

# DERECHO Y TECNOLOGÍAS DE LA INFORMACIÓN

---

*Coordinador:*

IÑIGO DE LA MAZA GAZMURI

*Comité de edición:*

GONZALO ANGELI GUTIÉRREZ

SERGIO CRUZ CRUZ

SALVADOR MILLALEO HERNÁNDEZ

UNIVERSIDAD DIEGO PORTALES  
FACULTAD DE DERECHO  
FUNDACIÓN FERNANDO FUEYO LANERI

Primera edición de  
1.000 ejemplares  
Abril de 2002

Registro de Propiedad Intelectual  
Inscripción N° 125.329

*Diseño de portada:*  
Ximena Escobar

*Impresión:*  
Alfabeta Artes Gráficas  
Carmen 1985  
Fono Fax: 551 5657

# Contenido

---

<b>Presentación</b>	9
<b>PARTE 1: El derecho en los tiempos de Internet</b>	13
1 <i>La ley del caballo: lo que el ciberderecho podría enseñar</i> , LAWRENCE LESSIG.	15
2 <i>El Derecho Informático como rama autónoma del Derecho. Naturaleza jurídica del Derecho Informático</i> , HÉCTOR RAMÓN PEÑARANDA QUINTERO.	69
<b>PARTE 2: Un vistazo a la nueva economía</b>	85
3 <i>Chile ante los desafíos de la nueva economía</i> , GEORGE LEVER.	87
4 <i>Capital de riesgo e inversión en empresas de tecnología en Latinoamérica: consideraciones de un inversionista</i> , CRISTIÁN SHEA CAREY.	103
<b>PARTE 3: El comercio electrónico</b>	113
<b>PARTE 3.1: Perspectivas</b>	115
5 <i>Relaciones comerciales en Internet: aproximación a las nuevas relaciones surgidas como consecuencia del e-commerce</i> , MCS. YARINA AMOROSO FERNÁNDEZ.	117
6 <i>Sobre la realidad de hacer e-commerce</i> , ERICK IRIARTE AHON	149

---

# La ley del caballo: lo que el ciberderecho podría enseñar\*

---

LAWRENCE LESSIG\*\*

## Introducción

Hace algunos años, en una conferencia sobre “La ley del ciberespacio” llevada a cabo en la Universidad de Chicago, el juez Frank Easterbrook dijo a la asamblea, un salón lleno de devotos del ciberderecho —y otros peores— que no existía una “ley del ciberespacio” más de lo que existía una “Ley del caballo”<sup>1</sup>; que el esfuerzo de hablar como si esta ley existiera enturbiaría en vez de aclarar; y por lo tanto los académicos del derecho (“diletantes”) deberían hacerse a un lado, dejando a los jueces, abogados y tecnólogos trabajar en los problemas cotidianos que estos teléfonos potenciados presentarían. “Váyanse a casa”, fue la bienvenida del juez Easterbrook.

Como suele suceder, cuando mi entonces colega habla, la intervención, aunque brillante, produjo un incómodo silencio, algunos aplausos de cortesía y un rápido pase al próximo conferencista. Resultaba atractivo pensar que esa conferencia sería tan relevante como aquella sobre la ley del caballo. (Un ansioso estudiante sentado detrás de mí susurró que él nunca había escuchado acerca de la “ley del caballo”). Dos hora más tarde en ese día completo de conferencias, sin embargo, este pensamiento no parecía demasiado útil; de esta manera, fue rápidamente dejado de lado. Los discursos cambiaron en el balance del día y el balance de las contribuciones se orientó hacia la idea que, después de todo, ni la ley del caballo ni la ley del ciberespacio eran algo relevante.

No obstante lo anterior, algunos de quienes asistimos a ese día de conferencias no pudimos dejar la cuestión atrás, yo soy uno de ellos. Confieso que he pasado mucho tiempo pensando acerca de qué es lo que la ley del ciberespacio podría enseñar. Este ensayo es una introducción a la respuesta<sup>2</sup>.



La preocupación de Easterbrook es razonable. Los cursos en las escuelas de derecho, argumenta Easterbrook, deben estar limitados a materias que puedan iluminar el ordenamiento jurídico completo<sup>3</sup>. “[E]l mejor camino para aprender la ley aplicable a materias especializadas”, argumenta, “es estudiar las reglas generales”<sup>4</sup>. Esta “ley del ciberespacio” concebida como responsabilidad extracontractual en el ciberespacio, contratos en el ciberespacio, propiedad en el ciberespacio, no cumple con este requisito.

Mi argumento es el contrario. Estoy de acuerdo en que debemos enfocarnos hacia cursos que resulten capaces de “arrojar luz sobre el ordenamiento jurídico completo”, pero, a diferencia de Easterbrook, creo que existe un punto general e importante que surge de la reflexión acerca de la forma en que el derecho y el ciberespacio se conectan.

Este punto general es acerca de los límites del derecho como un regulador y acerca de las técnicas para escapar de esos límites. Esta escapatoria, tanto en el mundo real como en el ciberespacio<sup>5</sup>, proviene del reconocimiento del conjunto de herramientas que una sociedad dispone para constreñir la conducta de los sujetos. El Derecho en su sentido tradicional —un mandato respaldado por la amenaza de una sanción<sup>6</sup>— es solamente una de estas herramientas. El punto general es que el derecho puede afectar a las otras herramientas, aquellas que se utilizan para constreñir la conducta y pueden funcionar como herramientas del derecho. La elección entre estas herramientas depende obviamente de su eficacia. Sin embargo, y este es un punto importante, la elección también implica una cuestión acerca de valores. A través de algunos ejemplos de interacción entre derecho y ciberespacio, arrojaremos cierta luz sobre un conjunto de preguntas generales acerca de la regulación legal fuera del ciberespacio.

No argumento en estas líneas que cualquiera otra área especializada del derecho produzca las mismas ventajas. No defiendo aquí la ley del caballo. Mi argumento es específico para el ciberespacio. Cuando reflexionamos acerca de la regulación del ciberespacio vemos algo que nuestros estudios sobre otras áreas del derecho no nos muestran.

Mi ensayo se desarrolla en tres partes. Comienzo con dos ejemplos paradigmáticos de los problemas que subyacen a la regulación del ciberespacio. Estos ejemplos deberían sugerir una aproximación distintiva al problema de la regulación en general. En la Parte I, resumo un modelo de esta aproximación general.

En la Parte II aplico esta aproximación general a un espectro más amplio de ejemplos. Es en los detalles de estos ejemplos donde pueden ser encontradas lecciones generales. Estas lecciones generales sobrepasan las fronteras del ciberespacio. Se trata de lecciones aplicables al ordenamiento jurídico en general, aunque la falta de plasticidad del espacio real tiende a oscurecerlas.

La Parte final describe tres de estas lecciones –la primera es acerca de los límites de la ley en el ciberespacio, la segunda acerca de la transparencia de la regulación y la tercera sobre un ajuste exacto (*narrow tailoring*) del código.

La primera lección es acerca de restricciones constitucionales –entendida la constitución no como un texto legal, sino más ampliamente. Así como la división de poderes establece limitaciones sobre hasta dónde puede llegar el gobierno federal, de la misma manera las características del ciberespacio que describiré establecen límites a las posibilidades del gobierno.

La lección sobre transparencia resultará más familiar, aunque sospecho que su relación con el ciberespacio no lo será tanto. Haciendo la “no-transparencia” sencilla y aparentemente natural, el ciberespacio provee una oportunidad especial para apreciar tanto el valor como los costos de la transparencia. La última lección acerca de los límites en el diseño del código, resultará menos familiar, aunque es potencialmente la característica más relevante en la interacción entre ciberespacio y derecho del mundo real. En los ejemplos de regulación en el ciberespacio, veremos la amenaza que una falla en la determinación de los límites produce. Las lecciones acerca de transparencia y límites tienen ambas importancia más allá del mundo de los ingenieros. Mejor dicho, las regulaciones producidas por los ingenieros tendrán importantes consecuencias para el resto.

Concluyo con una respuesta al desafío de Easterbrook. Si mi argumento es correcto, entonces estas tres lecciones presentan desafíos respecto a la regulación tan problemáticos en el espacio real como en el ciberespacio. Esto es, se trata de preocupaciones generales, no particulares; sugieren, por lo mismo, razones para estudiar la ley del ciberespacio que exceden las particularidades del ciberepacio.

## I. ESPACIOS REGULATORIOS, REALES Y “CIBER”

En esta sección considero dos ciberespacios y los problemas que cada uno de ellos crea para dos metas sociales diferentes. Ambos espacios poseen diferentes problemas de “información” –en el primero no hay suficiente y, en el segundo, existe demasiada. Ambos problemas provienen de una circunstancia acerca del *código* (code)– acerca del software y hardware que configura cada ciberespacio de la forma que es. Como argumento más detalladamente en lo que sigue, el desafío regulatorio central en el contexto del ciberespacio es cómo hacer sentido de este efecto del código.

### A. Dos problemas con las expresiones sectorizadas (Zoned Speech)

1. *Expresiones sectorizadas.* En el espacio real la pornografía es restringida a los niños. Ya sea por la ley (a través de la prohibición de la venta de pornografía a menores), las normas sociales (que nos hacen rehuir a aquellos que venden pornografía a niños), o el mercado (la pornografía cuesta dinero). En general, aunque no siempre, es difícil, no imposible, para los niños adquirir pornografía en el espacio real; sin embargo, un balance de los efectos de las distintas regulaciones del espacio real indica que estas cumplen satisfactoriamente su cometido: mantienen a los niños alejados de la pornografía.

Estas regulaciones del espacio real dependen de ciertas características del “diseño” del espacio real. En el espacio real resulta dificultoso ocultar que usted es un niño. En el espacio real la edad es un hecho autoautentificante (self-authenticating). Es cierto que un niño puede intentar ocultar su edad; puede utilizar un bigote o caminar sobre tacos. Con todo, estos disfraces son costosos y no demasiado efectivos; por lo demás, caminar utilizando tacos es difícil. Lo normal es que un niño transmita que es un niño; por lo general el vendedor de pornografía sabe que un niño es un niño<sup>7</sup>, y de esta manera, ya sea por consideración a la ley o a las reglas sociales, al menos el vendedor puede identificar a los clientes menores de edad. La autoautenticación hace la restricción de este tipo de expresiones relativamente sencillas.

En el ciberespacio la edad no es autoautentificante de la misma manera. Aun si las mismas leyes o reglas sociales se aplicaran en el ciberespacio y aun si las restricciones impuestas por el mercado fueran las mismas (como si no fueran las mismas), cualquier esfuerzo por restringir el acceso de menores a la pornografía enfrentaría una dificultad bastante seria. La edad es extraordinariamente difícil de certificar. Para un sitio web que acepta tráfico, todas las peticiones de ingreso son iguales. No existe una forma sencilla de distinguir a los adultos de los niños y, por lo mismo, no existe una forma sencilla para un adulto de probar que es un adulto. Esta *característica* del espacio hace que la restricción de este tipo de expresiones sea costosa —tan costosa—, que la Corte Suprema concluyó en *Reno v. ACLU*<sup>8</sup> que la Constitución debía prohibir este tipo de restricciones<sup>9</sup>.

2. *Privacidad protegida.* Si usted entrara a una tienda y el guardia a la entrada anotara su nombre; si cámaras siguieran cada uno de sus pasos, advirtiéndole qué productos vio y cuáles ignoró; si un empleado lo siguiera mientras recorre la tienda, calculando el tiempo que usted gasta en cada sección de productos; si antes que usted pudiera comprar el producto que ha seleccionado, el cajero le exigiera revelar su identidad, si cualesquiera de estas cosas ocurriera en el mundo real, usted lo nota-

ría. Usted advertiría y podría entonces elegir si desea o no comprar en dicha tienda. Probablemente algunos vanidosos disfrutarían la atención que se les presta; quizás aquellos que gustan de ahorrar se sentirían atraídos por los precios más bajos. Es posible que vanidosos y ahorrativos no tuvieran problemas con este régimen de recolección de información. Sin embargo, al menos, tendrían noticia de él. Cualquiera que sea la razón y la consecuente elección, en el espacio real usted sabría lo suficiente como para hacer su propia elección.

En el ciberespacio usted no lo sabría. Usted no advertiría este monitoreo, porque dicha vigilancia en el ciberespacio no es similarmente visible. Como Jerry Kang<sup>10</sup> describe acertadamente, cuando usted entra a una tienda en el ciberespacio, la tienda puede grabar quién es usted; monitores click (que vigilan qué es lo que usted elige con su mouse) irán configurando una bitácora de su itinerario, del tiempo que utilizó en cada página; un empleado (aunque se trate solamente de un bot<sup>11</sup>) puede seguirlo durante todo su recorrido, y cuando haga una compra, grabar quién es usted y de dónde viene. Todo esto sucede—invisiblemente— en el ciberespacio. La información es recolectada, pero esta vez, sin su consentimiento. De esta manera, usted no puede (no simplemente al menos) elegir o consentir si participará en esta vigilancia o no. En el ciberespacio la vigilancia no es auto-autentificante. Nada revela que usted está siendo observado<sup>12</sup>, de esta manera, no existe una base sobre la cual consentir esa vigilancia.

Estos ejemplos se asemejan uno al otro y presentan un patrón común. En cada uno de ellos un pedazo de la información está ausente, lo que significa que en cada caso un objetivo no puede ser perseguido. En el primer caso este fin es colectivo (restringir el acceso a la información); en el segundo, es individual (elegir la privacidad). Sin embargo, en ambos casos, es una característica del ciberespacio la que interfiere con el objetivo perseguido. Por lo mismo, en ambos casos, el derecho enfrenta un desafío, a saber, si regular para cambiar esta característica de la arquitectura del ciberespacio o dejar al ciberespacio funcionar y renunciar a este objetivo individual o colectivo. ¿Debería modificarse el derecho como resultado de estos cambios o debería el derecho intentar cambiar las características del ciberespacio para hacerlo conformarse a ella?, y, en este último caso, ¿qué restricciones deberían existir en el esfuerzo del derecho por cambiar la “naturaleza” del ciberespacio, ¿qué principios deberían regular esta iniciativa inútil? o, una vez más, ¿cómo debería *regular* el derecho?

\* \* \*

La mayoría de estas preguntas parecerán muy extrañas. Mucha gente piensa que el ciberespacio simplemente no puede ser regulado. La conducta en el ciberespacio, insisten estos memes\*, está más allá del alcan-

ce del gobierno. El anonimato y la multijurisdiccionalidad del ciberespacio hacen que su control por parte del gobierno sea imposible. La naturaleza del espacio hace que allí la conducta sea *irregulable*<sup>13</sup>.

Esta creencia acerca del ciberespacio es errónea, pero errónea de una forma interesante. Al afirmar lo anterior pueden estar asumiéndose dos cosas, o bien se asume que la naturaleza del ciberespacio es inmutable —esto que la arquitectura y el control que subyace a ella, no pueden ser modificados— o bien se asume que el gobierno no puede emprender iniciativas para cambiar esta arquitectura.

Ninguna de las asunciones es correcta. El ciberespacio no tiene naturaleza; no posee una arquitectura particular que no pueda ser modificada<sup>14</sup>. Su arquitectura es una función de su diseño, o, como lo describo en la sección siguiente, de su código<sup>15</sup>. Este código puede cambiar o porque evoluciona en un modo distinto, o bien porque el gobierno o los negocios presionan su evolución en un determinado sentido. Y mientras versiones particulares del ciberespacio resisten la regulación efectiva, de esto no se sigue que todas las versiones del ciberespacio lo harán. Dicho de otra manera, hay versiones del ciberespacio donde la conducta puede ser regulada y el gobierno puede tomar medidas para incrementar esta posibilidad de regular.

Para ver cómo es posible esto debemos pensar más ampliamente acerca del problema de la regulación. ¿Qué significa decir que alguien es regulado? ¿Cómo se consigue esa regulación? ¿Cuáles son sus modalidades?

## **B. Modalidades de regulación**

*1. Cuatro modalidades de regulación en el espacio real y en el ciberespacio.* La conducta, podríamos afirmar, se encuentra regulada por cuatro tipos de restricciones (constraints)<sup>16</sup>. El derecho es solo una de estas restricciones. El derecho (al menos en uno de sus aspectos) ordena a la gente comportarse de una cierta manera; amenaza con sanciones si ellos no obedecen<sup>17</sup>. El derecho me dice que no compre ciertas drogas, que no venda cigarrillos sin una licencia y que no comercie entre fronteras internacionales sin primero llenar un formulario de aduanas. El derecho amenaza con sanciones severas si estas órdenes no son cumplidas. En este sentido decimos que el derecho regula.

Pero no solo el derecho regula en este sentido. Las normas sociales también lo hacen. Las normas controlan dónde puedo fumar; ellas afectan la forma en que me comporto frente a personas del sexo opuesto; limitan mi forma de vestir, e influyen en mi decisión de pagar o no impuestos. Como el derecho, las normas regulan a través de la amenaza de castigo *ex post*. Sin embargo, a diferencia del derecho, los castigos de estas normas no son centralizados. El cumplimiento de las normas es

exigido (si es que lo es) por la comunidad, no por el gobierno. En este sentido, las normas suponen restricciones a la conducta y, por lo tanto, regulan.

Los mercados también regulan. En este caso, a través del precio. El precio de la gasolina limita la cantidad que uno conduce su automóvil, más en Europa que en los Estados Unidos. El precio de los boletos de los trenes subterráneos afecta el uso del transporte público, más en Europa que en los Estados Unidos. Por supuesto, el mercado es capaz de restringir la conducta de esta manera únicamente porque existen las restricciones impuestas por el derecho y las normas sociales: los derechos de propiedad y contratos regulan los mercados; los mercados operan dentro de la esfera permitida por las normas sociales. Pero, dadas estas normas y el derecho, el mercado presenta otro conjunto de restricciones en la conducta individual y colectiva.

