, acelerando al mismo tiempo la implantación de un acceso a Internet de banda ancha y seguro. Por su parte, i2010 es el nuevo marco estratégico de la Comisión Europea por el que se determinan las orientaciones políticas generales de la sociedad de la información y los medios de comunicación. Esta nueva política integrada se propone, en particular, fomentar el conocimiento y la innovación al objeto de fomentar el crecimiento y la creación de empleo, tanto cualitativa como cuantitativamente. Asimismo, se inscribe en el marco de la revisión de la estrategia de Lisboa.

El plan de acción de 2002 introdujo tres objetivos principales. En primer lugar se pretende lograr una red de Internet rápida, barata y segura. Desde la liberalización de los servicios de telecomunicaciones, el 1 de enero de 1999, las tarifas de las llamadas internacionales y de larga distancia han disminuido considerablemente. Sin embargo, la mayoría de los consumidores acceden a Internet a través de las líneas locales, donde los precios han bajado mucho menos, debido a la falta de competencia. Hasta ahora, el mercado, por sí mismo, ha sido relativamente lento a la hora de ofrecer nuevos sistemas de tarifas, como la cuota única o el acceso gratuito. La existencia de precios bajos es especialmente importante para una rápida asimilación del acceso multimedia a Internet de alta velocidad que permiten las nue-

317. para renovar el desarrollo urbano y regional y fomentar tecnologías seguras para el medio ambiente, siendo esencial para cumplir tales objetivos la creación de condiciones para que prosperasen adecuadamente el comercio electrónico e Internet, exigiendo todo ello planteamientos normativos nuevos y más flexibles en el futuro. Para la consecución de tales objetivos resulta necesario tener en cuenta en primer término la denominada convergencia de los distintos servicios e infraestructuras de telecomunicaciones y medios audiovisuales, en cuanto en particular las posibilidades de interactividad que ofrece Internet están determinando un interés creciente de las empresas audiovisuales para su utilización conjunta con los medios de comunicación; como la televisión. La posible combinación de televisión e Internet está llevando a los distintos operadores a ofrecer servicios de televisión interactiva y de valor añadido con la información que hay en Internet, siendo previsible en un futuro próximo la convergencia entre los PC informáticos y la televisión, que hará de los televisores dispositivos de acceso y proceso de información y a los ordenadores personales instrumentos capaces de integrar todo tipo de información y también de contenidos de televisión.

vas tecnologías, como la xDSL³¹⁸, el cable, la fibra óptica, la televisión digital y las tecnologías de radio. Asimismo, la seguridad en las redes es esencial, las redes seguras y el acceso seguro mediante tarjetas inteligentes son aspectos vitales para crear confianza entre los usuarios en el ámbito del comercio electrónico.

En segundo lugar el plan perseguía realizar una inversión en capital humano y en su formación. En tercer lugar se trabajaba en el estímulo para el uso de Internet³¹⁹ mediante la aceleración del comercio electrónico, el desarrollo de la Administración y la sanidad en línea, la elaboración de contenidos digitales exportables a las redes mundiales y el desarrollo de sistemas de transporte inteligentes que solucionen tres problemas básicos del transporte clásico: la saturación, la seguridad y la escasez de nuevos servicios.

Componen este marco regulatorio numerosas iniciativas de la Comisión que afectan a distintos aspectos de la vida de Internet tales como decisiones sobre la liberalización definitiva de las telecomunicaciones, la introducción de un dominio general de alto nivel “.eu”³²⁰, el

318. *X Digital Subscriber Line, líneas de suscripción digital, tecnología de transmisión que permite que los hilos de cobre convencionales transporten hasta 16 Mbps (megabits por segundo) mediante técnicas de compresión. Hay diversas modalidades, siendo actualmente la más empleada el ADSL.*

319. *FERNÁNDEZ ESTEBAN, M. L., “Internet y los derechos fundamentales”, op. cit., p. 96.*

320. *Después de la exitosa conclusión de las negociaciones con ICANN (Internet Corporation for Assigned Names and Numbers) en marzo de 2005 para la introducción del country-code top level domain “.eu”, los registros abiertos bajo esta denominación son un hecho desde el 7 de Abril del 2006. La creación de la extensión .eu marca el reconocimiento de una identidad europea en Internet, asimismo es un medio efectivo para luchar con el dominio de los Estados Unidos en la red. Aunque la idea de un dominio europeo empieza a gestarse en julio de 2000 en el Parlamento Europeo, el primer paso para su creación no se da hasta el 22 de marzo de 2002 con la adopción del Reglamento 733/2002, que define las grandes líneas del .eu. En mayo de 2003, el Parlamento Europeo elige, entre siete candidatos, al consorcio belga-italo-sueco EURid para hacerse cargo de la gestión del dominio .eu. Un año más tarde, mientras EURid se preparaba para asumir este papel, el Parlamento Europeo aprobó el Reglamento 874/2004, que marca las principales pautas de la normativa de los dominios ►►*