Y, finalmente, existe una cuarta característica del espacio real que regula la conducta: la "arquitectura". Cuando utilizo la palabra "arquitectura" quiero decir el mundo físico tal como lo encontramos, aun si "*como lo encontramos*" es simplemente *como había sido hecho*. El hecho que una carretera divida dos vecindarios, limita la posibilidad de integración que los vecindarios facilitan. El hecho que una ciudad posea una plaza con un conjunto de tiendas fácilmente accesibles, incrementa la integración de los habitantes de esa ciudad. El hecho de que París posea extensos bulevares, limita la posibilidad de los revolucionarios de protestar<sup>18</sup>. El hecho que el Tribunal Constitucional alemán esté en Karlsruhe, mientras la capital está en Berlín, limita la influencia de un poder del Estado sobre el otro. Todas estas restricciones funcionan de una forma que modelan la conducta. En este sentido, ellas también regulan.

Estas cuatro modalidades regulan la conducta unidas. La "red regulatoria" (net regulation) de cualquier política de regulación es la suma de los efectos de estas cuatro modalidades juntas. Una política de regulación implica una comparación y elección (trade-off) entre estas cuatro herramientas regulatorias. Se selecciona una herramienta dependiendo cuál sea la que funciona mejor en un escenario determinado.

Entendido de esta manera, este modelo puede ser también utilizado para describir la regulación del ciberespacio. Aquí también podemos encontrar cuatro modalidades de regulación.

El derecho regula la conducta en el ciberespacio, los derechos de autor, las leyes sobre difamación y las leyes sobre obscenidad continúan amenazando sanciones *ex post* por sus violaciones. Cuán eficiente sea la regulación de las leyes en el ciberespacio es otra historia, en algunos casos es muy eficiente y en otros no. Mejor o peor, el derecho continúa constituyendo la amenaza de una sanción. Los legisladores promulgan leyes<sup>19</sup>, los fiscales se encargan de la amenaza<sup>20</sup> y los tribunales de sancionar su incumplimiento<sup>21</sup>.



Las normas sociales también regulan la conducta en el ciberespacio: hable acerca de políticas demócratas (democratic politics) en el alt.knitting newsgroup, y se expone a una "llamarada" (una respuesta, con base de texto [text-based] encolerizada). Utilice la identidad de otro ("Spoof") en un MUD (una realidad virtual con base de texto) y usted verá su carácter removido ("toaded")<sup>22</sup>. Hable demasiado en una lista de discusión y probablemente se encontrará con un filtro "bozo" (bloqueando los mensajes que usted envíe). En cada caso las normas restringen la conducta y, como en el caso del espacio real, la amenaza de sanciones *ex post* (pero descentralizadas) hace que estas normas se cumplan.

Los mercados también regulan la conducta en el ciberespacio. La estructura de precios frecuentemente limita el acceso, y si ellas no lo hacen, las señales de congestión (busy signals) cumplen esta función. (America Online (AOL) aprendió esta lección cuando cambió su sistema de tarifas desde un sistema de tarifa hora a uno de tarifa plana)<sup>23</sup>. Algunos sitios de la red cobran por acceso, como los servicios en línea, como AOL, lo han hecho por algún tiempo. Los avisadores recompensan a los sitios populares; los servicios en línea bajan aquellos foros que no resultan populares. Estas conductas son todas una función de las restricciones impuestas por el mercado y reflejan el papel regulatorio del mercado.

Y finalmente la arquitectura del ciberespacio, o su *código*, regulan también la conducta en el ciberespacio. El código, o el hardware y software que configuran al ciberespacio de la forma que es, determinan un conjunto de limitaciones acerca de cómo puede comportarse uno<sup>24</sup>. La esencia de estas restricciones varía, el ciberespacio no es un solo lugar. Sin embargo, lo que distingue las restricciones arquitectónicas de otras es la forma en que ellas son experimentadas. Como sucede en el caso de las restricciones que impone la arquitectura en el mundo real —líneas de ferrocarriles que dividen vecindarios, puentes que bloquean el acceso de buses, tribunales constitucionales ubicados a millas del asiento del gobierno—, ellas son experimentadas como las condiciones de acceso del ciberespacio. Estas condiciones, sin embargo, son diferentes. En algunos lugares uno debe utilizar un password antes de poder obtener acceso<sup>25</sup>; a otros lugares se puede ingresar independientemente de si uno se identifica o no<sup>26</sup>. En algunos lugares, las transacciones que uno realiza dejan huellas, o "excrementos de ratón" que permiten vincular las transacciones al sujeto que las realizó<sup>27</sup>, en otros lugares, este vínculo solo puede llevarse a cabo si el sujeto presta su consentimiento<sup>28</sup>. En algunos lugares uno puede elegir hablar un lenguaje que solo el receptor puede entender (a través de la encriptación)<sup>29</sup>; en otros lugares la encriptación no es una opción<sup>30</sup>. El código establece estas características; ellas son elegidas por quienes escriben los códigos; ellas restringen algunas conductas (por ejemplo, el fisgoneo electrónico [electronic eaves-

dropping]) haciendo otras conductas posibles (encriptación). Estas características hacen posible la realización de ciertos valores o tornan imposible la de otros. En este sentido, así como la arquitectura en el espacio real regula, estas características del ciberespacio también lo hacen<sup>31</sup>.

Estas cuatro restricciones –tanto en el espacio real como en el ciberespacio– actúan juntas. Para cualquier política regulatoria, su interacción puede ser cooperativa o competitiva<sup>32</sup>. De esta manera, para entender cómo una regulación puede resultar exitosa, debemos examinar cómo estas cuatro modalidades operan sobre un mismo problema y entender cómo interactúan.

Los dos problemas considerados al comienzo de esta sección constituyen ejemplos simples de este punto:

- a) *Expresiones sectorizadas*. Si existe un problema con las expresiones sectorizadas en el ciberespacio, este es un problema que puede ser explicado (al menos en parte) por la arquitectura del lugar. En el espacio real la edad es (relativamente) autoautentificante. En el ciberespacio no lo es. La arquitectura básica del ciberespacio permite que los atributos de los usuarios permanezcan invisibles. De esta manera, resulta más difícil hacer cumplir las leyes o normas sociales referidas a la edad mínima en el ciberespacio. La arquitectura del ciberespacio debilita la actuación de estas leyes y normas.
- b) *Privacidad protegida*. Una historia similar puede ser contada acerca del “problema” de la privacidad en el ciberespacio<sup>33</sup>. La arquitectura del espacio real hace que la vigilancia generalmente sea autoautentificante. En general podemos advertir si estamos siendo seguidos o si información sobre nuestra tarjeta de identidad está siendo recolectada. Saber esto nos permite rehusar dar esa información si no queremos que sea conocida. De esta manera el espacio real interfiere con la recolección no consentida de información. Ocultar que uno está espionando es relativamente difícil.

La arquitectura del ciberespacio no evita en forma similar el espionaje. Nos adentramos en el ciberespacio sin que advirtamos las tecnologías que buscan y recopilan nuestra información. No podemos funcionar en la vida cotidiana si asumimos que a cualquier lugar donde vayamos nuestra información está siendo recolectada. Las prácticas de recolección varían dependiendo de los sitios y sus objetivos. Para consentir la vigilancia debemos saber que nuestra información está siendo recolectada. Pero, comparado con el espacio real, esta arquitectura debilita nuestra capacidad de saber cuándo estamos siendo vigilados y la toma de medidas para limitar esta vigilancia.

En ambos casos, la diferencia en la posibilidad de regulación –la diferencia en la regulabilidad (tanto colectiva como individual) del es-



pacio— se transforma en diferencias en las modalidades de restricción. De esta manera, como primer paso para entender por qué una determinada conducta en el ciberespacio puede ser distinta a una en el mundo real, debemos entender estas diferencias en las modalidades de regulación.

### C. *Cómo interactúan las modalidades*

1. *Efectos directos e indirectos.* Aunque he descrito estas cuatro modalidades como distintas, resulta obvio que ellas no operan independientemente, ellas, evidentemente, interactúan. Las normas sociales afectarán qué objetos se comerciarán en el mercado (normas en contra de la venta de sangre<sup>34</sup>); el mercado afectará la plasticidad, o maleabilidad, de la arquitectura (material de construcción de menor precio crea en el diseño una mayor plasticidad); la arquitectura afectará la posibilidad de algunas normas de desarrollarse (habitaciones públicas o comunes afectan la privacidad<sup>35</sup>); las tres determinarán qué leyes son posibles.

De esta manera, una descripción completa de la interacción entre las cuatro modalidades podría indicar las influencias de una sobre otra. En lo que sigue, sin embargo, me centro únicamente en dos. Una es el efecto del derecho sobre el mercado, las normas y la arquitectura; la otra es el efecto de la arquitectura sobre el derecho, el mercado y las normas.

Aíslo estas dos modalidades por razones diferentes. Me concentro en el derecho porque es el agente de regulación más obviamente autorreferente. Me concentro en la arquitectura porque en el ciberespacio será el agente más penetrante. La arquitectura será el regulador de la elección. Con todo, como argumento más adelante, nuestra intuición para pensar en un mundo regulado por la arquitectura esta subdesarrollada. Notamos cosas sobre un mundo regulado por la arquitectura (ciberespacio) que pasan inadvertidas cuando pensamos en un mundo regulado por el derecho (espacio real).

Con cada modalidad hay dos efectos diferentes. Uno es el efecto de cada modalidad con respecto al individuo que está siendo regulado. (¿Cómo es que el derecho, por ejemplo, restringe directamente a un individuo? ¿Cómo es que la arquitectura restringe directamente a un individuo?). El otro es el efecto de una modalidad de regulación dada sobre una segunda modalidad de regulación, un efecto que a la vez cambia el efecto de la segunda modalidad sobre el individuo. (¿Cómo es que el derecho afecta la arquitectura, que a la vez afecta las obligaciones del individuo?). Este primer efecto es *directo*, el segundo es *indirecto*<sup>36</sup>.

Un regulador utiliza ambos efectos, directo e indirecto, para producir un comportamiento determinado<sup>37</sup>. Cuando el regulador actúa indirectamente, podemos decir que utiliza o coopta la segunda modalidad de restricción para lograr su fin regulador. Así por ejemplo, cuando el dere-

cho ordena un cambio en la arquitectura, lo hace para utilizar la arquitectura como medio para un fin. La arquitectura se transforma en una herramienta del derecho cuando la sola acción directa del derecho no sería suficientemente efectiva.

Cualquier ejemplo dejará claro el punto uno, sin embargo, bastará.

2. *Fumar y la imagen de la regulación moderna.* Supongamos que el gobierno busca reducir el consumo de cigarrillos. Hay numerosas maneras por las cuales el gobierno podría lograr esta meta. El derecho podría, por ejemplo, prohibir fumar<sup>38</sup>. (Esto sería el derecho regulando directamente el comportamiento que desea cambiar.). O el derecho podría aumentar los impuestos a los cigarrillos<sup>39</sup>. (Esto sería el derecho regulando el suministro de cigarrillos en el mercado, para disminuir su consumo). O el derecho podría financiar una campaña en contra de fumar<sup>40</sup>. (Esta sería el derecho regulando las normas sociales, como un medio para regular la conducta de los fumadores). O el derecho podría regular el contenido de nicotina en los cigarrillos, solicitando a los productores que reduzcan o eliminen la nicotina<sup>41</sup>. (Esto sería el derecho regulando la "arquitectura" de los cigarrillos como una forma de reducir su efecto adictivo y por consiguiente reducir su consumo). De cada acción se puede esperar algún efecto (llamémoslo su beneficio) en el consumo de cigarrillos; asimismo, cada acción tiene su costo. La pregunta en cada caso es si el costo supera el beneficio. Si, por ejemplo, el costo de la educación para cambiar las normas sociales acerca de fumar fuera el mismo que el costo de cambios en la arquitectura, el valor que le damos a la autonomía y la elección individual podría inclinar la balanza en favor de la educación.

Esta es la imagen de la regulación moderna. El regulador siempre está haciendo una elección, considerando que estas cuatro modalidades de regulación pueden ser utilizadas directamente, acerca de si usar o no el derecho directa o indirectamente con el objetivo de alcanzar una meta normativa. No se trata de una elección binaria; el derecho no escoge una estrategia en lugar de otra, siempre se escoge una mezcla de estrategias directas e indirectas. La pregunta que el regulador siempre debe hacerse es: *¿Cuál combinación es la óptima?*

La respuesta va a depender del contexto de la regulación. En una comunidad pequeña y densa, las normas sociales pueden ser el modo más óptimo de regulación; a medida que una comunidad se vuelve más dispersa, el derecho o el mercado pueden ser los segundos mejores substitutes. En la Europa del siglo décimo, regular a través de apremios arquitectónicos puede haber sido un poco difícil, pero en la época de la construcción de modernos edificios de oficinas, la arquitectura se vuelve una técnica regulatoria factible y bastante eficaz (piense en un cubículo transparente como una forma de vigilar el comportamiento). La mezcla óptima depende de la plasticidad de las diferentes modalidades. Por

supuesto que el método que funcione en un contexto no necesariamente va a funcionar en todas partes. Pero dentro de un contexto en particular podemos inferir que ciertas modalidades van a predominar.

Yo sugiero que este es el caso en el ciberespacio. Como lo describo más extensamente en la sección que sigue, la manera más efectiva de regular el comportamiento en el ciberespacio será a través de la regulación de código, regulación directa ya sea del código del ciberespacio en sí mismo, o de las instituciones (escritores de códigos) que producen el código. Sujetos a una calificación cada vez más exigente<sup>42</sup>, debemos esperar que, con el tiempo, los reguladores se concentren más intensamente sobre este código<sup>43</sup>.

Mi objetivo en las próximas dos secciones es explorar con mayor profundidad esta dinámica. Espero mostrar (1) que el gobierno puede regular el comportamiento en el ciberespacio (a pesar de los eslóganes existentes sobre la imposibilidad de regular el ciberespacio); (2) que el modo óptimo de regulación gubernamental será diferente cuando controle el comportamiento en el ciberespacio, y (3) que esta diferencia planteará la pregunta urgente que aún debe ser respondida por el derecho constitucional. (¿Qué límites deben haber sobre la regulación indirecta? ¿Hasta dónde podemos permitir que el derecho coopte a las otras modalidades de restricción?).

## II. Interacciones: derecho y arquitectura

### A. *El derecho domesticando al código: incrementando la regulabilidad del ciberespacio*

He advertido anteriormente la percepción general sobre la imposibilidad de regular el ciberespacio; que su naturaleza lo hace así y esa naturaleza está fija. Argumenté que si el ciberespacio puede ser regulado o no, no es algo que dependa de su naturaleza, sino que de su arquitectura o su código<sup>44</sup>. Es decir, su *regulabilidad* es una función de su diseño. Hay diseños en los cuales el comportamiento dentro de la Red esta al total alcance del gobierno. Mi argumento en esta sección es que el gobierno puede adoptar medidas para alterar el diseño de Internet.

Ofrezco dos ejemplos que, en conjunto, deberían ilustrar mejor la idea general.

1. *Aumentando la regulación colectiva: sectorización.* Volvamos al problema de la sectorización de la sección I. Mi argumento era que en el espacio real las características que presenta un niño hacen posible que el cumplimiento de las reglas sobre acceso sean exigidas coactivamente, mientras que en el ciberespacio, donde la edad no es autoautentificante, su exigibilidad resulta difícil.

Una respuesta sería hacer que la identidad se autoautenticara por medio de una modificación en el código de la Red. De esta manera, cada vez que me conectara a un sitio de Internet, información acerca de mí sería transmitida a ese sitio. Esta transmisión permitiría a los sitios en la Red determinar si, dadas mis características, se me puede permitir el acceso.

¿Cómo?

En algún sentido, la Red ya facilita algunas formas de identificación. Un servidor, por ejemplo, puede determinar si mi navegador es Macintosh o Windows. Estos son ejemplos de autoautenticación que se encuentran dentro del código de la Red (o http) actualmente.

Otro ejemplo es la "dirección" del usuario. Cada usuario de Internet tiene, por el periodo de tiempo que esté en la Red, una dirección, conocida como Protocolo de Internet (IP)<sup>45</sup>. Esta dirección IP es única, es de uso exclusivo de esa máquina por ese periodo de tiempo. Las aplicaciones utilizan esta dirección para saber dónde enviar los paquetes de información solicitados en la Red. Sin embargo, mientras estas direcciones son únicas, no existe necesariamente unión entre una dirección y una persona. Aunque algunas máquinas tienen IP "estáticos", es decir, asignado permanente a esa máquina, muchas tienen IP "dinámicos" que se asignan solamente para una sesión y pueden cambiar cuando la máquina vuelva a conectarse a Internet. Así, aunque se revela una cierta información cuando la máquina está en la Red, Internet no requiere actualmente ninguna autenticación más allá de una dirección IP.

Otras redes son diferentes. Las *Intranets*<sup>46</sup>, por ejemplo, son redes que se conectan a Internet. Estas redes funcionan con los protocolos básicos de Internet, pero sobre estos protocolos adjuntan otros protocolos. Entre estos últimos, hay protocolos que permiten la identificación del perfil de un usuario por parte del controlador de Intranet. Es decir, tales protocolos permiten una forma de autoautenticación que facilita la identificación. El alcance de esta identificación varía. En un extremo están las técnicas biométricas que vinculan alguna característica física del usuario (huella digital o scanner del ojo) a una identidad (ID), identificando así específicamente al usuario. En el otro extremo están los certificados que simplemente identifican las características de una persona, que es mayor de dieciocho, que es una ciudadana americana, etc.

Está más allá del alcance de este ensayo hacer un bosquejo de la gama completa de estas tecnologías. Mi objetivo es mucho más limitado. Es suficiente mostrar aquí que la identificación es posible, para después explicar cómo el gobierno puede actuar para facilitar el uso de estas tecnologías.