estímulo de contenidos multimedia europeos y la educación a través de las nuevas tecnologías, la protección de los derechos de propiedad intelectual en la red, la lucha contra la delincuencia en el Ciberespacio, la regulación de los contenidos en Internet, la regulación del comercio electrónico, la protección de datos personales y de la intimidad en las comunicaciones electrónicas, la nueva regulación de la encriptación y la firma electrónica.

Existen tres métodos principales mediante los cuales se plantearon el logro de los objetivos de e-Europe 2002. En primer lugar mediante la aceleración de la creación de un entorno legislativo adecuado. En el ámbito europeo, se está preparando y discutiendo una amplia gama de propuestas legislativas. E-Europe tiene previsto acelerar su aprobación estableciendo plazos fijos para todos los afectados. En segundo lugar, se buscaba apoyar nuevas infraestructuras y servicios en toda Europa. La evolución en este terreno depende principalmente de la financiación del sector privado. Esta actividad puede apoyarse mediante financiación comunitaria, aunque su éxito dependerá en buena parte de las actuaciones de los Estados Miembros. Evidentemente, esta actuación no debe poner en peligro la disciplina presupuestaria. Por último, aplicar el método abierto de coordinación y evaluación comparativa. Este método tiene por objeto asegurar que estas acciones se lleven a cabo de manera eficiente, consigan el efecto deseado y tengan la fuerte incidencia necesaria en todos los Estados Miembros.

Los logros del mencionado plan, así como los obstáculos que siguen entorpeciendo el pleno desarrollo de la Sociedad de la Información en Europa, son detallados en el Informe final eEurope 2002/Comunicación al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones de Febrero de 2003³²¹. El informe establece dos conclusiones significativas. En primer lugar se detecta que la conexión

320. europeos: *www.arsys.es*. EURid cuenta con un sistema propio de resolución de controversias para los dominios .eu, que se conoce por ADR (Alternative Dispute Resolution), se trata de normativa similar a la política ICANN de UDRP (Uniform Domain Name Dispute Resolution Policy). El órgano encargado de llevarlos a cabo es la Corte de Arbitraje checa con sede en Praga: <http://www.adr.eu/index.php>

321. COM (2003) 66 final. On line:

http://europa.eu.int/eur-lex/es/com/cnc/2003/com2003_0066es01.pdf

a Internet ha crecido rápidamente. Cuando se lanzó eEurope 2002, pocos podían acceder a Internet. En 2002, más del 90% de las escuelas y empresas están en línea y más de la mitad de los europeos son usuarios habituales. Europa cuenta con la red central de investigación más rápida del mundo. La amplia extensión de las conexiones de alta velocidad en los hogares y las PYME será el próximo reto. Aun así, siguen existiendo diferencias significativas entre los Estados miembros en lo que respecta a las conexiones. En segundo lugar, se ha acordado un marco legislativo para las comunicaciones electrónicas y el comercio electrónico. La legislación sobre las telecomunicaciones se ha concebido para reforzar la competencia en el mercado y, en consecuencia, reducir los precios y fomentar la innovación. Los precios han disminuido y la competencia ha aumentado. En cuanto al comercio electrónico, se ha adoptado una serie de directivas para mejorar la seguridad de transacciones electrónicas, especialmente en el comercio transfronterizo, y para garantizar una adecuada protección del consumidor.

Por su parte, el Plan de Acción eEurope 2005³²², que continúa con la labor de su predecesor, pretende crear un marco favorable a la inversión privada y a la creación de nuevos puestos de trabajo, impulsar la productividad, modernizar los servicios públicos y ofrecer a todos la posibilidad de participar en la sociedad de la información mundial, logrando una utilización más eficiente de Internet. E-Europe 2005 trata, pues, de fomentar la seguridad de los servicios, aplicaciones y contenidos basados en una infraestructura de banda ancha ampliamente disponible. En el mismo marco nos encontramos con la Decisión n° 2256/2003/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, por la que se adopta un programa plurianual (2003-2005) *para el seguimiento del plan de acción eEurope 2005, la difusión de las buenas prácticas y la mejora de la seguridad de las redes y la información*.

El citado plan de acción se estructura en dos grupos que se refuerzan mutuamente. Por una parte, pretende fomentar los servicios, aplicaciones y contenidos, incluyendo tanto los servicios públicos en línea como los negocios electrónicos; por otra, aborda la infraestructura de banda ancha subyacente y las cuestiones relativas a la seguridad. El plan incluye cuatro instrumentos independientes, aunque interrelacionados.

322. Bruselas, 28- Mayo- 2002; COM(2002) 263 final.

En primer lugar, medidas políticas encaminadas a revisar y adaptar la legislación a nivel nacional y europeo, garantizar que la legislación no obstaculice innecesariamente los nuevos servicios, reforzar la competencia y la interoperabilidad, mejorar el acceso a diversas redes y hacer gala de iniciativa política. E-Europe 2005 enumera las áreas en que la política pública puede aportar un valor añadido y, por consiguiente, se centra en un conjunto limitado de acciones en las áreas prioritarias. En segundo lugar, eEurope facilitará el intercambio de experiencias, buenas prácticas y proyectos de demostración, pero permitirá igualmente compartir las enseñanzas extraídas de los fracasos. Se ejecutarán proyectos encaminados a acelerar la instalación de aplicaciones e infraestructuras de vanguardia. En tercer lugar, será posible efectuar un seguimiento de las medidas políticas y reencauzarlas en su caso a través de una evaluación comparativa de los progresos realizados en el cumplimiento de los objetivos y de las políticas al servicio de dichos objetivos. Por último, una coordinación general de las políticas existentes permitirá crear sinergias entre las acciones propuestas. Un grupo de dirección se encargará de facilitar una panorámica de la evolución de la política y garantizar un buen intercambio de información entre los responsables nacionales y europeos y el sector privado. Este grupo hará posible igualmente la participación de los países candidatos desde los primeros momentos.

El plan de acción 2005 constituye una propuesta para que los Estados Miembros asuman algunos compromisos de amplio alcance. Constituye asimismo una invitación al sector privado para que colabore con la Comisión y los Estados Miembros en el logro de los objetivos de eEurope. En él se exponen las iniciativas que la Comisión adoptará o desea adoptar. Considerado globalmente, el plan sienta las bases de un enfoque coordinado de la política europea en relación con la sociedad de la información. De tener éxito, este plan tendrá importantes repercusiones sobre el crecimiento y la productividad, sobre el empleo y la cohesión social en Europa³²³.

323. *En el marco de la actividad legislativa de la Unión Europea se pretende que la Comisión, en cooperación con los Estados Miembros, pasará revista a la legislación pertinente, cuando proceda, con el objetivo de detectar y suprimir los factores que impiden a las empresas la realización de negocios electrónicos. El objetivo del ejercicio será, especialmente, extender la actual normativa favorable al comercio electrónico al suministro fuera de línea de bienes y servicios, con el fin de situar los diferentes modos de intercambio (en línea y fuera de línea) en igualdad de condiciones.*

Finalmente con i2010, la Unión Europea aborda de manera integrada la sociedad de la información y las políticas audiovisuales. Su propósito es coordinar la acción de los Estados miembros para facilitar la convergencia digital y afrontar los desafíos vinculados a la sociedad de la información. Para elaborar este marco estratégico, la Comisión ha llevado a cabo una amplia consulta con los agentes en torno a iniciativas e instrumentos anteriores, tales como eEurope y la Comunicación sobre el futuro de la política reguladora europea en el sector audiovisual. En el terreno de las políticas europeas de la sociedad de la información y los medios de comunicación, la Comisión propone tres prioridades que deben cumplirse antes de 2010: la consecución de un espacio europeo único de la información, el refuerzo de la innovación y de la inversión en el campo de la investigación en las tecnologías de la información y la comunicación (TIC), y la consecución de una sociedad de la información y los medios de comunicación basada en la inclusión.

Con estos ejemplos europeos se comprueba la viabilidad de la regulación de algunos aspectos o problemas concretos de la red Internet en un número relativamente elevado de países, aunque cultural y jurídicamente homogéneos. La experiencia europea debe servir, al menos, como un punto de partida para una reflexión acerca de la creación, de momento utópica, de una legislación única y global para la Red de las redes. Queda comprobado como la cooperación en el ámbito de la Unión Europea referida a Internet es numerosa y eficaz, no obstante, esta cooperación no se ciñe exclusivamente al mencionado ámbito sino que se desarrolla asimismo, de manera constante, en el ámbito internacional.