Mi afirmación en esta sección es la siguiente: si estas tecnologías de la identificación fueran de uso general en Internet, la posibilidad de regular el comportamiento en el ciberespacio aumentaría, y el gobierno puede afectar la generalidad del uso de estas tecnologías.

Concentrémonos ahora en el asunto de proteger a los niños de las expresiones para adultos en la red<sup>47</sup>. Hasta la fecha, el Congreso ha intentado dos veces promulgar legislación que regularía la disponibilidad de estas expresiones para los "menores"<sup>48</sup>. Al tiempo de escribir este ensayo, el Congreso ha fallado las dos veces<sup>49</sup>. En ambos casos su fracaso fue producto de cierta torpeza en la ejecución. En el primer caso, el Congreso intentó regular de una manera demasiado amplia; en el segundo, corrigió ese problema, pero agobió a la clase incorrecta de usuarios: los adultos<sup>50</sup>.

Considere una tercera alternativa, que en mi opinión no produciría el mismo nivel de problemática constitucional<sup>51</sup>. Imagine el siguiente estatuto:

1. *Modalidad infantil de navegación.* (Kids-Mode-Browsing o KMB). Los fabricantes de navegadores permitirán a sus respectivos softwares de navegación funcionar en "Modalidad Infantil" [KMB]. Al ser activado, KMB señalará a los servidores que el usuario es un menor de edad. El software del navegador debe permitir la protección de contraseña de paso para la Modalidad-No-Infantil de búsqueda. El navegador debe también impedir cualquier recolección de datos sobre el usuario de un navegador en modalidad infantil. Más precisamente, no transmitirá a ningún sitio datos personales que identifiquen al usuario.
2. *Responsabilidad del servidor.* Cuando un servidor detecta a cliente de KMB, deberá (1) bloquear el acceso del cliente hacia cualquier material considerado como propiamente "dañino para menores de edad"<sup>52</sup> y (2) abstenerse de recoger cualesquiera datos personales que identifiquen al usuario, excepto los datos necesarios para procesar peticiones del propio usuario. Cualesquiera datos recogidos serán purgados del sistema dentro de X días.

A pesar de la retórica sobre la imposibilidad de regular el ciberespacio, nótese lo simple que sería implementar y reforzar estas normativas. En un mundo en el cual el noventa por ciento de los navegadores son fabricados por dos compañías<sup>53</sup>, los autores de los códigos son demasiado prominentes para pasar desapercibidos. Y de todos modos por qué esconderse; dada la simplicidad del requisito, su cumplimiento sería sencillo. En un tiempo muy corto dicha ley produciría navegadores con la característica de KMB por lo menos para aquellos padres que desean tal control en los computadores de su hogar.

Asimismo, sería fácil que los sitios desarrollen software para bloquear el acceso si el usuario señala que él/ella es un niño. Tal sistema no requeriría ninguna identificación costosa, ninguna base de datos de identidad y ninguna tarjeta de crédito. En cambio, el servidor sería programado para validar a los usuarios que no tienen seleccionada la Modalidad Infantil y rechazar a los usuarios que sí la tienen.

Mi punto no es endosar tal legislación: pienso que la respuesta ideal para el Congreso es no hacer nada. Pero si el Congreso adoptara esta forma de regulación, mi opinión es que sería factible y constitucional. Netscape y Microsoft no tendrían ninguna objeción viable según la Primera Enmienda a una regulación de su código<sup>54</sup>; y los sitios Web no tendrían ninguna objeción constitucional ante el requisito de bloquear a los usuarios en Modalidad Infantil<sup>55</sup>. Nunca, en un caso, se ha sostenido que un individuo tiene derecho a no ser sujeto de ninguna carga si la carga es necesaria para procurar la satisfacción de una necesidad del Estado; el único requisito de *Reno v. ACLU*<sup>56</sup> es que dicha carga sea la carga menos restrictiva<sup>57</sup>. Yo sugiero que la carga de KMB sería la menos restrictiva.

El sistema KMB sería relativamente efectivo<sup>58</sup>. Imagínese que el FBI activase un bot para examinar (spider) la Red, con la configuración del navegador de KMB funcionando. El bot intentaría acceder a los sitios; si consiguiera el acceso, reportaría al investigador tanto del contenido como le fuese posible extraer. Este contenido podría entonces ser analizado; y el contenido que pudiese ser considerado para adultos entonces sería devuelto al investigador, quien determinaría si estos sitios eran "sitios para adultos"; y si lo fuesen, procedería una investigación contra estos sitios. El resultado sería un sistema extremadamente eficaz para vigilar el acceso al contenido para adultos en la Web. COPA, por lo tanto, debe ser declarada inconstitucional, ya que es posible una alternativa menos restrictiva que cumple con los mismos objetivos.

Para los propósitos de sectorizar el material para adultos, este cambio alteraría fundamentalmente la posibilidad de regular la Red, y lo haría no por medio de una regulación directa de los niños, sino que alterando una característica de la "arquitectura"<sup>59</sup> de la Red, la capacidad de un navegador para proveer de cierta información sobre el usuario. Una vez que este recurso fuera incorporado de forma general en los navegadores, la capacidad de los proveedores de material para adultos de discriminar entre los menores y los adultos cambiaría. Esta regulación del código haría así posible la regulación de comportamiento.

2. *Aumentando la regulabilidad individual: privacidad.* La sectorización de la pornografía es un ejemplo de la regulación vertical (top-down regulation). El Estado, probablemente con el apoyo popular, impone una decisión sobre quién puede tener acceso a qué. Impone esa decisión llamando a los codificadores a codificar en conformidad con las reglas del Estado. El Estado necesita imponer estas reglas porque la



arquitectura inicial de la Red impedía la regulación vertical (esto más que un vicio era una virtud podría haber pensado la mayoría. El Estado, sin embargo, probablemente no formaba parte de "la mayoría"). Esta arquitectura interfirió con el control vertical. La respuesta era modificar esa arquitectura.

El problema con la privacidad en el ciberespacio es diferente. La característica de la Red que crea el problema con la privacidad (la recolección invisible y automática de datos) interfiere con la regulación horizontal (bottom-up regulation), esto es, aquella impuesta por los individuos por su propia voluntad.

Las arquitecturas pueden permitir o imposibilitar la opción individual proveyendo (o fallando en proveer) al individuo tanto de la información necesaria para tomar una decisión como de la opción de llevar a cabo dicha decisión. El ejemplo de privacidad se basa en una arquitectura que no permitía las decisiones individuales, escondiendo información necesaria y determinante para dicha elección, imposibilitando, por ende, el control horizontal. La autorregulación, como la regulación estatal, dependen de las arquitecturas de control. Sin esas arquitecturas, ninguna forma de regulación es posible.

Pero, una vez más, las arquitecturas pueden ser modificadas. Así como con la sectorización de la pornografía, las arquitecturas que invalidan la autorregulación están sujetas a decisiones colectivas. El gobierno puede actuar para imponer un cambio en el código, haciendo la autorregulación menos costosa, y por consiguiente facilitando su expansión.

En este caso, sin embargo, la técnica para imponer este cambio es una herramienta tradicional del derecho. El problema de proteger la privacidad en el ciberespacio viene, en parte, de la arquitectura que permite la recolección de datos sin el consentimiento del usuario<sup>60</sup>. Pero el problema viene también de un régimen de titularidades de fondo que no exige al recolector obtener el consentimiento del usuario. Como el usuario no tiene un derecho de propiedad sobre su información personal, esta queda disponible en forma gratuita para tomarla. De esta manera, las arquitecturas que permiten el uso de esa información personal son eficientes para el recolector, y consistentes con el régimen legal.

El truco sería cambiar los derechos legales de una manera suficiente como para cambiar los incentivos de los que construyen las tecnologías del consentimiento. El Estado podría (1) dar a los individuos un derecho de propiedad sobre sus datos personales, y (2) crear un incentivo para los creadores de sistemas con el objetivo que faciliten a la persona el prestar su consentimiento antes de traspasar los datos<sup>61</sup>.

El primer paso viene a través de una declaración por parte del Estado sobre quién es dueño de qué<sup>62</sup>. El gobierno podría declarar que la información personal obtenida a través de una red computacional es de propiedad de los individuos; otros podrían tomar esa información, y

usarla solo con la autorización de dichos individuos. Esta declaración de derechos podría ser protegida y hecha efectiva a través de numerosos medios tradicionales. El Estado podría considerar como criminal el hurto de dicha información, o podría proveer a los afectados de acciones civiles especiales e incentivos civiles para hacer cumplir los derechos individuales en aquellos casos en que se recolecte esta información.

Este primer paso, sin embargo, solamente sería útil si indujera a la segunda medida; esta vez, un cambio en la arquitectura del espacio, y no tan solo en las leyes que gobiernan ese espacio. Este cambio en la arquitectura apuntaría a reducir los costos de elección, a facilitar a los individuos la expresión de sus preferencias en cuanto al uso de datos personales, y facilitaría las negociaciones acerca de esa información. Los regímenes de propiedad tienen poco sentido a menos que las transacciones que involucra esa propiedad sean sencillas y expeditas, y un problema con las arquitecturas existentes, nuevamente, es que es difícil para los individuos tomar decisiones sobre su propiedad.

Pero hay soluciones. El consorcio de la "World Wide Web", por ejemplo, ha desarrollado un protocolo, llamado P3P<sup>63</sup>, para el control de la información privada. P3P puede permitir a los individuos seleccionar sus preferencias acerca del intercambio de información privada, y después habilitarlos para negociar el intercambio de dicha información cuando alguien se conecta a un determinado sitio. Si, por ejemplo, no quiero visitar nunca un sitio que grabe mi dirección IP y las páginas que he visitado, P3P podrá indicar esta preferencia. Cuando visite un sitio Web, un agente negociaría con el sitio mis preferencias de acceso.

P3P funciona como un lenguaje para expresar las preferencias sobre la información, y como un marco de trabajo para facilitar las negociaciones sobre dichas preferencias. Es decir, sería un marco dentro del cual los individuos podrían regular mejor sus vidas en el ciberespacio<sup>64</sup>.

No obstante lo anterior, sin la intervención de Estado, no está claro que tal marco pueda desarrollarse. P3P crea cargas que los sitios Web no asumirán en un mundo donde pueden conseguir la misma información de manera libre. Únicamente cambiando los incentivos de estos sitios —denegándoles el acceso gratuito a la información— podemos esperar crear un incentivo suficiente para que los sitios adopten las tecnologías que faciliten las transacciones. Establecer derechos de propiedad sobre los datos privados crearía tal incentivo; y es el gobierno quien entonces facilita este interés.

Hay muchos problemas con P3P, y hay alternativas que pueden funcionar mucho mejor<sup>65</sup>. Pero mi propósito no ha sido adherir a una solución determinada. Mi propósito ha sido mostrar la posible necesidad de una acción colectiva, aunque sea solamente para permitir el control individual. La arquitectura existente inhibe los incentivos necesarios para proteger la privacidad; la arquitectura existente beneficia a los consumidores de información privada y obstaculiza la posibilidad de elección de



los sujetos sobre si proveer o no su información privada. El éxito de una política que permita este cambio requerirá por lo tanto de la acción colectiva.

\* \* \*

3. *Conclusiones respecto de la arquitectura y la regulabilidad.* Las regulaciones pueden provenir desde cualquier dirección, algunas desde arriba [verticales] y otras desde abajo [horizontales]. Mi argumento en esta sección ha sido que la regulabilidad de ambas formas depende de la arquitectura del espacio y esta arquitectura puede ser modificada.

El código del ciberespacio puede inhibir la opción del gobierno, pero la arquitectura puede inhibir también la opción de los individuos. No existe una alineación general y natural entre la regulación horizontal y la arquitectura existente de Internet. Permitir la opción *individual* podría requerir la modificación colectiva de la arquitectura del ciberespacio; a su turno, permitir la opción *colectiva* también podría requerir la modificación de esta arquitectura. La arquitectura del ciberespacio es neutral; puede permitir o impedir cualquiera de estas opciones. La opción sobre cuál permitir, sin embargo, no es neutral en ningún sentido.

## **B. El código desplazando al derecho**

Hasta aquí el argumento es que el derecho puede modificar las restricciones del código. De esta manera, el código puede regular la conducta en una forma diferente. En esta sección considero la situación inversa, es decir, que el código puede modificar las restricciones del derecho, de esta manera el derecho podría (en efecto) regular en forma diferente. La clave aquí es la frase calificativa *en efecto*, toda vez que en mis ejemplos el código no consigue un cambio real en el derecho. El derecho continúa igual en los libros. Los siguientes ejemplos, en cambio, refieren al código modificando la efectividad del derecho. En otras palabras, se trata de ejemplos acerca de cómo los efectos indirectos del código pueden alterar la regulación o las políticas legales.

En estos casos los legisladores enfrentan un desafío. Donde las arquitecturas del código modifican las restricciones del derecho, ellas, en efecto, desplazan los valores contenidos en la regulación. Los legisladores tendrán que decidir por lo tanto si reforzar estos valores existentes o permitir que la modificación tenga lugar. En los ejemplos que he seleccionado aquí, mis preferencias se encuentran a favor de los valores que contiene el derecho, aunque también existen muchos ejemplos para encaminarse en un sentido diverso. Mi punto no es que siempre debamos utilizar al derecho; con frecuencia el mercado será suficiente. Lo que me interesa es únicamente mostrar por qué el derecho, a veces, debe ser utilizado.

He extraído mis ejemplos de la regulación de la propiedad intelectual y del derecho contractual. En ambos casos identifico valores públicos que son desplazados por las arquitecturas emergentes del ciberespacio. Argumento que estas arquitecturas posibilitan un sistema de protección de la propiedad intelectual que funciona demasiado perfectamente e inhibe la influencia del derecho público en los contratos. El código en estos ejemplos amenaza con desplazar valores públicos contenidos en esas regulaciones, forzando de esta manera a una opción sobre si permitir o no este potencial desplazamiento.

1. *El código desplazando al derecho: propiedad intelectual.* Tenemos leyes especiales para protegernos contra el hurto de autos o botes<sup>66</sup>. No disponemos, sin embargo, de leyes especiales para protegernos del hurto de rascacielos. Los rascacielos se cuidan ellos mismos. La arquitectura del espacio real, o más sugerentemente, el código del espacio real, protege a los rascacielos en forma más efectiva que el derecho. La arquitectura es una aliada de los rascacielos (haciendo imposible moverlos); y es una enemiga de los autos y botes (haciendo demasiado fácil su desplazamiento).

En el espectro que abarca desde los botes a los enormes edificios, la propiedad intelectual es algo parecido a los botes y muy distinta a los grandes rascacielos. En efecto, así como es el mundo actualmente, la propiedad intelectual anda bastante peor que los autos o botes. Si alguien toma mi auto, al menos yo lo advertiría. En ese caso puedo llamar a la policía y ellos tratarán de encontrarlo. Sin embargo, si alguien hace una copia ilegal de mi artículo (copiándolo sin pagar por ello), yo no necesariamente me enteraría. Las ventas pueden disminuir, mi reputación puede aumentar (o disminuir), pero no hay forma de vincular directamente la caída en las ventas a este hurto individual ni forma de explicar el aumento (o descenso) de mi fama a través de esta distribución subsidiada.

Cuando los teóricos de la Red comenzaron a pensar sobre la propiedad intelectual, ellos argumentaron que las cosas irían mucho peor. "Todo lo que nos han dicho acerca de la propiedad intelectual está equivocado"<sup>67</sup>. La propiedad no puede ser controlada en la Red; los derechos de autor no tienen sentido<sup>68</sup>. Los autores tendrían que encontrar otras formas de hacer dinero en el ciberespacio toda vez que la tecnología había destruido la posibilidad de hacer dinero a través del control de las copias<sup>69</sup>.

Las razones eran sencillas: la Red es un medio digital. Las copias digitales son perfectas y gratuitas<sup>70</sup>. Uno puede copiar una canción de un CD a un formato llamado MP3. La canción puede ser puesta en USENET para millones de personas en forma gratuita. La naturaleza de la Red, nos dijeron, hacía el control de los derechos de autor imposible. Los derechos de autor estaban muertos.

Hubo algo extraño acerca de este argumento, aun en sus comienzos. El argumento traicionó una cierta diferencia entre lo que es y lo que puede ser (is-ism); "de la forma que es el ciberespacio, es la forma que tiene que ser". El ciberespacio era un lugar donde "un número infinito de copias podían ser hechas en forma gratuita". Pero ¿por qué exactamente? Por su código. Un número infinito de copias podía ser realizado porque el código permitía dicho proceso. Pero entonces, ¿por qué no podía ser cambiado el código? ¿Por qué no podríamos imaginarnos un código diferente, uno que protegiera mejor la propiedad intelectual?

Imaginar estos códigos alternativos requirió una gran cantidad de imaginación al comienzo de este debate. No resultaba obvio que una arquitectura alternativa pudiera permitir mayor control sobre los objetos digitales. Sin embargo, ahora estamos lo suficientemente avanzados como para ver algunas de esas alternativas<sup>71</sup>.

Considere las proposiciones de Mark Stefik de Xerox PARC. En una serie de artículos<sup>72</sup>, Stefik describe lo que él denomina "sistemas de confianza" (trusted systems) para la administración de los derechos de autor. Los sistemas de confianza permiten a los propietarios de propiedad intelectual controlar el acceso a esa propiedad y mensurar perfectamente el uso de dicha propiedad. Este control sería codificado en el software a través del que se distribuiría la propiedad y, por lo tanto, regularía el acceso a material protegido por derechos de propiedad intelectual. Este control sería extremadamente acucioso y permitiría a los propietarios un control extraordinario sobre su material protegido por derechos de propiedad intelectual.