Se ha mencionado como en Diciembre de 1997, durante una cumbre del G-8 en Washington, se determinó que *es imposible que un país actúe solo, por lo que es necesario tener en cuenta las vías de cooperación internacional*³²⁴. A pesar de ello, no fue hasta la cumbre del G-8 celebrada en París en Mayo de 2000 por iniciativa de Francia y de Japón, cuando las intenciones de este grupo de países se plasmaron en respuestas prácticas contundentes y eficaces. En esta cumbre se estableció que era suficiente la cooperación internacional para

324. MUÑOZ MACHADO, S., *La regulación de la red, op. cit., p. 153.*

regular la red, a través de la cooperación de los distintos Estados soberanos. De modo efectivo, ésta fue la primera vez que los representantes de los países afectados abordaron este problema en una instancia multilateral, en la que afloraron las diferencias entre los proyectos de sociedad a ambos lados del Atlántico. En esta misma cumbre se rechazó la idea propuesta por los Estados Unidos de crear una policía común del Ciberespacio.

El Consejo de Europa pronto secundó esta dirección de cooperación internacional promoviendo una convención contra los crímenes y delitos cometidos a través de la red o contra la red, que quedó plasmada en la primera Convención Internacional sobre el Cibercrimen³²⁵. Este Convenio supone el resultado de cuatro años de trabajo por parte del Consejo de Europa, juntamente con los Estados Unidos, Canadá, Japón y Sudáfrica. Su aprobación estaba programada para Diciembre de 2000, aunque no fue hasta el 23 de Noviembre de 2001 cuando, durante una reunión extraordinaria del Organismo en Budapest, la primera Convención Internacional sobre Cibercrimen quedó abierta a la firma. El Tratado fue aprobado por el Comité de Ministros del Consejo de Europa el 8 de Noviembre de 2001 en Estrasburgo, presentándose a la firma de los Estados en la mencionada conferencia extraordinaria de Budapest. Finalmente esta Convención ha entrado en vigor el día 1 de Julio de 2004, al ser ratificada por cinco países, tres de los cuales tenían que ser Estados miembros del Consejo de Europa³²⁶. Después de más de treinta borradores del Convenio, y de cuatro años de discusiones infructuosas sobre su contenido, resulta interesante que el consenso necesario para su aprobación tuviese lugar inmediatamente después de los actos terroristas del 11 de Septiembre. Hecho que pone de manifiesto el poder y control que los Estados Unidos ejercen sobre el Ciberespacio.

325. *El texto íntegro de este Convenio puede ser consultado en la siguiente página Web: www.agpd.es*

326. *Con la intención de promover el cumplimiento del Convenio contra el Cibercrimen, el Consejo de Europa ha celebrado en Estrasburgo, durante los días 15 a 17 de Septiembre de 2004, una conferencia sobre el Cibercrimen en la que han participado 180 políticos de diferentes gobiernos y expertos del sector privado en el ámbito mundial. El principal objetivo de esta conferencia ha sido aunar esfuerzos para la lucha efectiva contra el Cibercrimen.*

Con esta medida se pretende adoptar una política común entre los diferentes países para luchar de forma efectiva contra la ciberdelincuencia, pues según señala el propio preámbulo del mismo, el Convenio tiene como finalidad perseguir y evitar los actos delictivos cometidos contra o con la ayuda de Internet. De este modo, se procura definir una política criminal común a todos los Estados miembros sobre la utilización de las redes de datos y de información electrónica para evitar actividades terroristas o ilegales. Según reveló un miembro de la comisión el *objetivo principal de la convención es impulsar la cooperación internacional de manera que se proteja a la sociedad del cibercrimen*³²⁷.

Según el texto hay cuatro grandes tipos de infracciones que constituyen cibercrimen si se demuestra que son intencionadas:

- 1- Aquellas que atentan contra la confidencialidad, la integridad y la disponibilidad de datos y de sistemas.
- 2- Las infracciones informáticas (fraudes y falsificaciones)
- 3- Las relacionadas con los contenidos (pornografía infantil, por ejemplo)
- 4- Las que se refieren a la propiedad intelectual. En este punto los defensores de la convención consideran esencial su tipificación ya que, afirman, la mayoría de la población sigue viendo el pirateo informático y otros delitos electrónicos como una cuestión principalmente moral, sin darse cuenta de los daños materiales y personales asociados.