Piense en esto de la siguiente forma: Actualmente, cuando usted compra un libro, usted tiene el "derecho" de hacer casi cualquier cosa con ese libro, puede leerlo una o cien veces, puede prestárselo a un amigo, puede fotocopiar sus páginas o escanearlo en su computador, puede quemarlo, puede utilizarlo como pisapapeles, puede venderlo, puede guardarlo en un estante y no abrirlo siquiera una vez.

Algunas de estas cosas las puede hacer porque la ley le da el derecho de hacerlas: usted puede vender el libro porque la ley de propiedad intelectual explícitamente le concede ese derecho<sup>73</sup>. Algunas de estas cosas las puede hacer porque realmente no existe forma de impedírselo. Un vendedor de libros puede venderle el libro a un precio determinado si usted promete leerlo solo una vez, y a un precio distinto si usted quiere leerlo cien veces. Sin embargo, no existe forma en que el vendedor realmente sepa si usted lo leyó una o cien veces, y, así, no hay forma en que el vendedor sepa si usted cumplió o no el contrato. En principio, el vendedor podría incluir un oficial de policía con cada libro, de esta manera el oficial lo seguiría a usted adonde fuera, asegurándose que utilizara el libro de acuerdo a los términos convenidos en el contrato. Sin embargo, los costos de esto serían francamente prohibitivos. El vendedor está atrapado.

¿Pero qué sucedería si cada uno de estos derechos pudiera ser controlado y cada uno de estos derechos pudiese ser individualizado y vendido por separado? ¿Qué pasaría si se pudiera regular si usted lee un libro una o cien veces; si usted copia algo del libro; o simplemente si lo lee sin copiarlo; si usted lo envía adjunto como documento a un amigo; o simplemente lo conserva en su computador; si usted lo borra; si usted lo utiliza en otro trabajo; o si simplemente lo deja en su estante?

Stefik describe una red (network) donde esta individualización de derechos resulta posible. Él ofrece una arquitectura para esta red que permitiría a los propietarios de material protegido por derechos de autor vender el acceso a dichos materiales en los términos que ellos mismos fijen y una arquitectura que hace posible la exigibilidad de estos contratos.

Los detalles de estos sistemas no son importantes aquí<sup>74</sup>. La esencia del asunto es suficientemente sencilla para entenderla. Los objetos digitales podrían ser distribuidos a través de protocolos que se encuentran instalados (layered) sobre los protocolos básicos de la Red. Estos sistemas más sofisticados funcionarían interactuando selectivamente con otros sistemas. De esta manera, un sistema que controla el acceso en esta manera más cuidadosa, únicamente permitiría el acceso de otros sistemas que controlaran el acceso de una manera igualmente cuidadosa. Así se desarrollaría una jerarquía de sistemas y el material protegido por derechos de autor sería comercializado únicamente a través de aquellos sistemas que controlaran idóneamente el acceso.

Stefik ha transformado aeroplanos en rascacielos —él ha descrito una forma para cambiar el código del ciberespacio y hacer posible la protección de la propiedad intelectual en un modo mucho más efectivo de lo que resulta posible en el espacio real.

Imagine ahora por un momento el surgimiento de una estructura de sistemas de confianza. ¿Cómo afectaría la naturaleza de la regulación de los derechos de autor este cambio en el código?

Los derechos de autor son un bicho raro. Establecen una extraña clase de propiedad, al menos en relación con otros tipos de propiedad. La Cláusula de los Derechos de Autor de la Constitución de los Estados Unidos da al Congreso el poder de otorgar a los "Autores" un derecho exclusivo sobre sus "Obras" por "Tiempos limitados"<sup>75</sup>. Concluido este tiempo, el derecho se transforma en no exclusivo. El trabajo ingresa al dominio público. Es como si el dominio que usted tiene sobre su auto equivaliera a los derechos derivados de un contrato de arrendamiento (lease) que se extendiera por cuatro años y luego expirara; una vez concluido, su auto quedaría a disposición del público.

Las razones para esta limitación a la protección de los derechos de autor son muchas, sin embargo, no se superponen completamente. Algunas de ellas son económicas y, en última instancia, pragmáticas. Los sistemas de propiedad (costosos y complejos) se justifican solamente si

producen algún bienestar social. En el caso de los bienes tangibles, el bienestar social es obvio. El derecho protege mi goce de la propiedad tangible, por ejemplo mi auto. Si usted usa mi auto sin permiso, yo no puedo usarlo. Si cualquiera pudiese usarlo sin mi autorización, existirían pocas razones para que me interesara en ser el propietario del auto. Asignándome el poder de controlar el uso de mi auto, el derecho adjunta un beneficio a mi propiedad y, por lo tanto, un incentivo para desear esa propiedad.

La propiedad intangible difiere significativamente. A diferencia del goce de mi auto, el goce de su poema no interfiere en ningún sentido en que yo también lo disfrute. Los bienes intangibles son no rivales. Cuando una idea es divulgada, su utilidad no disminuye. Como escribió Thomas Jefferson: "[N]adie posee el mínimo, porque todo los demás poseen el total. Aquel que recibe una idea de mí, recibe conocimiento sin debilitar el mío; tal como aquel que enciende su vela recibe luz sin oscurecerme"<sup>76</sup>. De esta manera, mientras el derecho necesita proteger la propiedad tangible por dos razones, para que exista un incentivo para producir y también para que el propietario pueda disfrutarla, el derecho únicamente necesita proteger la propiedad intangible con el solo objeto de crear incentivos para producirla.

Sin embargo, las razones económicas no constituyen la única justificación para limitar las protecciones "como si fuera propiedad" (propertylike) de la propiedad intelectual. El derecho constitucional es otra razón<sup>77</sup>. Las regulaciones del derecho de autor son regulaciones de la expresión. Los derechos de autor no solamente dan al autor derecho a controlar las copias exactas, sino además los trabajos derivativos y la ejecución de ciertos trabajos. Estas regulaciones de la expresión están en tensión con la idea que el derecho debería dejar a la expresión libre. En el caso de un derecho de autor restringido existe un compromiso que alivia esta tensión; se otorga protección al trabajo que cae bajo la esfera del derecho de autor en términos que provea incentivos para crear, pero no más. Como la Corte Suprema ha sostenido en *Harper & Row, Publishers Inc. v. Nation Enterprises*<sup>78</sup>, los constituyentes (Framers) imaginaron a los derechos de autor como un "motor de la libre expresión"<sup>79</sup>. Por lo tanto, estos derechos están justificados solo en la medida que cumplan con esta misión.

Finalmente, y relacionado con lo anterior, los límites de la propiedad intelectual reflejan un compromiso con los bienes comunes intelectuales (intellectual commons)<sup>80</sup>. Es verdad que algunos bienes comunes enfrentan tragedias<sup>81</sup>, sin embargo, una vez que el problema de los incentivos es solucionado, los bienes comunes ya no se enfrentan a estas tragedias. Las limitaciones en el enfoque de la ley de propiedad intelectual sirven para estimular los bienes comunes intelectuales, para generar un recurso sobre el cual otros puedan trabajar<sup>82</sup>.



La naturaleza esencial de los comunes es que cada individuo es libre de usarlos sin la autorización de ningún otro<sup>83</sup>. Desde una perspectiva más acotada, se trata de un bien común si el usuario es libre respecto a cualquier decisión sobre si el bien puede o no ser utilizado, ya sea que la decisión esté basada en el contenido, en un punto de vista cualquiera, o simplemente en la discreción. Yo puedo tener que pagar un pequeño precio por ingresar a un parque, pero si lo pago, tengo el derecho a ingresar. El parque es un recurso abierto para cualquiera. Es un espacio que los sujetos pueden utilizar sin pedir autorización a nadie<sup>84</sup>.

Estas tres justificaciones para limitar la propiedad intelectual se superponen, pero no son coextensivas. Todas ellas, por ejemplo, justificarían algún tipo de "uso justo" (fair use), una defensa que la ley de los derechos de autor da a los usuarios de material protegido por derechos de autor<sup>85</sup>.

Desde una perspectiva económica, el uso justo puede ser justificado o porque este tipo de uso es reducido con relación a los costos de cobrar por su utilización, o bien porque generalmente ciertos usos tienden a incrementar la demanda por trabajos protegidos por derechos de autor. El derecho a usar extractos de un libro en la crítica literaria beneficia en general a los autores toda vez que permite el comentario de dichos libros que, a su turno, incrementa la demanda total por esos libros<sup>86</sup>.

Desde la perspectiva de la libertad de expresión, lograr una justificación para el uso justo dependerá del tipo de discurso que se trate. Melville Nimmer, por ejemplo, sugiere un caso hipotético en el cual los intereses protegidos por la Primera Enmienda justificarían el uso justo más allá de los márgenes fijados por los derechos de autor<sup>87</sup>.

Sin embargo, desde la perspectiva de los comunes, lo que resulta relevante respecto del uso justo no es tanto el valor del uso justo o su relación con asuntos de importancia pública. Lo que es importante es el derecho a utilizarlos sin autorización. Esta es una concepción de la autonomía. El derecho garantizado es el derecho a utilizar estos recursos sin la autorización de nadie<sup>88</sup>.

De esta manera, el "uso justo" equilibra los derechos del autor individual y los derechos del usuario bajo cualquiera de las justificaciones de la ley del derecho de autor. Sin embargo, una vez más, resulta claro que, sin perjuicio de la justificación, el desarrollo de los sistemas de confianza amenaza con alterar este balance. Desde una perspectiva económica, amenaza con dar poder a los autores individuales contra los intereses de los usuarios; desde una perspectiva constitucional, amenaza con enclaustrar (bottle-up) la expresión sin perjuicio de su relación con asuntos de interés público; y desde la perspectiva de los comunes, altera fundamentalmente la naturaleza del acceso.

En la estructura de los sistemas de confianza, el acceso es posible únicamente a través de su autorización. La base de estos sistemas es el control, sin que resulte relevante cuánto se utilice este control.

Este es un problema particular del ciberespacio. En el espacio real, el ordenamiento jurídico puede garantizarme el derecho al uso justo, o a utilizar un trabajo que se encuentra en el dominio público. El ordenamiento jurídico me garantiza este derecho dándome una defensa si el dueño de la propiedad intelectual intenta demandarme por tomar su propiedad. El ordenamiento jurídico, en efecto, deniega al dueño cualquier curso de acción; la ley le retira su protección y deja su propiedad en el dominio común.

No existe, sin embargo, una garantía similar con la propiedad protegida por sistemas de confianza<sup>89</sup>. No hay razón para pensar que el código que describe Stefik será un código que garantice el uso justo o un periodo de tiempo limitado. Por el contrario, el código de los sistemas de confianza podría proteger absoluta e indefinidamente<sup>90</sup> la propiedad intelectual. El código no necesita ser equilibrado en el sentido que los derechos de autor lo son. El código puede ser configurado como lo desee su diseñador y los diseñadores de código poseen escasos incentivos para hacer sus productos imperfectos<sup>91</sup>.

De esta manera, los sistemas de confianza son formas de derecho privatizado. Son arquitecturas de control que desplazan las arquitecturas de control contenidas en el derecho público. Y en la medida que las arquitecturas del derecho equilibran los intereses públicos y privados, debemos preocuparnos si ellas son desplazadas por otras que respetan los intereses individuales en desmedro de los públicos.

Es imposible predecir en abstracto si este será el resultado de los sistemas de confianza. Existen buenas razones para esperarlo y poca base para sugerir lo contrario. Sin embargo, mi intención aquí no es predecir, sino aislar una respuesta: Si la ley privatizada desplaza los valores públicos, ¿debería la gente hacer algo?

2. *El código desplazando al derecho: "contratos"*. Los sistemas de confianza son un ejemplo del código desplazando al derecho. Un segundo ejemplo es el derecho contractual. Ha existido una gran cantidad de posturas en la literatura del ciberespacio acerca de que el ciberespacio es un lugar en que será el "contrato" más que la "ley" lo que gobernará la conducta de los individuos<sup>92</sup>. AOL, por ejemplo, lo obliga a ingresar su nombre cada vez que usted entra a su sistema. Los teóricos dicen que esto es "como" un contrato<sup>93</sup>, toda vez que usted queda vinculado por un conjunto de restricciones acordadas cuando firma con AOL por el servicio. Esto es nada más como si usted prometiera identificarse cuando ingresara a AOL, y cuando no lo hiciera, AOL podría reclamar incumplimiento contractual. Es "como si" pero aun mejor: la obligación es impuesta y su cumplimiento exigido en forma más eficiente que si la obligación fuera impuesta y exigida por el derecho contractual.

Como profesor de derecho contractual, encuentro esta afirmación extraña. Las restricciones impuestas por el código *no* son "contratos". De acuerdo, ellas son "como" contratos en el sentido que son obligacio-

nes autoimpuestas pero de que sean "como" contratos no se sigue que "sean" contratos. Un "león" es como un "gato", pero usted sería bastante torpe si dejara a su hijo jugar con un león. De la misma manera, sería igualmente torpe asumir que los contratos código (code contracts) son igualmente benignos.

La diferencia es esta: en cada contrato susceptible de ser exigido judicialmente —con cada acuerdo cuyo cumplimiento puede ser subsecuentemente exigido a través de la acción de un tercero— existe una decisión tomada por el tercero acerca de si los términos del contrato debieran o no ser exigidos. En general<sup>94</sup>, estas decisiones son tomadas por un tribunal. Y cuando los tribunales toman estas decisiones, consideran no solamente la regulación privada configurada a través del acuerdo, sino además razones de interés público que, en algunas situaciones, pueden sobrepasar estos esquemas de regulación privada. Cuando un tribunal declara la exigibilidad del acuerdo, decide hasta dónde debe utilizarse el poder de los tribunales para llevar adelante un acuerdo. En ocasiones, los acuerdos serán completamente exigibles; sin embargo, frecuentemente, la decisión implicará que no todos los términos del acuerdo sean exigibles. Doctrinas como la imposibilidad o el error dejarán sin efecto ciertas obligaciones. Las reglas sobre las acciones judiciales (remedies) limitarán las acciones judiciales que las partes puedan utilizar. Excepciones basadas en consideraciones de orden público condicionarán las clases de acuerdos que pueden ser legalmente exigidos. Los "contratos" incorporan todas estas doctrinas y es la mezcla de estos valores públicos y obligaciones privadas las que combinadas producen aquello que denominamos "contrato".

Sin embargo, cuando lo que torna exigible un contrato es el código, o cuando el código contiene una restricción autoimpuesta, estos valores públicos no necesariamente ingresan a la combinación<sup>95</sup>. Consecuencias que un tribunal podría resistir (confiscaciones por ejemplo<sup>96</sup>), pueden ser impuestas de manera irrestricta por el código. Quien escribe el código opera libre de todas las limitaciones implícitas en el derecho contractual. Él o ella pueden construir un régimen alternativo de exigibilidad de las restricciones voluntarias. Nada requiere o asegura que este régimen alternativo será compatible con los valores de aquel régimen de fondo (background regime) que denominamos "contrato".

Esto no significa necesariamente criticar las restricciones autoimpuestas del código. Muchas de ellas son, sin duda, inofensivas; y muchas serían exigibles si se trasladaran al espacio real.

Esto, sin embargo, es resistirse a la implicación contraria, que estas obligaciones son "como" los contratos, por lo tanto son inmunes al cuestionamiento como sus obligaciones equivalentes del mundo real constituidas a través de un contrato.

Una vez más, en el espacio real uno podía pensar que el conjunto de las obligaciones impuestas a través de contratos no eran problemáticas.



Determinadas por leyes antimonopolios, limitadas por principios de equidad, cercadas por las doctrinas del error y la excusa, las obligaciones serían examinadas por un tribunal antes que las restricciones fueran hechas efectivas. Existe un examen estructural de la seguridad de las obligaciones de esta especie, el cual asegura que las obligaciones no irán demasiado lejos. Cuando los tribunales intervienen para exigir el cumplimiento de estas obligaciones, un tribunal dispone de un conjunto de herramientas que el derecho de contratos ha desarrollado para modificar o sortear las obligaciones que de otra manera el derecho de contratos haría exigible.

El ciberespacio no posee una caja de herramientas como la mencionada. Las obligaciones no quedan determinadas por los valores públicos contenidos en el derecho de contratos. Las obligaciones, en cambio, fluyen automáticamente de las estructuras impuestas en el código. Estas estructuras sirven los objetivos privados de quienes escriben los códigos; ellas son una versión privada del derecho de contratos. Pero, como enseñó el realismo jurídico durante una generación, y nosotros siempre parecemos dispuestos a olvidar: el derecho contractual es derecho *público*. Derecho privado público es un oximoron<sup>97</sup>.

En algún sentido, este punto acerca de los contratos es el mismo examinado acerca de los derechos de autor. En ambos contextos, el *derecho* sirve a valores públicos; en ambos contextos se articula un régimen privatizado para establecer una protección relacionada; en ambos contextos deberíamos preguntar si debería permitírsele a este sustituto desplazar valores públicos.

Mi respuesta en cada caso es no. En la medida que estas estructuras del código desplacen valores del derecho de orden público, este posee una razón para intervenir restaurando estos valores públicos. Hacerlo y cómo hacerlo son problemas diferentes. Hasta aquí mi punto ha sido únicamente identificar una razón para hacerlo.

### C. El derecho regulando el código

Mis ejemplos de la sección anterior eran escenarios en los que el código podría desplazar valores contenidos en el derecho. Los ejemplos de esta sección son escenarios más familiares en los que el derecho puede desplazar a los valores contenidos en el código. Los dos conjuntos de ejemplos sugieren un punto más general: las modalidades compiten.

Los valores implícitos en una modalidad dada de regulación, o en una instancia concreta de esa modalidad, pueden competir con los valores en una modalidad diferente de restricción. Esta competencia puede inducir a una respuesta. Como el código desplaza al derecho, el derecho puede responder para reclamar los valores desplazados. Como el derecho regula el código, quienes escriben el código pueden responder para

neutralizar el efecto del derecho<sup>98</sup>. Cada modalidad funciona como una especie de soberanía. Cada soberanía compite con las otras.