Asimismo, el Convenio preveía el desarrollo de un protocolo adicional para prohibir la propagación de ideas racistas, antisemitas o xenófobas en la red. Finalmente, el *Protocolo Adicional al convenio sobre Cibercrimen relativo a la criminalización de actos de racismo y xenofobia cometidos mediante el uso de sistemas de información (Additional protocol to the Convention on Cybercrimen, concerning the criminalisation of acts of a racist and xenophobic nature, committed through the use of computer system)* fue adoptado por el Consejo de

327. En www.ciberlex.br (20-Diciembre-2001)

Ministros del Consejo de Europa el 7 de Noviembre de 2002 y firmado el día 28 de Enero de 2003 por 11 Estados miembros. El protocolo amplía el ámbito de aplicación del Convenio sobre el Cibercrimen, y contempla la distribución a través de Internet de propaganda racista o xenófoba, al tiempo que establece las medidas necesarias para fomentar la cooperación de los Estados firmantes en la tipificación y persecución de las conductas en sus ordenamientos jurídicos. En cuanto a su contenido, el protocolo establece la definición de lo que se entiende por material racista y xenófobo, considerando como tal cualquier material escrito, imagen u otra representación de ideas o teorías que promueva o incite la discriminación o violencia contra grupos de individuos, basados en la raza, el color, el origen racial o étnico, así como la religión. Además se establecen medidas que deberán adoptar los Estados firmantes en el ámbito nacional y la relación de éstas con el Convenio sobre el Cibercrimen. En concreto, las medidas nacionales a adoptar por cada estado serán las necesarias para perseguir la comisión de conductas que sean racistas o xenófobas.

La introducción de esta materia dentro del Convenio se justifica por el dramático aumento de propaganda racista y xenófoba en la red. *Algunos expertos hablan ya de una comunidad electrónica del odio*³²⁸. Lógicamente, la aplicación de las leyes nacionales contra el racismo y la xenofobia corren la misma suerte que el resto de normas que tratan de regular los contenidos en Internet con carácter y eficacia nacional. En estos casos, como en muchos otros, nos enfrentamos a problemas derivados de la naturaleza global de Internet y de la distinta estrategia seguida por los países para combatir estos trascendentes problemas. Internet se ha convertido en un lugar perfecto para toda clase de grupos organizados que fomentan el odio racial. Estos grupos crean sitios en Internet en nombres de dominios genéricos como “.org” (lo que hace creer que estamos ante organizaciones no gubernamentales ONGs) generando centenares de conexiones internacionales a otras fuentes de información racista y xenófobas. En este tipo de páginas se utiliza todo tipo de estrategias para seducir a futuros miembros de estos grupos, tales como publicación de música con contenido racista, videojuegos de alto contenido antisemita y comercialización de libros, ropa o detalles nazis.

328. FERNÁNDEZ ESTEBAN, M.L., *“Internet y los derechos fundamentales”*, op. cit., p. 114.

Es indudable que el problema de la delincuencia en la Red es un tema polémico que demanda una actuación firme, de forma conjunta con la participación de la sociedad y del Estado, de cara a su erradicación o, al menos, su disminución. Sin embargo, y pese a su propósito, el Convenio contra la Ciberdelincuencia ha levantado posturas y voces enfrentadas pues, como resulta obvio, a mayor vigilancia de la red, menor es la libertad de que se puede gozar en la misma. Nos encontramos aquí frente al eterno dilema social y jurídico consistente en la elección entre libertad o seguridad. El binomio libertad-seguridad se encuentra presente en todos y cada uno de los problemas sociales a los que tiene que dar respuesta el Derecho. A mayor libertad, menor seguridad; por el contrario, a mayor seguridad, menor es la libertad. La alternativa es obvia y parece que los Estados ya han tomado una decisión, mayor seguridad en detrimento de las libertades de la sociedad, tanto dentro como fuera de la red. El incremento de vigilancia que se lleva a cabo para evitar el cibercrimen, preocupa en gran medida a los defensores de los derechos civiles, que ven peligrar los derechos conseguidos desde hace tiempo de privacidad y libertad en la red, ya que el poder de los Estados se incrementa considerablemente con este acuerdo.

Existen otras teorías basadas en la cooperación internacional aplicada al Ciberespacio que se alejan de los clásicos Tratados Internacionales. Una de las más famosas es la que defiende BURK. Para este autor lo más conveniente para regular el Ciberespacio es aplicar al mismo una estructura federalista similar a la existente entre los Estados de los Estados Unidos³²⁹. Para muchos observadores, un marco jurídico internacional podría presentar ciertas ambigüedades, en particular cuando se trata de acordar, en el ámbito internacional, los criterios para juzgar la ilicitud de algunos temas relacionados con concepciones diferentes de la civilización. Como ya hemos mencionado, la no-homogeneidad ética, así como la falta de criterios universales de licitud o ilicitud entorpecen enormemente la creación de marcos normativos de carácter mundial. Según BURK, en los Estados Unidos, el poder está dividido de manera vertical entre los Estados y el Gobierno Federal, y de manera horizontal entre los distintos Estados. Es esta última divi-

329. BURK, D.L., "Federalism in cyberspace", *op. cit.*, on line: www.temple.edu/lawschool/dpost/burk%20federalism.pdf

sión la que puede ser importante en el ámbito del Ciberespacio. La aplicación de la estructura y la cooperación-competitividad del federalismo al Ciberespacio, puede manifestarse como la solución más adecuada a la problemática reguladora del mismo.

III.4. OTROS MECANISMOS DE HETERORREGULACIÓN

Para finalizar este capítulo es conveniente analizar, aunque muy sucintamente, otros mecanismos de control y ordenación del Ciberespacio que han sido defendidos desde diversos foros. No obstante, hay que precisar que muchas de las propuestas regulatorias recogidas en este último epígrafe son formas mixtas de autorregulación y heterorregulación, participando más de uno u otro componente según las circunstancias, la materia regulada y el autor. Por ello, las opciones de regulación aquí propuestas no se corresponden exactamente con la heterorregulación, pero tampoco con la autorregulación pura.

Es famosa, y punto de partida de cualquier estudio relacionado con la red y las reglas que en ella se dan, la teoría desarrollada magistralmente por Lawrence LESSIG profesor de Derecho en la Universidad de *Harvard*. Este autor mantiene una de las posturas más originales sobre la regulación de la red, defendiendo la existencia de un sistema constitucional donde el Código informático es la ley. Para LESSIG *incluso sin la colaboración del Estado, la red se irá desplazando paulatinamente hacia una arquitectura de control (...) Las tendencias actuales anticipan una red altamente regulable, no la utopía libertaria, sino una red cuya esencia sea su carácter controlador*³³⁰. La esencia de la red es el control, y el control viene dado precisamente por la estructura de la misma, es decir el modo en que el hardware y el software se interrelacionan en el Ciberespacio. El código así entendido sienta las bases de la arquitectura de la red, la cual, usada en la dirección adecuada, puede ser el elemento único necesario para controlar el Ciberespacio. Por ello, LESSIG sabe que el Ciberespacio será controlado por aquel que consiga entender la arquitectura de la red y someterla a sus deseos de intervención.

330. LESSIG, L. *El código y otras leyes del Ciberespacio, op. cit., p. 65.*

La red está compuesta por una gran variedad de arquitecturas, unas más tendentes a la regulabilidad del Ciberespacio que otras. *La naturaleza de la red viene determinada fundamentalmente por sus arquitecturas, y las posibles arquitecturas del Ciberespacio son muy numerosas. Cada una de dichas arquitecturas se basa en unos principios diferentes, y una de las características en que se pueden diferenciar es la regulabilidad. Es decir, la capacidad para controlar la conducta en el seno de un Ciberespacio dado: algunas arquitecturas hacen que la conducta resulte más regulable y otras hace que resulte menos regulable. Estas arquitecturas están desplazando a las arquitecturas de la libertad*³³¹. El mismo autor continúa afirmando que *entre las muchas arquitecturas posibles que la red podría tener, mi intención es demostrar que esta evolucionando en una dirección muy concreta; de un espacio irregulable a otro altamente regulable*³³².

Es más, indica que *los cambios que posibilitan el comercio a través de la red son los mismos que facilitarán la regulación, ya que el comercio exige confianza y la estructura de la red debe configurarse de tal modo que ofrezca esa confianza a los usuarios*³³³. La confianza del mercado nos lleva a la regulación del Ciberespacio. Ya vimos cómo esta era una de las tres causas que considerábamos como determinantes a la hora de justificar la regulación de la red por parte de los Estados.

Para entender correctamente la postura de este autor es necesario analizar el proceso de desarrollo de la red desde una fase de no regulación a otra de total control, pasando por los medios empleados para ello. LESSIG está convencido de que la red ha dejado de ser el paraíso de la libertad que era, para convertirse en un verdadero espacio de control y regulación. Cuatro son las restricciones que se imponen sobre la libertad de la red: el mercado, la arquitectura, la ley y los usos³³⁴.

Las leyes, como normas generadas por las autoridades gubernamentales respaldadas por una sanción, regulan el Ciberespacio. Las

331. *Ibíd.*, p. 67.

332. *Ibíd.*, p. 58.

333. *Ibíd.*, p. 67.