Ya he esquematizado un par de ejemplos de esta competencia, existen más ejemplos del derecho regulando el código.

*Telefonía digital:* Cuando la red telefónica se volvió digital, los gobiernos perdieron la importante habilidad de intervenir los teléfonos; la arquitectura de las redes digitales hizo difícil la intervención, pero el gobierno simplemente respondió ordenando una arquitectura diferente, con un diseño diferente<sup>99</sup>.

*Tecnología de audio digital:* DAT es un código que hace copias digitales de audio digital. Estas copias digitales son, en principio, perfectas e ilimitadas. De esta manera, el código hace difícil el control de las copias. El Congreso respondió con regulaciones que requerían que el código limitara el número de copias de serie que pudieren hacerse, y en caso de exceder este límite, bajara la calidad de la copia<sup>100</sup>.

*Antivulneración (anti-circumvention):* Los sistemas de confianza, como los he descrito, son sistemas que permiten el control sobre la distribución de objetos digitales por medio de las tecnologías de encriptación, que hacen difícil el uso desautorizado. Estas, sin embargo, no son perfectas; existe código capaz de vencer dicha encriptación. Así la amenaza de este código es una amenaza al sistema del control. El año pasado, el Congreso respondió a esta amenaza decretando una disposición de antivulneración a través de Digital Millennium Copyright Act<sup>101</sup>. Esta ley convierte en un delito vulnerar algún sistema de protección, aun si el uso del material subyacente no es en sí mismo una violación al derecho de autor<sup>102</sup>.

*V-Chip:* El V-Chip modifica el código de las transmisiones televisivas para facilitar la discriminación *ex ante* de los programas disponibles. Antes del V-Chip, el código de la televisión no era capaz de discriminar automáticamente basándose en el contenido del programa. Este código hacía difícil que los padres ejercieran control sobre lo que sus hijos veían. El Congreso respondió requiriendo el uso de un código de televisión capaz de reconocer, y bloquear, el contenido por medio de estándares generados por la industria<sup>103</sup>.

*Encriptación:* El gobierno ha conducido una larga campaña para limitar el acceso a las tecnologías de encriptación, por temor a que la encriptación haga muy simple el ocultamiento de crímenes. Para enfrentar el problema que presentan los mensajes encriptados de forma indecifrabable, el Congreso ha flirteado con la idea de regular directamente el código de encriptación. En septiembre de 1997, el Comité de la Casa de Comercio (House of Commerce Committee) se quedó corto por un voto, al recomendar una ley que requiriese que las tecnologías de encriptación permitiesen la interceptación y desciframiento de la información protegida por dicha tecnología<sup>104</sup>.

Estos ejemplos muestran que la arquitectura del ciberespacio puede habilitar o inhabilitar los valores implícitos en el derecho. Por su parte, el derecho, actuando sobre la arquitectura del ciberespacio, puede habilitar o inhabilitar los valores implícitos en el código. A medida que una modalidad desplaza a la otra, se puede transformar en una competencia. Los autores del código pueden elaborar un código que desplace al derecho; los autores del derecho pueden responder con leyes que desplacen al código.

El Código de la Costa Este (escrito en Washington, publicado en el U.S. Code) puede así competir con el Código de la Costa Oeste (escrito en Silicon Valley, o en Redmond, publicado en dígitos binarios soldados en plástico). Asimismo, los autores del Código de la Costa Este pueden cooperar con los autores del Código de la Costa Oeste. No está claro a qué código se le debe temer más<sup>105</sup>. El conflicto desplaza los valores en ambas esferas, pero la cooperación también amenaza los valores.

Mi objetivo en este ensayo no es trabajar todo el alcance de esta interrelación<sup>106</sup>, tampoco pretendo predecir qué lado prevalecerá. Mi objetivo aquí es utilizar este recuento como una forma de sugerir las lecciones que pueden aprenderse de un análisis más completo.

Este conflicto entre código y derecho debería llevarnos a considerar principios. Deberíamos pensar de nuevo acerca de los valores que deberían guiar, o restringir, el conflicto entre las autoridades. En la última parte quiero esquematizar dos principios. Estos no son, de ninguna manera, los únicos principios que deben preocuparnos; son simplemente los dos cuyas soluciones posiblemente parecen menos obvias. Y son dos que pueden mostrarnos algo sobre lo que una ley del ciberespacio puede enseñar más generalmente.

### III. LECCIONES

He bosquejado la historia de una competencia inevitable entre un conjunto de valores a los que el derecho aspira, y un conjunto de valores aún existentes dentro de una configuración determinada del código. Mi argumento no ha sido que una persona o institución se encuentre siempre detrás de la defensa completa de estos valores ni que estos sean siempre entendidos en forma consistente. No obstante lo anterior, si los valores son defendidos, pero estos valores no son percibidos completamente, ellos inevitablemente entrarán en conflicto. Este conflicto inducirá a menudo una respuesta, frecuentemente del derecho, y a veces de los arquitectos del código. Mi argumento es que podemos aprender algo de esta respuesta.

En esta sección final, deseo sugerir tres lecciones que surgen de esta competencia. La primera es una lección sobre límites del poder del derecho para regular el código. No solo el comportamiento es más regu-

lable bajo algunas arquitecturas que bajo otras, sino que, además, las arquitecturas en sí mismas pueden ser más o menos regulables. Esta diferencia no es tanto una función del código como del diseño organizacional. Como discutiré más adelante, cómo se *posea* el código afectará si puede o no ser regulado.

Esta lección posee resonancias con un argumento familiar de la filosofía política, aunque aquí debe considerarse el argumento en forma invertida. En la filosofía política, el argumento es que la propiedad es un jaque para el gobierno; en el contexto del ciberespacio, mi propuesta es la contraria.

La segunda lección es sobre la transparencia. La transparencia de las regulaciones ha sido por largo tiempo un valor en regímenes constitucionales. La opción entre la regulación por el derecho y la regulación por código pone gran presión en ese valor. Como otros han observado —y el ciberespacio hará sistemáticamente evidente— la no-transparencia puede ser una ayuda eficaz a la regulación. El ciberespacio hará de la no-transparencia una opción constante.

Finalmente, la tercera lección es sobre la adaptación (*tailoring*). Existen únicamente unos pocos contextos en el derecho constitucional en los cuales el gobierno debe adaptar ajustadamente su regulación para un fin del Estado. Las leyes que protegen la expresión y el *status* son los dos ejemplos primarios. El ciberespacio, sin embargo, hará mucho más evidente la preocupación acerca del alcance de una regulación que, de otra manera, resultaría legítima. La regulación de las arquitecturas es un tema delicado y muy determinante que asemeja la regulación de la creación o modificación del ADN. Como en el caso del ADN, la manipulación imprudente se ramifica.

### **A. Los límites a la regulabilidad**

He argumentado que el ciberespacio no es intrínsecamente irregular; que su regulabilidad es una función de su diseño. Algunos diseños hacen el comportamiento más regulable; otros hacen el comportamiento menos regulable. El gobierno, he dicho, puede influenciar el diseño del ciberespacio de maneras que potencien la capacidad del gobierno de regular.

Hay un límite cada vez más significativo al poder del gobierno para regular. Extrañamente, el poder depende de quién sea el dueño del código. Mientras que el “código de aplicación” del ciberespacio sea privado —en un sentido que describo más abajo—, el poder del gobierno aumentará. Mientras que el código del “espacio de aplicación” del ciberespacio no sea privado, sino poseído por toda la comunidad, el poder del gobierno se verá reducido.

Por privado, me refiero a que el “espacio de aplicación” está desarrollado de la manera en la cual hoy se desarrolla la mayoría del código

comercial. Las compañías de software diseñan este código y lo venden como conjunto completo. El producto que licencian no contiene el código fuente. La licencia no da al usuario el derecho de modificar el código fuente; el producto se vende como es, y se espera que el producto sea utilizado como es. El contenido y la función de la aplicación son fijados por el vendedor; no existe la intención de que el usuario juegue un papel en su diseño. Aunque se distribuye a través de contratos (licencias), este código es efectivamente propiedad del vendedor. El vendedor mantiene un derecho exclusivo sobre su diseño y desarrollo.

La alternativa a este modelo "comercial" es el modelo de desarrollo de software inicialmente defendido por la "Free Software Foundation" y, más recientemente, por el movimiento "Open Source"<sup>107</sup>. En este modelo, el software es distribuido con su fuente. Se les permite a los usuarios modificar esa fuente. Dependiendo de la licencia, pueden tener permiso para usar esa fuente modificada en otras empresas comerciales. Si una característica en particular de una aplicación popular es desagradable, entonces los usuarios de este modelo estarán facultados y podrán — toda vez que el código viene con su fuente— removerla.

Esta forma de organización produce "códigos comunes", códigos que no son de propiedad privada ni de propiedad del Estado, sino de la comunidad<sup>108</sup>. La esencia de los comunes es que ninguna persona en particular ejerce un derecho exclusivo sobre el código. Dentro de los términos fijados por un rango de licencias, cualquiera es libre de tomar este código y desarrollarlo como desee.

Existe una cantidad extraordinaria de literatura acerca de este movimiento de Software Libre (Free Software) o de Fuente Abierta (Open Source)<sup>109</sup>. Mi objetivo aquí es dejar en claro un pequeño punto. Mientras que el código del "espacio de aplicación" sea un código comunitario, el poder del gobierno para regularlo será débil; mientras que el código de "espacio de aplicación" sea privado, el poder del gobierno para regularlo será fuerte. En este sentido, el poder del gobierno depende de la *organización* del código que constituye el ciberespacio, no tan solo sobre su arquitectura, sino que también sobre quien controle esa arquitectura.

La razón es evidente. El gobierno regula consiguiendo que la gente se comporte de ciertas maneras. Cuando regula códigos, lo logra haciendo que los autores de los códigos escriban un código diferente. Cuando describí una normativa que sectorizara mejor las expresiones "dañinas para menores de edad", ese esquema dependía significativamente del hecho que gran porción del mercado de navegadores está controlado por un pequeño número de firmas. Ya que Netscape y Microsoft son grandes compañías con bienes reales, son blancos fáciles para regular.

Pero cuando ninguna organización en particular o pequeño grupo de organizaciones controla el código, o cuando el código, aun cuando ini-

cialmente estuviese controlado por solo una compañía, es abierto y por ende modificable, el gobierno tiene menos posibilidades de regular el código. Un requisito poco popular impuesto sobre el código común simplemente será removido por las personas, quienes no son blancos tan fáciles para el gobierno. Así, expandiendo el número de personas que pueden controlar el código, se contrarresta el poder del gobierno para regular el código. Los códigos comunes son mucho menos fáciles de controlar que los códigos privados.

Nada en esta afirmación es absoluto. No estoy argumentando que la organización del código sea el único factor relevante, ni estoy discutiendo que el gobierno no pueda conseguir ningún efecto en los códigos comunes<sup>110</sup>; sin embargo, de existir este efecto es únicamente marginal.

No obstante lo anterior, el argumento sugiere algo importante acerca del valor de los comunes, por lo menos para los que controlarían el poder para regular del gobierno. Si el código es concebido como propiedad privada, y si a los dueños del código se les otorgan fuertes derechos de propiedad, entonces este régimen aumentará el poder regulatorio del gobierno. El poder para regular sería aun más grande si el Estado controlase el código, porque el código estatal sería más regulable que el código privado. Sin embargo, el código estatal sería también menos eficiente. Estamos más allá de los días en que los burócratas producían; es mejor dejar la producción al mercado.

En lo que refiere al código común, sin embargo, el código privado es más regulable. Si la ley de propiedad localiza el derecho a controlar, entonces la propiedad privada hace ese derecho exclusivo; la propiedad común hace ese derecho no exclusivo. La propiedad común no identifica a una entidad particular con un derecho exclusivo de control. Así la propiedad común produce muchas fuentes de control y restringe el poder del gobierno para regular.

La propiedad privada ha sido considerada como un medio para controlar el poder del Estado. Ha sido criticada por crear su propio problema de concentración de poder, pero muchos creen que es un poder menos peligroso. Sea esto o no verdad, entender el papel que el código puede jugar en el control de la conducta en el ciberespacio, arroja una observación sobre la propiedad, que de otra forma no habría sido advertida. Los derechos exclusivos pueden ser necesarios para crear incentivos para la actividad creativa dentro del ciberespacio; estos derechos pueden justificarse por un aumento en la eficiencia; sin embargo, otra justificación es que dichos derechos ayudan a racionalizar un poder de controlar. En la medida que una constitución aspira a controlar el poder del gobierno, debe tener en cuenta el incremento en este poder que generarán los derechos exclusivos en el ciberespacio.



## **B. Preguntas acerca de la regulación del código por el derecho**

Mientras que la organización del código se mantenga sujeta a la influencia del gobierno, hay dos temas de discusión que el ciberespacio hará más evidentes. Uno será el alcance de dicha regulación. La pregunta acerca de si esa regulación está confeccionada ajustándose estrechamente a un fin legítimo. La otra pregunta refiere a la transparencia de esta regulación: si las restricciones impuestas por el gobierno son reconocidas como restricciones, y si son reconocidas como restricciones impuestas por el gobierno.

Mi argumento no ha sido que esta forma de regulación (a través de la arquitectura y del derecho) es nueva como el ciberespacio; mi argumento, a lo más, es que su importancia es novedosa. Aunque en el pasado, en contextos limitados, el estado ha tenido la oportunidad de regular de una manera que por sí misma aumentaría la regulabilidad<sup>111</sup>, no ha tenido esta oportunidad de una manera tan fundamental.

1. *Amplitud excesiva* (Over-inclusiveness), la primera pregunta que levanta la regulación del código es una cuestión general de la amplitud excesiva. Para un objetivo dado, existe un número indeterminado de maneras de crear una solución de código. Algunas de estas soluciones serán más ajustadas que otras. Por ajustadas, quiero decir menos generalizables; estas soluciones de código resolverán un problema, pero no permitirán la regulación de muchos otros asuntos. Una pregunta "constitucional" sobre esto es si hay un valor en ajustar o reducir el alcance de aquellas regulaciones que permiten otras regulaciones (regulation-enabling regulation).

Dos ejemplos aclararán el punto. El Congreso incluyó una disposición antivulneración en la Digital Millennium Copyright Act<sup>112</sup>. Esta disposición regula las tentativas para vulnerar las tecnologías designadas con el objeto de proteger el material protegido por derecho de autor. Si se intenta evadir estas tecnologías se habrá cometido un delito. Análogamente, si usted trata de descerrajar un candado, usted habrá cometido una infracción.

Sin embargo, el problema con esta estructura es que da mayor protección que la propia ley de derecho de propiedad intelectual. Como lo hicieron notar los críticos de la ley antivulneración<sup>113</sup>, la ley convierte en un delito el evadir dichas tecnologías aun cuando el uso que se le dé al material protegido no hubiese sido una violación del derecho de autor.

Con todo, la disposición antivulneración castiga una evasión que simplemente permite un uso justo. La ley entonces protege el código más de lo que protege el material subyacente protegido por derecho de autor.

Habría sido simple construir una ley que sancionara la vulneración de las medidas tecnológicas que no fuera tan excesiva en este sentido. La ley, por ejemplo, podría haber hecho de la vulneración un factor agravante en cualquier proceso por violación de derechos de autor. Pero protegiendo el código más que al derecho de autor, la ley crea un incentivo para la privatización del derecho de autor que describí en la Parte II. Es decir, la ley protege los esquemas cuyo último efecto bien puede ser desplazar el equilibrio que logra la ley de derechos de autor.

Algunos pueden justificar esta forma de regulación como un tipo de ley de violación de la propiedad (trespass law). Bajo este concepto, la antivulneración solo protege a los dueños del ingreso desautorizado a su propiedad. Pero aquí la metáfora es peligrosa. Si la disposición antivulneración alcanzase tan solo intentos de introducirse a un sistema computacional, entonces la "violación" sería una metáfora útil. Pero, en la medida que la disposición tenga como objetivo el entender la propiedad intelectual más como propiedad verdadera, protegiendo contra el acceso a la información, más que contra el acceso a los ordenadores, entonces la metáfora de "violación" no ayuda. Yo no vulnero su idea por el solo hecho de pensarla.

Un segundo ejemplo de adaptaciones exactas es más problemático. En la Parte II describí un esquema para facilitar la sectorización de la expresión en el ciberespacio. En mi visión, el derecho podría guiar la arquitectura del ciberespacio hacia un espacio que permita la identificación. Creando el incentivo para que los individuos porten identificaciones digitales, u ordenando a los sistemas que controlen estas identificaciones digitales, el derecho podría inducir el abastecimiento de identificaciones, y por ende a aumentar la regulabilidad.

Sin embargo, existen muchos diseños posibles para un ciberespacio que permita la identificación, estos variados diseños generalmente tienen diferentes consecuencias para la regulabilidad del ciberespacio. Describí en la Parte II una versión de una identificación infantil. Este sería un navegador que escondería información personal acerca del usuario, pero señalaría que es un menor. Este diseño haría posible para los servidores con contenido para adultos identificar al cliente como un niño, y así negarle el acceso; también haría que los sitios que recolectan datos cumplieran con las leyes que prohíben la recolección de datos sobre menores.

Otra alternativa para un ciberespacio que permitiera la identificación sería uno que creara incentivos para que los usuarios portaran identificaciones digitales<sup>114</sup>. Estos certificados digitales verificarían ciertos elementos acerca del portador del certificado, por ejemplo, el nombre, edad, ciudadanía, y sexo del portador.

Para el propósito de controlar el material para adultos, el único elemento esencial del certificado sería la edad. Y así como las identificaciones infantiles pueden habilitar otras regulaciones relacionadas con



ser un menor, una identificación de la edad permitiría también otras regulaciones relacionadas con ser un adulto, como lo son las regulaciones sobre apuestas o votación.

Sin embargo, en la medida que tales identificaciones certifiquen más que la edad, facilitan un ámbito de regulación sumamente creciente. Si certifica ciudadanía o residencia, permitiría regulaciones que condicionarán el acceso según esas características. Mientras más certifique la ID (identificación), mayor será la sectorización que permita el sistema.

Si el objetivo específico de la regulación por parte del Congreso era proteger a los niños, entonces el método menos restrictivo de lograrlo hubiera sido el KMB, Modalidad Infantil de Navegación. Pero si la Corte discrepa, entonces el amplio rango de alcance puede convertirse en un problema, ya que creando los incentivos necesarios para facilitar identificaciones mucho más amplias, el Estado podría crear los incentivos necesarios para facilitar una regulación mucho más amplia del comportamiento en el ciberespacio. Una regulación así se extendería sobrepasando el legítimo interés del Estado por regular, y facilitaría la regulación mucho más allá de limitar el acceso a materiales con contenido para adultos.

En los ejemplos de antivulneración y de KMB, la estructura de una potencial regulación es la misma. En ambos, al menos dos cambios en la arquitectura podrían lograr el objetivo del Estado. Un cambio facilitaría solamente ese objetivo; el otro facilitaría este objetivo y, como un subproducto, crearía la oportunidad de regular más allá de ese objetivo. En el caso de la antivulneración, esa regulación adicional es la regulación privada; en el caso de las identificaciones, esa regulación adicional es pública.

La pregunta en cada caso es si alguna cosa se inclina en favor de la regulación más estrecha más que por la regulación más amplia. Dentro del contexto de la regulación de la expresión, el valor del discurso libre obviamente lo hace. Pero la regulación de la identificación se relaciona ambiguamente con la expresión. La regulación de la identificación podría avanzar por razones que no tienen relación con la protección de la expresión. Aun cuando estuviera relacionada —por ejemplo, facilitar el uso en línea de la tarjeta de crédito o de las actividades bancarias—, seguiría existiendo la misma pregunta sobre los subproductos de esta regulación. El gobierno puede tener una necesidad legítima de regular para incentivar la identificación, pero la consecuencia de la identificación creciente puede alterar drásticamente la irregularidad del espacio en general.

*2. Transparencia.* Un segundo problema con la regulación legal del código es la falta de la transparencia. Cuando el Estado exige que los individuos se comporten de una manera determinada, los individuos reconocen que es el Estado que está regulando. Si no les gusta esa

regulación, pueden elegir a los representantes que la abrogarán. La regulación de tal modo es controlada por el proceso político<sup>115</sup>.

La transparencia también ha sido tradicionalmente un valor que obliga a la promulgación de la regulación. Aunque los constituyentes (Framers) conservaron en secreto sus deliberaciones, y aunque el Senado haya preservado este secreto hasta 1795<sup>116</sup>, el estado de derecho (rule of law) siempre ha requerido que una ley sea pública antes de que entre en efecto. El acto del procedimiento administrativo (APA) empujó este valor incluso más lejos; en respuesta al Estado administrativo emergente, la APA estableció procedimientos que demandaban apertura en el proceso administrativo<sup>117</sup>.

¿Pero y si la regulación pudiese ser secreta, o más precisamente, qué si el hecho que un gobierno regulase de cierta manera pudiese mantenerse en secreto? Entonces este apremio de la responsabilidad política desaparecería. En este caso no sería claro que la fuente de la regulación es el gobierno, el gobierno podría alcanzar su meta sin pagar el precio político o disminuir la eficacia de la regulación.

El caso *Rust vs. Sullivan*<sup>118</sup> es un ejemplo de la potencia de la no-transparencia. La Administración de Reagan se oponía al aborto. Un grupo de las mujeres que resultaban susceptibles de ser disuadidas del aborto, eran las que visitaban las clínicas de planificación familiar. Obviamente, desde *Roe vs. Wade*<sup>119</sup> el gobierno está limitado en los medios que puede utilizar para disuadir los abortos. Aunque el gobierno no necesita financiar el aborto, no puede prohibir toda clase aborto. Aunque el gobierno puede argumentar contra el aborto, por ejemplo, poniendo anuncios o carteles que digan "la Administración cree que elegir la vida es mejor que elegir el aborto", en cualquier clínica de planificación familiar financiada por el gobierno, lo más probable es que estos anuncios sean ineficaces. Las alertas del gobierno serían tratadas simplemente como alertas del gobierno, un producto de la política, muchos las creerían, y poco más.

La Administración de Reagan eligió una técnica diferente y más eficaz. Prohibió a los doctores en clínicas de planificación familiar recomendar o discutir el aborto como método de planificación familiar. Si eran consultados al respecto, estos doctores debían decir que el programa "no consideraba el aborto un método apropiado de planificación familiar y por lo tanto no lo aconsejaban, o no se referían al aborto"<sup>120</sup>.

Ahora, la genialidad de este método de regulación es que efectivamente esconde la mano del gobierno. Como lo alegó Laurence Tribe ante la Corte Suprema<sup>121</sup>, le permite al gobierno transmitir su mensaje sin ligar el mensaje al gobierno. Muchas mujeres tienden a pensar que es su doctor el que las está guiando lejos del aborto, ya que es el doctor quien está diciendo o no diciendo algo acerca del aborto. El gobierno logra su objetivo lesionando la transparencia. El éxito del programa depende de vencer la transparencia.

El ciberespacio presenta la gran oportunidad para la sentencia de *Rust*. Lo anterior porque es una característica de la experiencia de la gente en el ciberespacio la escasa probabilidad de asociar cualquier restricción determinada a una opción hecha por un codificador. Cuando uno entra en un cuarto de charla en AOL que permite solamente veintitrés personas en el cuarto, probablemente uno crea que esta restricción está en un cierto sentido determinada por la naturaleza del espacio. Pero por supuesto, veintitrés es una cantidad arbitraria; habría podido también ser 230. La diferencia es una opción, y las razones de la opción no se dan.

Esto crea una oportunidad extraordinaria para el gobierno. En la medida que el gobierno puede ocultar sus opciones en el código del espacio, puede, como la Administración de Reagan en *Rust*, evitar las consecuencias políticas de sus opciones. En la medida que el gobierno puede utilizar la arquitectura para llevar a cabo sus opciones, puede alcanzar sus metas más rápida y fácilmente que persiguiéndolas abiertamente.

Mi argumento no es que esta oportunidad sea nueva, ni que cada regulación por medio de la arquitectura no sea transparente. Cuando Robert Moses construyó los puentes a Long Island que bloquearon los buses, y de tal modo evitaron el ingreso a los pasajeros de los buses —y así el de los menos ricos— a las playas públicas<sup>122</sup>, eso era una regulación por medio de la arquitectura, y esa regulación ocultó con éxito sus motivos. Pero cuando el Estado construye un lomo de toro en una rampa de acceso del aeropuerto, esa también es una forma de usar la arquitectura para regular. Esta última regulación no oculta su objetivo, nadie cree que la naturaleza o la coincidencia han puesto el lomo de toro en el centro del camino.

La diferencia entre el ciberespacio y el espacio real nuevamente es de grado. Las oportunidades para una regulación no transparente se multiplican en el ciberespacio y el problema fundamental, o constitucional es si esto debe importarnos. ¿Deberían nuestras creencias acerca del valor de la transparencia alejarnos de las regulaciones a través del código que obstaculizan nuestra meta? ¿Deberíamos exigir que el Estado haga públicos sus propósitos?

El ciberespacio plantea el problema de la transparencia en un nuevo contexto. Cuando el Estado regula indirectamente a través de la regulación del código del ciberespacio, ¿debería exigírsele hacer transparente dicha regulación?<sup>123</sup> Creo fuertemente, y esta creencia resulta consistente con nuestra tradición, que la respuesta debiera ser sí<sup>124</sup>. Sin embargo, creo fuertemente también que nada dentro de nuestra gama de principios constitucionales requeriría al gobierno hacerlo. Si la Constitución es para enfrentar los problemas del ciberespacio, debería resultar capaz para hacerse cargo de estos.

### **C. Preguntas acerca de la regulación del derecho por el código**

He argumentado que el derecho es vulnerable a la soberanía competitiva del código. Los escritores del código pueden diseñar códigos que desplacen los valores comprendidos en el derecho. Si estimamos que los valores del derecho deben sobrevivir, el derecho debería responder a esto.

Mis ejemplos en la Parte II describen dos casos particulares en los cuales los valores de un régimen legal están siendo desplazados. Sin embargo, podemos describir este desplazamiento en forma más general. Generalmente, los valores que la presente arquitectura permite son valores de control horizontal (bottom-up), excepto, como ya he advertido, en el caso de la privacidad. Ellos permiten el control a través de estructuras horizontales, como aquellas que asemejan los contratos o los sistemas de propiedad. Este tipo de estructuras interfiere con la imposición de esquemas regulatorios impuestos verticalmente (top-down), que los usuarios no elegirían por ellos mismos.

Esto no significa que el gobierno no pueda regular, como he advertido, el gobierno puede utilizar técnicas indirectas para crear incentivos que lesionarán la regulación horizontal. Lo que significa es que hace más evidente la debilidad de una potencial autorregulación para Internet.

Como en cualquier otro tipo de regulación, existe una política económica para la autorregulación de la Red. Como en otros casos, algunos intereses individuales ganan más con una arquitectura particular que otros. Estos intereses financian una determinada evolución de la Red. Es probable que prevalezca un diseño que privilegie las estructuras horizontales en esta evolución, aun si la ganancia neta de este tipo de diseños es menor que la ganancia que se obtendría con otros diseños alternativos.

Este punto obvio sugiere un segundo punto. Los usuarios requieren un mecanismo de actuación colectiva en el relativamente pequeño número de casos donde la regulación horizontal deja ciertos valores legales desprotegidos, o donde este tipo de regulación amenaza algunos valores legales importantes. Actualmente esta regulación colectiva es resistida por muchos en la Red<sup>125</sup>. Sin embargo, lo que deberíamos resistir son las distinciones simplonas; la opción nunca ha sido entre anarquía y totalitarismo, o entre libertad y control. Algunas regulaciones pueden intensificar la opción individual, aun en el caso que otras restrinjan la opción respecto de ciertas metas colectivas.

Existen dos ilustraciones obvias de este punto. Ya he introducido la primera: la privacidad. Ahora la examinaré más cuidadosamente. La segunda: el spam, es descrita más abajo.

1. *Privacidad.* He descrito una forma en que el gobierno podría subsidiar arquitecturas que favorecieran la privacidad. Debería resultar claro, sin perjuicio de la retórica sobre autorregulación que, sin este subsidio, no es demasiado probable que la privacidad de los consumidores resulte protegida. Existen, por supuesto, organizaciones que intentan establecer protecciones a la privacidad. Sin embargo, su eficacia es mínima en comparación a los intereses y el poder de mercado del comercio en el ciberespacio. Como ha descrito la FTC<sup>126</sup>, los esfuerzos de estos cuerpos autorregulativos han resultado completamente inútiles en traer cambios en lo que refiere a la protección de la privacidad en el ciberespacio y nada en el horizonte sugiere que el futuro de la privacidad de los consumidores será diferente de su pasado.

Resulta poco probable que para valores como la privacidad las regulaciones horizontales permitan modificar una arquitectura —en este caso la arquitectura del comercio— que tan significativos beneficios provee a una clase particularmente poderosa de usuarios. El desafío aquí es instalar estructuras e incentivos sobre estos diseños horizontales que permitan alguna acción colectiva más allá del efecto acumulativo y desorganizado de expresión de preferencia individuales.

2. *Spam.* Spam<sup>127</sup> es el envío de e-mails [correos electrónicos] con información comercial no solicitada, generalmente en grandes cantidades (bulks), a listas de cuentas de correo electrónico a través de Internet. Estas listas son extremadamente baratas, US\$ 500 por 500.000 nombres de una fuente<sup>128</sup>; porque el precio es tan bajo, uno puede mandar 10.000.000 de e-mails usando dicha lista y cosechar el beneficio aun si la tasa de retorno por cada receptor es muy baja.

Lo lucrativo del spam es una función del diseño del e-mail. La arquitectura inicial de los e-mails hacía poco por autenticar a los usuarios que enviaban (relay) e-mails. SMTP (Simple Mail Transfer Protocol), por ejemplo, es aún el protocolo de correos dominante, permite los envíos de correos electrónicos de terceras personas\* (third-party relays) sin una cuenta en el sistema de correo primario<sup>129</sup>. Con los sistemas SMTP configurados para aceptar los envíos de terceras partes, yo puedo dirigir mi correo enviándolo a través de estos sistemas, aun cuando yo no posea cuenta en estos sistemas. De esta manera, los spammers pueden usar los sistemas de transmisión de terceras partes para inundar la Red con e-mails<sup>130</sup>.

Los envíos de terceras partes no son la única técnica utilizada por los spammers, pero constituyen el objeto de un importante debate sobre spam en Internet. Mientras muchos servidores no utilizan un sistema que permita envíos de terceras partes, algunos administradores de sistemas desean que el canal de transmisión permanezca abierto y estos toman otras medidas para que este canal no sea objeto de abusos por parte de los spammers<sup>131</sup>.

Otros en la Red, considerando los envíos de terceras partes como la mayor causa de spam, quieren mantener estos canales cerrados, y algunos de estos otros tienen listas negras organizadas de sistemas de envío abiertos. Los suscriptores usan estas listas negras para determinar los correos electrónicos de quien harán rebotar<sup>132</sup>. Si su administrador de correo electrónico ha dejado la posibilidad de envíos por terceras partes abierta, es probable que su sitio sea añadido a estas listas; si su sitio es añadido a estas listas, entonces su correo dirigido a sitios administrados por suscriptores de estas listas, en muchos casos, simplemente desaparecerá.

Esta confección de listas negras es una especie de vigilancia (vigilantism), es un ejemplo de individuos privados tomando la ley en sus propias manos<sup>133</sup>. Llamar a esto vigilancia no es criticar a los vigilantes. En esta situación esta puede ser la única manera de la gente de luchar contra el crimen, y yo ciertamente creo que, en lo relativo a las normas de la Red, el spam es un crimen.

A pesar de sus virtudes, la vigilancia tiene sus costos. Estas listas negras llegan bastante más allá de la simple incorporación de los sitios en listas. Consideremos un ejemplo de una batalla potencialmente explosiva<sup>134</sup>.

En 1998, Jeff Schiller, el administrador de la red del MIT, comenzó a recibir correos electrónicos de los usuarios del sistema de MIT quejándose que sus correos dirigidos a personas fuera del dominio de MIT habían sido bloqueados. El correo había sido bloqueado por un vigilante de spam, Open Relay Behavior-modification System (ORBS), había decidido que la red de MIT tenía "malas prácticas de e-mail". Sin ningún aviso, MIT fue incorporado a la lista negra de ORBS y, automáticamente, los suscriptores de ORBS comenzaron a excluir los correos electrónicos de MIT. Una compañía en particular confirmó su política de bloqueo de acuerdo a la lista de ORBS: Hewlett Packard (HP). Los correos electrónicos de MIT a HP no serían recibidos mientras MIT no modificara sus políticas de red.

MIT no estaba para ser toreado. Su decisión de no bloquear automáticamente todos los correos electrónicos "envíos de terceras partes" (correos electrónicos que el servidor de MIT envía sin autenticar que quien lo envía se encuentra asociado con MIT) hace sentido para su red y para la comunidad de MIT. MIT disponía de medidas para limitar el spam a través de la vigilancia del uso de sus instalaciones de "envíos de terceras partes". Sin embargo, sus métodos no eran los de ORBS. Esto hacía a MIT un enemigo de ORBS.

Más que ocultarse de la presión de ORBS, MIT decidió pelear, y como tic lleva a tac, decidió pelear con HP. El plan era hacer rebotar cualquier correo electrónico de HP hasta que HP dejara de hacer rebotar los correos electrónicos de MIT.



Llegados a este punto, sin embargo, intervino la diosa fortuna. En respuesta a las quejas de otros ISP BC Tel, el proveedor de la red de servicios de ORBS decidió que el "test de envíos no autorizados" de ORBS constituía una violación de su acuerdo sobre políticas de red. De esta manera BC Tel expulsó a ORBS de la Red y los correos desde MIT a HP fluyeron libres una vez más.

Estas listas negras son una especie de regulación horizontal. Como las soluciones al problema de la privacidad, se trata de regulaciones horizontales imperfectas toda vez que ellas no pueden lidiar con el problema real que está afectando a la Red, a saber, el spam. Para luchar contra el spam, las listas negras adoptan técnicas que son insuficientes y excesivas, el hoyo negro al que estas listas llevan a los usuarios invita al conflicto<sup>135</sup>.

Un camino más simple y directo de lidiar con estos problemas sería algún tipo de regulación estatal. La ley que sanciona el ingreso sin permiso a la propiedad ajena (trespass law) es un primer ejemplo<sup>136</sup>; una ley que requiriese el etiquetamiento del spam sería un segundo ejemplo<sup>137</sup>. Ambas leyes podrían modificar los incentivos de los spammers, incrementando los costos del spam a un nivel donde sus beneficios no superarían dichos costos<sup>138</sup>.

Desde esta perspectiva, el spam era "causado" por los efectos que el código producía en el mercado: facilitar la publicidad a bajo costo. La respuesta es una ley que incremente los costos en el mercado, disminuyendo así la incidencia de los bajos costos de la publicidad. En otras palabras, el derecho debería compensar aquí los cambios introducidos por el código<sup>139</sup>. La comunicación voluntaria (no el spam) sería aún barata; la comunicación no voluntaria (spam) sería aún más barata que en el espacio real.