334. *Ibíd.*, pp. 167 y ss.

leyes referidas a propiedad intelectual, a delitos cibernéticos, así como muchas otras limitan la libertad en la red. Además de las leyes, los usos cibernéticos también regulan la conducta en el Ciberespacio, como una manifestación típica de la autorregulación. Las normas sociales restringen de manera diferente. Por normas sociales se entiende las normas impuestas, no por medio de las actuaciones organizadas y centralizadas del Estado, sino por medio de las más ligeras y a veces también más poderosas sanciones que los miembros de una comunidad imponen unos sobre otros. En el caso de los usos, así como en el caso de las leyes, un conjunto de consideraciones limitan la conducta por medio de sanciones a posteriori impuestas bien por los órganos legales, bien por la comunidad. Pero los agentes reguladores del Ciberespacio no finalizan aquí para LESSIG, demostrando la eficacia e importancia del mercado y de la arquitectura (principal aportación de toda su obra).

Los mercados también regulan la conducta en Internet. Así, las estructuras de precios y otras conductas de restricciones y oportunidades en el mercado limitan y condicionan a priori el acceso a la red y el comportamiento de los usuarios en ella. Finalmente, y como elemento más determinante en la regulación de la red encontramos el código. El hardware y el software que hacen del Ciberespacio lo que es, constituyen a su vez un conjunto de restricciones acerca de cómo uno puede comportarse en él. Las sustancias de estas restricciones pueden variar, pero todas se experimentan como condiciones para acceder al Ciberespacio. En la misma dirección el profesor TRUDEL afirma que *la arquitectura técnica constituye un componente del marco jurídico de las actividades que tienen lugar en el Ciberespacio. Se entiende por arquitectura técnica el conjunto de elementos o artefactos técnico, tales como los de tipo hardware, los de software, los Standard y las configuraciones que determinan el acceso y los derechos de uso de las fuentes del Ciberespacio*³³⁵.

Para este autor, al igual que sucede en el mundo físico, estas cuatro restricciones operan sobre el mundo de Internet. Las leyes, los usos, el mercado y las arquitecturas interactúan para construir el entorno que los ciberciudadanos conocen.

335. TRUDEL, P., “Derechos y responsabilidades de los usuarios en el Ciberespacio”, *op. Cit.*, p. 54.

Otros autores comparten con LESSIG la posibilidad de efectuar una regulación del Ciberespacio mediante la propia arquitectura. HICKS, por ejemplo, habla de regulación física del Ciberespacio como alternativa a la legislación del mismo. Hay, afirma este autor, *también un segundo acercamiento* -el primero sería la legislación- *a la regulación de Internet: podemos procurar manipular físicamente las computadoras del mundo sobre las que funciona Internet. Esto significa, por ejemplo, que los filtros electrónicos se pueden colocar en los puntos estratégicos de los caminos del Internet para filtrar el material indeseado. Este acercamiento sigue siendo, sin embargo, muy polémico, pues los tecnólogos y los ingenieros no se ponen de acuerdo en si esto está en todo factible*³³⁶.

Sabemos que es posible filtrar hacia fuera cierta información, a pesar de ello, este autor, tras analizar las ventajas y los inconvenientes de este tipo de regulación llega a la conclusión de está claro que el software de filtración, en general la regulación física, no se debe ver como la única solución. Internet necesita de la legislación, de la ley. Aunque este método puede ser una gran ayuda en la regulación de la red, debemos también mirar otros métodos para ayudarnos a encontrar una solución al desafío de Internet.

Otro examen interesante sobre los modos de regulación del Ciberespacio lo encontramos en la obra de D.G. POST. Este autor defiende la idea de abordar el control y la regulación de la red desde el punto de vista del consumidor. Defiende una curiosa idea de gobernación del Ciberespacio, estableciendo la idea de un mundo de usuarios voluntarios, donde las reglas no se imponen, sino que se eligen. Un mundo que minimiza el poder de los Estados, los cuales compiten por atraer y mantener los ciudadanos, ansiosos por complacer y temerosos de disgustar.

En este sentido, si a los cibernautas no les gusta una cibercomunidad concreta, así como las reglas de la misma, pueden marcharse, de una manera mucho más sencilla que en el espacio real. Dado que la salida es barata, se puede establecer como una manera de votar; así el mundo del Ciberespacio puede convertirse en un menú virtual de modo que, si al consumidor no le gusta la elección y el conjunto de normas que allí se desarrollan, puede decidirse por otra.

336. HICKS, B.D., *Choice of law issues in cyberspace*, op. cit.

Las comunidades en el Ciberespacio, afirma POST, están gobernadas por un *conjunto de reglas*. Los individuos pueden elegir en cual de los conjuntos de reglas ofertados se introducen. Puesto que los diferentes conjuntos de reglas competirán por nuestra atención, el mundo del Ciberespacio quedará definido por esta competencia entre soberanías para captar clientes. En este sentido, puesto que la presión de la competencia es mayor en el seno del Ciberespacio que en el espacio físico real, los Estados y otros propagadores de conjuntos de reglas actúan como las Empresas en el ámbito de un mercado libre.