3. *Valores a cuidar.* Mi objetivo en esta sección ha sido subrayar un conjunto de valores que deberíamos mantener a la vista cuando trabajemos sobre el conflicto entre la regulación del derecho y la regulación del código. Estos valores deberían ser protegidos de ambos: el efecto del derecho en el código y el efecto del código en el derecho. En la medida que el derecho no utilice el código transparentemente, tenemos razones para cuestionar la técnica del derecho. En la medida que el derecho pueda conseguir sus fines a través del código, tenemos razones para requerir que el código sea confeccionado de una forma que satisfaga solamente fines legítimos del Estado.

Dicho de otra manera, cuando una estructura del código afecta valores implícitos en el derecho, existen buenas razones para asegurar que esos valores no sean desplazados. En aquella clase de casos en que la agregación horizontal de preferencias no produzca la mezcla ideal de regulación, debemos vigilar este resultado conseguido a través del diseño horizontal del código.

## Conclusión

Al centro de cualquier lección sobre el ciberespacio yace la comprensión del rol del derecho. Debemos realizar una elección acerca de la vida en el ciberespacio, acerca de si los valores contenidos serán aquellos valores que queremos<sup>140</sup>. El código del ciberespacio constituye esos valores; puede ser configurado para constituir valores que coincidan con nuestra tradición, así como puede ser configurado para reflejar valores que resultan inconsistentes con esta.

En la medida que la Red crezca, que su poder regulatorio aumente, y que su poder como una fuente de valores se vuelva cierto, los valores de los soberanos del mundo real, en un primer momento, perderán relevancia. Sin duda que en muchos casos esto es bueno; sin embargo, no hay razón para creer que esto, en general o indefinidamente, sea una buena cosa. Nada garantiza que el régimen de valores constituido por el código sea un régimen liberal; y hay pocas razones para esperar que la mano invisible de los diseñadores del código empuje en esta dirección. En efecto, en la medida que los diseñadores del código respondan a los deseos del comercio, bien puede suceder que el rumbo que el código comience a tomar sea el de un poder para controlar<sup>141</sup>. Comprender este rumbo será un proyecto continuo de la “ley del ciberespacio”.

A pesar de esto, el juez Easterbrook argumentaba que no había más motivo para enseñar la “ley del ciberespacio” que aquel que existía para enseñar la “ley del caballo”, porque, según sugería, ninguna “iluminaría al derecho completo”<sup>142</sup>. Este ensayo ha sido un respetuoso desacuerdo con esto. Las amenazas a los valores implícitos en el derecho —amenazas que surgen por los cambios en la arquitectura del código— son solo ejemplos particulares de un punto más general: que no solamente el derecho posibilita los valores legales y que el derecho por si solo no puede garantizarlos. Si nuestro objetivo es un mundo constituido por esos valores, se trata entonces de determinar cuánto deben ser considerados estos otros reguladores, el código, pero también las normas sociales y el mercado. El ciberespacio muestra con claridad no solamente cómo ocurre esta interacción, sino, además, la urgencia de entender cómo dirigirla.

## Notas

\* Jack N. and Lillian R. Berkman, Profesor de Entrepreneurial Legal Studies. Harvard Law School. Una versión anterior de este artículo fue publicada en la Stanford Technology Law Review, <http://stlr.stanford.edu>. La presente es una revisión sustantiva de la versión anterior. Agradezco a Edward Felten, Deepak Gupta, David Johnson, Larry Kramer, Tracy Meares, Andrew Shapiro, Steve Shapiro, Polk Wagner, y Jonathan Zittrain por las valiosas discusiones que mantuvimos en versiones anteriores de este ensayo. Agradezco también a los workshops de teoría legal de las universidades de Stanford y Chicago. La asistencia en la investigación, mucha de ella de extraordinaria ayuda, me

fue provista por Karen King y James Staihar, y, en una versión anterior, por Timothy Wu. Muchos de los argumentos utilizados aquí son tratados con mayor detalle en mi libro *CODE AND OTHER LAWS OF CYBERSPACE* (1999).

**\*\* The Law of the Horse: What Cyberlaw Might Teach.** Harvard Law Review. Vol 113 pp. 501-546. © 1999 The Harvard Law Review Association, 1972. Traducido por Iñigo de la Maza Gazmuri y Ximena Escobar Pozo. Programa Derecho y Tecnologías de la Información. Fundación Fernando Fueyo Laneri, Facultad de Derecho Universidad Diego Portales.

1. Ver Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207. La referencia corresponde a un argumento de Gerhard Casper, quien, cuando era decano de la Escuela de Derecho de la Universidad de Chicago, se jactó que la Escuela de Derecho no ofrecía un curso de "La ley del caballo." *Id.* 207 (citando internas omitidas). La frase originalmente viene de Karl Lewellyn, quien comparó el U.C.C (Uniform Commercial Code) con las "reglas para transacciones idiosincráticas entre amateurs". *Id.* 214.

2. En otra parte he desarrollado un recuento completo de esta respuesta, al menos tan completo como un recuento puede ser. Ver LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999).

3. Easterbrook, *supra* nota 1, 207.

4. *Id.*

5. He discutido con considerable detalle la idea que uno está siempre en el espacio real, aun cuando se esté en el ciberespacio. Dicho de otra forma, he afirmado que el ciberespacio no es un lugar separado. Ver Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403 (1996).

6. Ver, por ejemplo, H.L.A. HART, *THE CONCEPT OF LAW* 6-7, 18-25 (2ed. 1994).

7. *Cf. Crawford v. Lungren*, 96 F. 3d 380, 382 (9th Cir. 1996) (reconociendo como constitucional una ley californiana que prohibía la venta de "material dañoso" (harmful matter) en máquinas ubicadas en veredas sin supervisión, toda vez que existe un interés del Estado en proteger a los menores de literatura orientada hacia los adultos).

8. 521 U.S. 844 (1997)

9. Ver *id.* 885; Lawrence Lessig, *What Things Regulate Speech: CDA 2.0 vs. Filtering*, 38 JURIMETRICS J. 630, 631 (1998).

10. Ver Jerry Kang, *Information in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198-99 (1998); *cf. Developments in the Law - The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1643 (1999) [de aquí en adelante *Developments*] (sugiriendo que la invisibilidad de los filtros es un problema potencial, problema de la solución propuesta al acceso de los niños a la pornografía).

11. Un "bot" es un programa computacional que actúa como un agente para un usuario y realiza una tarea, generalmente remota, en respuesta a una solicitud.

12. Ver FEDERAL TRADE COMMON, PRIVACY ONLINE: A REPORT TO CONGRESS 3 & .9 (1998). [De aquí en adelante *PRIVACY ONLINE*].

\* El término meme fue acuñado por Richard Dawkins y refiere un patrón de información contagiosa que se reproduce infectando mentes humanas y alterando su conducta, determinándolos a propagar el patrón. Eslóganes, frases pegajosas, melodías, íconos y modas son ejemplos típicos de memes (ver <http://maxwell.lucifer.com/virus/alt.memetics/what.is.html>. Visitado 02/10/01) (N. de los T.).

13. Ver, e.g., David R. Johnson & David Post -*The Rise of Law in Cyberspace*, 48 STAN L. REV. 1367, 1375 (1996); David Kushner, *The Communications Decency Act and the Indecent Indecency Spectacle*, 19 HASTINGS COMM. & ENT. L.J. 87, 131 (1996); David G. Post, *Anarchy, State and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. art. 3, 12-17 (1995) <http://www.law.cornell.edu/jol/post.html>; Tom Steinert-Threlkeld, *Of Governance and Technology*, INTER@CTIVE WK. ONLINE <<http://www1.zdnet.com/itweek/ltr/threlkl.html>>

14. Ver *Developments*, *supra* nota 10, 1635 ("La diferencia fundamental entre [espacio real y ciberespacio] es que la arquitectura del ciberespacio es abierta y maleable. Cualquiera que entienda como leer y escribir código es capaz de reescribir las instrucciones y redefinir las posibilidades").

15. Como defino la expresión *código* refiere al software y hardware que configura el ciberespacio como es, o más exactamente, las reglas contenidas en el software y hardware que unidos configuran al ciberespacio como es. Obviamente existe un montón de "código" que calza con esta descripción, y obviamente la naturaleza de ese código puede variar dramáticamente dependiendo del contexto. Algunos de estos códigos están dentro del nivel del Protocolo Internet (IP), donde operan los protocolos para intercambiar información en Internet incluyendo TCP/IP). Algunos de estos códigos están sobre este nivel IP, o como lo ha puesto Jérôme H. Saltzer están como su "límite" (end);

En el caso de la transmisión de los sistemas de comunicación de información, este rango incluye encriptación, detección de duplicación de mensajes, secuenciamiento de mensajes, entrega garantizada de mensajes, detección de fallas de anfitrión, y recibos de envíos. En un contexto más amplio, el argumento parece aplicarse a muchas otras funciones del sistema operativo de un computador, incluyendo su sistema de archivos.

Jerome H. Saltzer, David P. Reed & David D. Clark, *End-to-End Arguments in System Design*, in INNOVATIONS IN INTERNETWORKING 195, 196 (Craig Partridge ed., 1988). Más generalmente, este segundo nivel incluiría cualquier aplicación que pudiera interactuar con los programas de red (navegadores, programas e-mails, transferencia de archivos), así como con las plataformas de sistemas operativos sobre las cuales estas aplicaciones deberían funcionar.

En el análisis que sigue, el "nivel" más importante para mis propósitos será aquel que se sitúa sobre el nivel IP. Atendida la adopción de la Red del sistema extremo a extremo (end to end) de Salzer, las regulaciones más sofisticadas ocurrirán a este nivel. Ver también *infra* 24; cf. Timoty Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1164 (1999) (argumentando que el análisis legal de Internet enfocado hacia el usuario necesariamente debe focalizarse en este nivel).

Finalmente, cuando afirmo que el ciberespacio "no tiene naturaleza", lo que estoy diciendo es que un número indefinido de diseños posibles o arquitecturas puede afectar la funcionalidad que ahora asociamos al ciberespacio. No afirmo en cambio que, dada su presente arquitectura, no existan características que unidas configuren su naturaleza.

16. He adaptado este análisis de uno de mis trabajos anteriores sobre regulación. Ver, en general, Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 662-66 (1998) discutiendo la forma en la que el derecho, las normas, los mercados y la arquitectura operan como modalidades de restricción. El análisis está relacionado con la "aproximación instrumental a la acción del gobierno" ("tools approach to government action"), de John de Monchaux & J. Mark Schuster, sin embargo yo considero solo cuatro herramientas y ellos cinco. John de Monchaux & J. Mark Schuster, *Five Things to Do*, in PRESERVING THE BUILT HERITAGE: TOOLS FOR IMPLEMENTATION 3, 3 (J. Mark Schuster, con John de Monchaux & Charles A. Riley II eds., 1997). No pienso, sin embargo, que el número definitivo de herramientas sea lo que importe. Más relevante que el número es la comprensión de que se trata de formas funcionalmente distintas de modificar las restricciones a la conducta. Por ejemplo, el mercado puede o no ser simplemente una agregación de las otras modalidades; no obstante, mientras el mercado funcione y cambie diferenciadamente, es mejor considerarlo como distinto de las demás modalidades.

17. Obviamente el derecho hace más que esto, pero, como los positivistas, dejemos esto de lado. Mi punto aquí no es describir la esencia del derecho, sino solamente una parte del derecho.

18. En 1853, Louis Napoleon III transformó los planos de París, ensanchando las calles con el objeto de minimizar la posibilidad de revueltas. Ver ALAIN PLESSIS, *THE RISE AND FALL OF THE SECOND EMPIRE, 1852-1871*, 121 (Jonathan Mandelbaum trans., 1985) (1979); *Hausmann, George-Eugene Baron*, 5 *ENCYCLOPAEDIA BRITANNICA* 753 (15th ed. 1993).

19. Según la ACLU, once estados promulgaron regulaciones sobre Internet entre 1995 y 1997. Ver

ACLU, *Online Censorship in the States* (visited Nov. 2, 1999) <<http://www.aclu.org/issues/cyber/censor/stbills.html>>

20. Ver, por ejemplo, *Warning to All Internet Users and Providers* (visitado Nov. 2, 1999) <<http://www.ag.state.mn.us/home/consumer/consumernews/OnlineScams/memo.html>> (advertencia puesta en Internet por el abogado general (Attorney General) de Minnesota con respecto a las actividades ilícitas en Internet).

21. Ver, por ejemplo, *United States v. Thomas*, 74 F.3d 701, 716 (6th Cir. 1996); *Playboy Enters. v. Chuckleberry Publ'g, Inc.*, 939 F. Supp. 1032, 1034 (S.D.N.Y. 1996).

22. Ver Julian Dibbell, *A Rape in Cyberspace or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database Into a Society*, 2 ANN. SURV. AM. L. 471, 477-78 (1995).

23. Ver, por ejemplo, *America Online Plans Better Information About Price Changes*, WALL ST. J., May 29, 1998, B2; *AOL Still Suffering But Stock Price Rises*, NETWORK WK., Enero. 31, 1997, disponible en 1997 WL8524039; David S. Hilzenrath, "Free" Enterprise, Online Style: AOL, CompuServe and Prodigy Settle FTC Complaints, WASH. POST, mayo 2, 1997, G1.

24. Cf. *Developments*, *supra* nota 10, 1635 (sugiriendo que las alteraciones en el código pueden ser utilizadas para solucionar los problemas del ciberespacio). Al utilizar la expresión "código" en este ensayo, no me refiero a los protocolos básicos de Internet, por ejemplo, TCP/IP. Ver, en general, CRAIG HUNT, *TCP/IP NETWORK ADMINISTRATION* 1-22 (2d ed. 1998) (explicando cómo funciona TCP/IP); ED KROL, *THE WHOLE INTERNET: USER'S GUIDE & CATALOG* 23-25 (2d ed. 1992) (lo mismo); PETE LOSHIN, *TCP/IP CLEARLY EXPLAINED* 3-83 (2d ed. 1997) (lo mismo); Ben Segal, *A Short History of Internet Protocols at CERN* (visitado agosto 14, 1999) <<http://www.info.cern.ch/pdp/ns/ben/TCPHIST.html>> (describiendo en general la historia de los protocolos Internet, incluyendo los protocolos TCP/IP). Más bien me refiero al código de "aplicación de espacio" (application space) code, esto es, el código de las aplicaciones que operan sobre los protocolos básicos de Internet. Como lo describe Tim Wu, TCP/IP puede ser pensado como el tablero eléctrico (electric grid) de Internet; las aplicaciones se "enchufan" (plug into) a Internet. Ver Wu, *supra* nota 15, 1191-92 (1999). Utilizo la expresión "código" aquí para describir las aplicaciones que se enchufan a Internet.

25. Un ejemplo de este tipo de sitios son los servicios en línea como America Online (AOL).

26. Por ejemplo los postings USENET pueden ser anónimos. Ver *Answers to Frequently Asked Questions about Usenet* (visitado oct. 5, 1999) <<http://www.faqs.org/faqs/usenet/faq/part1/>>

27. Los navegadores que se utilizan para navegar en Internet hacen esta información disponible tanto en tiempo real como archivada en un archivo cookie. Ver *Persistent Cookie FAQ* (visitado agosto 14, 1999) <<http://www.cookiecentral.com/faq.htm>>

28. Los navegadores también permiten desactivar alguno de estos instrumentos de rastreo como las cookies.

29. PGP, por ejemplo, es un programa ofrecido tanto para fines comerciales como en forma gratuita para encriptar mensajes. Ver *The comp.security.pgp FAQ* (visitado oct. 5, 1999) <<http://www.cam.ac.uk.pgnet/pgpfaq/faq-01.html>>

30. En algunos contextos internacionales, por ejemplo, la encriptación es fuertemente limitada. Ver STEWART A. BAKER & PAUL R. HURST, *THE LIMITS OF TRUST* 130 (1998) (describiendo los controles del gobierno francés en la exportación, importación y uso de la encriptación); *Comments by Ambassador David Aaron* (visitado Oct. 5, 1999) <<http://www.bxa.doc.gov/Encryption/aaron.htm>>

31. Algunos académicos han comenzado a desarrollar la idea de que el código contiene a la ley. Ver, por ejemplo, Johnson & Post, *supra* nota 13, 1378-87 (1996); M. Ethan Katsh, *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*, 1996 U. CHI. LEGAL F. 335, 348-54 (1996); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 917-20; Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703, 715-23 (1998).

Para un tratamiento excepcional de la misma materia, ver GERALD E. FRUG, *CITY MAKING: BUILDING COMMUNITIES WITHOUT BUILDING WALLS* (1999).



32. Por supuesto la forma en que ellos regulan difiere. El derecho regula (en este sentido acotado) a través de la amenaza de sanciones *ex post*; las normas sociales (si regulan efectivamente) a través de sanciones *ex post* e internalización *ex ante*; los mercados y la arquitectura regulan a través de una restricción coetánea; las restricciones *ex ante* o *ex post* no son necesarias para disuadir a un sujeto de intentar pasar caminando a través de un muro de ladrillo.

33. Para una perspectiva bastante más profunda y sofisticada que la mía, ver DAVID BRIN, *THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM?* (1998). Brin detalla el crecimiento de las tecnologías del espacio real para monitorear la conducta, incluyendo un gran número que serían invisibles, tal como las tecnologías que según he argumentado definen la red. Ver *id.* 5-8.

34. Ver, e.g., Karen Wright, *The Body Bazaar* DISCOVER, oct. 1998, en 114, 116 (describiendo la proliferación de la venta de sangre en los últimos años).

35. Ver, e.g., BARRINGTON MOORE, JR., *PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY* 7 (1984) (describiendo cómo para una familia esquimal el compartir un pequeño iglú hace de la privacidad un bien inalcanzable).