En su artículo *Anarchy, State and the Internet*³³⁷, POST desarrolla su teoría sobre la creación de normas en el Ciberespacio, teoría más cercana a la autorregulación que a la heterorregulación, aunque por razones sistemáticas será incluida en este epígrafe. Analiza principalmente el aspecto de quién hará y dará fuerza a las reglas que se establezcan en él, examinando varios controladores o puntos desde los cuales las reglas pueden emitirse e imponerse. Los diferentes controladores presentan diferentes modelos para otorgar fuerza a las normas que cada uno pretende adoptar. Además, lo más característico e importante de esta postura es el hecho de que los destinatarios de las normas son absolutamente libres para entrar, salir o cambiar de jurisdicción, de cibercomunidad, y así cambiar de normas y de conjunto de reglas reguladoras. Basados en esta libertad, cada uno de los controladores trata de establecer las normas más adecuadas para evitar el abandono de los usuarios, formándose una situación equiparable al libre mercado.

Desde esta posición la pregunta de quién gobernará el Ciberespacio puede sustituirse por la de cómo va a llevarse a cabo la competencia entre todos estos controladores y sus normas. Cada uno de ellos actuará como empresario en un mercado de libre competencia, estableciendo las normas más atractivas para los cibernautas, ya que si no están de acuerdo con las mismas, les bastará con abandonar la cibercomunidad donde este controlador haya asentado su conjunto de reglas y marcharse a otra cibercomunidad con reglas que se adecuen más a sus necesidades o características.

337. POST, D.G., *Anarchy, State and the Internet: an essay on law-making in cyberspace*, op. cit.

Asimismo, HICKS reconoce la importancia de los proveedores de acceso a Internet en el marco de Gobierno de la red, afirmando que el Ciberespacio es totalmente diferente a los Estados geográficamente basados. Uno puede incluso decir que es una dimensión alternativa totalmente diversa en la cual los *Internet Service Provider*³³⁸ son los encargados de crear las reglas en la red. Los ISP gobiernan sus redes, y las cambian de cualquier manera para satisfacer sus necesidades. Por lo tanto *cada red se puede comparar a un país soberano que sea gobernado por el Internet Service Provider correspondiente*³³⁹. Pero hay un punto importante, tenemos dos mundos: el mundo verdadero con países geográficamente basados que son gobernados por Estados soberanos -y son los verdaderos poseedores del poder-, y el Ciberespacio, que consiste en diversas redes que son gobernadas por los *Internet Service Provider*. La pregunta que debe realizarse es por qué no establecemos simplemente las reglas que creen los ISP para el Ciberespacio como normas reguladoras de la red. La razón es simple. Aunque los *Internet Service Provider* son los gobernadores de Ciberespacio, no son los poseedores del poder en el *mundo verdadero*. No pueden hacer leyes y hacerlas cumplir allí. En este sentido hay que dejar claro que, aunque el Ciberespacio es diferente del mundo físico, existe dentro del *mundo verdadero*. El Ciberespacio se construye y transporta sobre el mundo físico. Los ciudadanos del Ciberespacio son también ciudadanos del mundo real, aunque están situados en diversos países. Cuando miramos mecanismos de aplicación, tenemos que mirar inevitable el *mundo verdadero*. El culpable vive en el mundo verdadero, y es solamente allí que podemos conseguirle.

Por ello, la regulación de los ISP es, a juicio de HICKS, insuficiente para regular la red, ya que olvida la importancia del mundo físico, y la importancia de los que allí ostentan el poder. Es necesario implementar el papel de estos operadores con la labor de detentadores de poder en el mundo real, a ser posible una Organización Internacional. Ya

338. *Internet Service Provider: Proveedor de servicios de Internet. Organización que se encarga de dar acceso a Internet a personas físicas y/o jurídicas, además les ofrece una serie de servicios adicionales en Internet (hospedaje de páginas web, consultoría de diseño, etc.)*

339. HICKS, B.D., *Choice of law issues in cyberspace*, op. cit., *Se puede acceder on line: www.geocities.com/athens/Academy/5090*

vimos cómo para HICKS una Organización Internacional es el instrumento perfecto para la regulación de la red, sobre todo de los detalles de la misma -los aspectos generales y básicos podían ser regulados por un Tratado multilateral-, contando con la ventaja adicional de que esta organización tiene poder para gobernar, ya que los Estados soberanos se lo han otorgado.

Nos encontramos claramente con un ejemplo típico de regulación compartida, autorregulación (ISP) y heterorregulación (Organización Internacional) han de actuar conjuntamente a fin de obtener resultados efectivos.