36. La distinción entre efectos "directos" e "indirectos" posee una historia problemática tanto dentro de la filosofía, ver, e.g., Judith Jarvis Thomson, *The Trolley Problem*, 94 YALE L.J. 1395, 1395-96 (1985) (discutiendo sobre el dilema moral del conductor de un trolley que debe decidir entre seguir su curso y que de manera indirecta sus acciones maten a cinco personas, o alterar su curso y que esto tenga como consecuencia directa la muerte de solo una persona), como en el derecho, ver, por ejemplo, *NLRB v. Jones & Laughlin Steel Corp.*, 301 U.S. 1, 34-41 (1937) (refiriéndose al grado en que los empleados de una compañía estaban directamente involucrados en comercio interestatal). Los problemas de distinguir entre las consecuencias directas e indirectas son similares a aquellas que aparecen en la doctrina de doble efecto. Ver PHILLIPA FOOT, *The problem of Abortion and the doctrine of the Double Effect* in VIRTUES AND VICES AND OTHER ESSAYS IN MORAL PHILOSOPHY; ver también Thomas J. Bole III, *The Doctrine of double effect: Its Philosophical Viability*, 7 SW. PHIL. REV. 1, 91- 103 (1991) (discutiendo y analizando problemas con la doctrina del doble efecto); Warren S. Quinn, *Actions, Intentions, and Consequences: The Doctrine of the Double Effect* 18 PHIL. & PUB. AFF. 41 (1989) (igual). La dificultad surge cuando se debe trazar una línea entre directo e indirecto; no hay necesidad en este ensayo de dibujar tal línea.

37. Mi punto en este esquema no es identificar todas las fuerzas que pueden influenciar cada obligación. Sin duda que cambios en el código influncian al derecho y los cambios en el derecho influncian el código, así como a las demás modalidades regulatorias. Un resumen completo de cómo estas obligaciones evolucionan tendría que incluir una cuenta de la interrelación de estas influencias. Pero, por el momento, me enfocaré solo en la intervención intencional del gobierno.

38. Ver, e.g., ALASKA STAT. § 18.35.305 (Michie 1990) (prohibiendo fumar en lugares públicos); ARIZ. REV. STAT. ANN. § 36-601.01 (Oeste 1993) (lo mismo); COLO. REV. STAT. ANN. § 25-14-103 (Oeste 1990).

39. Ver, e.g., 26 U.S.C. § 5701 (1994) (impuesto a la producción de cigarrillos); 26 U.S.C. § 5731 (1994).

40. Ver, e.g., *Feds Pick Up Arnold Spots*, ADWEEK, nov. 23, 1998 8 (reportando sobre la decisión de la Oficina Nacional de Políticas de Control de Drogas de USA para lanzar a nivel nacional siete comerciales antitabaco orientados hacia la juventud, que originalmente habían sido elaborados para el Departamento de Salud de Massachusetts); Pamela Ferdinand, *Mass. Gets Tough with Adult Smokers in Graphic TV Ads*, WASH POST, oct. 14, 1998, A3 (describiendo una serie de seis anuncios de 30 segundos de duración de contenido antitabaco, financiados por el Departamento de Salud Pública de Massachusetts, sobre la lucha de una mujer por sobrevivir mientras lentamente se sofocaba a causa de un enfisema).

41. No está claro si la FDA (Food and Drug Administration) tiene la autoridad para regular el contenido de nicotina de los cigarrillos. En agosto de 1996, la FDA publicó en el registro federal de la FDA "Regulaciones que restringen la venta y distribución de cigarrillos y tabaco (no para fumar) para proteger niños y adolescentes", 61 Fed. Reg.



44,396 (1996). En *Brown & Williamson Tobacco Corp. vs. FDA* 153 F.3d 155 (4th Cir. 1998), la Corte encontró que la FDA no tenía jurisdicción para regular la comercialización de los productos de tabaco porque excedería el objetivo del Acta Federal de Comidas, Drogas y Cosméticos. Ver *id.* 176.

42. Ver *infra* nota 105 (discutiendo el código abierto).

43. Un ejemplo reciente es el esfuerzo del FBI por lograr que la Internet Engineering Task Force (IETF) cambie los protocolos de Internet para que estos cumplan con el Acta de Aplicación de la Ley de Asistencia de Comunicaciones (CALEA), Pub. L. N° 103-414, 108 Stat. 4279 (codificado en 47 U.S.C §§ 1001-1010). La IETF resistió, pero el esfuerzo es precisamente lo que este modelo pronosticaba. Ver Declan McCullagh, *IETF Says "No Way" to Net Taps*, Wired News (visitado en Nov. 17, 1999) <<http://www.wired.com/news/politics/0,1283,32455,00.html>>

44. Por arquitectura o "diseño", me refiero tanto al diseño técnico de la Red como a su diseño social o económico. Como he de describir más extensamente en la nota 105, una característica crucial del diseño de la Red que habrá de afectar la posibilidad de regularla es su propiedad. Para ser más exacto, la habilidad del gobierno para regular la Red depende en gran parte de quién es el dueño del código de la Red.

45. Una dirección IP es: un número de 32-bit que identifica a quien envía o recibe información dirigida en paquetes a través de Internet. Cuando se solicita una página HTML o se envía un e-mail, el Protocolo de Internet, parte de TCP/IP, incluye su dirección IP en el mensaje (de hecho, en cada uno de los paquetes, si se requiere más de uno) y lo envía a la dirección IP que se obtiene a través del nombre de dominio en el URL requerido o en la dirección de e-mail a que se le está enviando el mensaje. Al otro extremo, el receptor puede ver la dirección IP del peticionario de la página de Internet o del remitente del e-mail, pudiendo responder el mensaje con esa dirección IP recibida. *IP address (Internet Protocol Address)* (visitado en agosto 14, 1999) <<http://www.whatis.com/ipaddress.htm>>

46. Las Intranets hoy en día son la porción de Internet de mayor y más rápido crecimiento. Son un extraño híbrido de dos redes computacionales tradicionales: una es el sistema abierto de Internet, la otra es aquella basada en la capacidad de control en las redes de propiedades tradicionales. Una Intranet mezcla valores de cada una para producir una red que es interoperable pero que da al administrador un gran control sobre el comportamiento del usuario. La Intranet se convierte así en un Internet controlado. Ver, *e.g.*, Steve Lohr, *Internet future at IBM Looks Oddly familiar*, N.Y. TIMES, Sept. 2, 1996 en 37 ("[I]nversiones en los Estados Unidos en programas de Intranet para servidores, los poderosos computadores que almacenan los datos de las redes, incrementaría a US\$ 6.1 billones hacia el año 2000 en relación a los US\$ 400 millones de este año. En contraste con la inversión en programas para servidores de Internet, que tiene proyectado aumentar de US\$ 550 millones a US\$ 2.2 billones para el año 2000"); Steve Lohr *Netscape Talking on Lotus With New Corporate Systems*, N.Y. TIMES, oct. 16, 1996 en D2 ("Ejecutivos de Netscape señalaron estudios que proyectaban que el mercado del Intranet crecerá a US\$ 10 billones para el 2000").

47. Ver *Developments*, *supra* nota 10, 1637-43 (sugiriendo soluciones de código para este conflicto).

48. Ver Child Online Protection Act (COPA), Pub. L. N° 105-277, 112 Stat. 2681 (1998) (a ser codificada en 47 U.S.C. § 231); Telecommunication Act of 1996 (Communication Decency Act, o CDA), Pub. L. N° 104-104, §§ 501-502, 505, 508-509, 551-552, 110 Stat. 56, 133-43 (1996).

49. Ver *Reno v. ACLU*, 521 US 844, 849 (1997) (revocando parte de la CDA); *ACLU v. Reno*, 31 F. Supp. 2° 473, 492 98 (PA 1999 de E.d.) que aceptan la moción de los demandantes para una medida cautelar (injunction) en razón de la alta probabilidad de éxito de la demanda que sostiene que COPA es presuntamente inválida y está sujeta a un profundo escrutinio.

50. La CDA reguló la expresión "indecente". La Corte no ha reconocido dicha expresión (fuera del contexto de difusión radiotelevisiva) como una categoría de discurso susceptible a ser proscrito por el Congreso. COPA regula las acciones de los adultos que desean tener el acceso a material para adultos. Como describo abajo, una alternativa menos restrictiva cargaría de forma más leve a los adultos.

51. Aunque esta idea ha estado rondando por un tiempo, le estoy agradecido a Mark Lemley por incitarme a reconocerlo. Para un análisis más formal de la pregunta si esta alternativa es constitucional, vea Lawrence Lessig & Paul Resnick, "*The Constitutionality of Mandated Access Controls*", 98 MICH. L. REV. (próxima aparición 1999). Podría pensarse una ley menos rigurosa, una que simplemente ordene que los servidores reconozcan y bloqueen aquellos navegadores identificados como de niños. Bajo esta solución, algunas compañías de navegadores tendrían un incentivo en el mercado para proporcionar KMBs; otros no. Pero para crear ese incentivo, la señal debe ser reconocida.

Nótese que Computadores Apple ha llegado cerca de este modelo con su OS 9. El OS 9 permite a múltiples usuarios tener acceso a una sola máquina. Cuando la máquina se configura para los utilizadores múltiples, cada usuario debe proporcionar una clave para acceder a su cuenta. Sería un cambio pequeño agregar a este sistema la capacidad de señalar que el usuario es un menor. Esa información podría entonces señalarse como parte de la identificación de la máquina.

52. Ver *Ginsberg v. New York*, 390 U.S. 629, 641 (1968) ("Sostener el poder del Estado de excluir el material definido como obsceno... requiere solamente que seamos capaces de afirmar que no era irracional para la legislación encontrar que la exposición al material condenado por el estatuto es dañino para los menores de edad").

53. Ver Greg Meckbach, *Microsoft IE Tops in New Poll; Browsers Gains Edge over its Netscape Competitor as Organizations Warm to Pre-Installed Software*, COMPUTING CAN., julio 9, 1999, at 25 (citando datos de Positive Support Review, Inc., según los cuales Microsoft Internet Explorer tiene 60.5% del mercado comparado con el 35.1% obtenido por el navegador de Netscape).

Hago una calificación importante a este argumento abajo. Ver *infra* pp. 534-36.

54. Cf. *Junger v. Daley*, 8 F. Supp. 2a 708, 717-19 (N.D. Ohio 1999) (sosteniendo que "el código de origen es por diseño funcional" y que "en razón de que los elementos expresivos de la fuente de los códigos de encriptación no son ni "inequívocos" ni aplastantemente evidentes, su exportación no se protege bajo la Primera Enmienda.") En última instancia, la pregunta de si un código determinado es expresivo o puramente funcional se decide caso por caso, y es un tema sobre el que las cortes están actualmente en desacuerdo. Comparar *id.* y *Karn v.*, 925 F. Supp. 1, 9 n. 19 (D.D.C. 1996) (sosteniendo que "los códigos de origen son simplemente los medios para ordenar a un computador realizar una función"), con *Bernstein v. United States Dep't of State.*, 176 F.3d 1132, 1141 (9th Cir. 1999), *reh'g granted*, 1999 WL 782073 (concluyendo que un software de encriptación, en su forma de código de fuente y según lo empleado por aquellos en el campo de la criptografía, se debe ver como expresivo para los propósitos de la Primera Enmienda."). Para un artículo útil que critica la extensión de la decisión de la corte de distrito en *Bernstein*, vea Patrick Ian Ross, *Computer Programming Language* 13 BERKELEY TECH. L.J. 405 (1998).

55. Por lo menos siempre y cuando *Ginsberg* sea la ley. Ver *Ginsberg*, 390 U. S. 633 (ratificando la condena de un vendedor de tienda por venderle a un menor material dañino para menores).

56. 521 U.S. 844 (1997).

57. Vea *id.* 874. Así, convengo con la lectura de Reno ofrecida por el profesor Volokh. Ver Eugene Volokh, *Freedom of Speech, Shielding Children, and Transcending Balancing*. 1997, SUP. CT. REV. 14 1, 141-42 ("El material para adultos puede ser restringido con el objeto de servir el interés mayor de proteger a los niños, pero solamente si esta restricción es el medio menos gravoso de hacerlo").

58. Mi argumento no es que la regulación sería perfectamente eficaz, porque obviamente ninguna regulación es perfectamente eficaz. A menudo los niños saben más sobre computadores que sus padres y pueden llegar a evadir fácilmente los controles que sus padres les imponen. La pregunta relevante, sin embargo, es si la capacidad de evadir el control parental es más fácil con el sistema de la identificación del adulto que con el sistema de la identificación de los niños. Para evadir el sistema de la identificación del adulto, los niños necesitarían solamente un número válido de tarjeta de crédito, que en algunos casos les daría acceso al sitio sin siquiera hacer un cargo a la tarjeta de crédito.

Más importante, el estado existente del conocimiento parental no es una base justa sobre la cual juzgar la eficacia potencial de un sistema. Los padres tendrían un incentivo para aprender si las tecnologías para el control fueran presentadas más simplemente.

La cuestión de la eficacia también se presenta en el contexto de sitios extranjeros, ya que en la mayoría es poco probable que estén dispuestos a someterse a una regulación establecida por el gobierno de los Estados Unidos. Pero otra vez la pregunta relevante es si estarían más inclinados a respetar una ley de la identificación del adulto o una ley de la identificación de los niños. A mi juicio, estos sitios serían más proclives a respetar la ley menos restrictiva.

59. Mi uso del término "arquitectura" es algo idiosincrásico, pero no totalmente. Utilizo el término en el sentido que lo usa Charles R. Morris y Charles H. Ferguson. Vea a Charles R. Morris y a Charles H. Ferguson, *How Architecture Wins Technology Wars*. HARV. BUS. REV., mar.-abr. 1993, 86. Mi uso del término no corresponde exactamente a la manera en la cual es utilizado por los informáticos, excepto en el sentido de la "estructura de un sistema". Ver e.g., PETE LOSHIN. TCP/IP CLEARLY EXPLAINED 394 (2ª ed. 1997) (definiendo "arquitectura").

60. Cf. JOEL R. REIDENBERG & PAUL M. SCHWARTZ, 2 ON-LINE SERVICES AND DATA PROTECTION AND PRIVACY-REGULATORY RESPONSES 65-84 (1998) ("La transparencia es uno de los principios básicos de la ley europea de la protección de datos. Este estándar requiere que el procesamiento de la información personal esté estructurado en una manera que sea abierto y comprensible para el individuo. Por otra parte, la transparencia requiere que los individuos tengan derechos de acceso y corrección sobre la información personal guardada.").

61. Cf. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972) (discutiendo que cuando el Estado protege un derecho con reglas de propiedad, "alguien que desea quitar el derecho de quien lo posee debe comprarlo de él en una transacción voluntaria en la cual el valor del derecho sea convenido con el vendedor").

62. Hay un importante tema constitucional que estoy pasando por alto aquí, a saber, si el Estado puede conceder un interés de propiedad sobre "datos privados".

63. Ver *Platform for Privacy Preferences (P3P) Syntax Specification: W3C Working Draft* (visitado agosto 14, 1999) <<http://www.w3.org/TR/WD-P3PIO-syntax/>>

64. Ver *Developments*, *supra* nota 10, 1645-48 (describiendo P3P). Mi aproximación considera las soluciones del derecho y el código inextricablemente ligadas. Desde mi perspectiva, el cambio en las titularidades legales es necesario para crear los incentivos que determinen el surgimiento de la solución de código.

65. P3P ha sido el objeto de un gran número de críticas y de preocupaciones. Primero, P3P por sí mismo no hace nada para asegurar que los proveedores de servicio cumplirán con los acuerdos de privacidad alcanzados a través de las negociaciones de P3P. Ver Graham Greenleaf, *An Endnote on Regulating Cyberspace - Architecture vs. Law?* 21 U. NEW S. WALES L.J. 593, 615 (1998). Segundo, P3P puede conducir en los hechos a un aumento en la explotación de la información personal permitiendo que los sitios web populares condicionen la entrada por medio de la revelación de información altamente personal, dando a los usuarios de la red la opción menos que deseable de renunciar a todos los sitios o de ceder a peticiones, a veces excesivamente, intrusivas de información. Ver Simson L. Garfinkel, *The Web's Unelected Governmente*, TECH REV, nov.-dic. 1998, 38, 44; Greenleaf, *supra*. Tercero, P3P probablemente implicará el costo social de aumentar las tarifas de acceso, puesto que "muchas de la información personal que es recopilada en línea es usada para dirigir la publicidad en Internet, toda vez que la publicidad es una importante fuente de ganancia para los proveedores de sitios, la reserva de información personal puede limitar la capacidad de los proveedores de sitios para atraer anuncios, y así deteriorar su fuente principal de rédito". *Developments*, *supra* nota 10, 1648 (notas al pie omitidas). Cuarto, "[l]a reserva de la verdadera identidad en el ciberespacio... [posible gracias a P3P] puede crear un desinterés [en los usuarios de la Red] en cooperar y puede animar a un comportamiento social imprudente". *Id.* (notas al pie omitidas). Otra preocupación con P3P envuelve la pregunta crítica... [de] [c]uáles serán las configuraciones supletorias proporcionadas a los usuarios [.] Pocos usuarios

de computadores saben siquiera cómo cambiar las configuraciones de la preferencia en sus propios software. Por lo tanto, la manera en que un navegador de la Red, equipado con P3P, se configura con ciertos valores por defecto va a ser la manera en que la mayoría de la población de Internet lo utilizará.

Garfinkel, *supra*, 44, 46. También hay un número de soluciones privadas al problema de la reserva de datos. Para una variedad de anonimizadores, infomediarios, servidores y navegadores seguros, ver *Online Privacy Alliance: Rules and Tools for Protecting Personal Privacy Online* (visitado sept. 30, 1999) <<http://www.privacyalliance.org/resources/rulesntools.shtml>>

66. En el Código Penal Modelo, bajo cuyo modelo muchos de los códigos criminales estatales han sido redactados, el robo de un automóvil, aeroplano, motocicleta, bote a motor u "otros vehículos impulsados a motor" es un delito. MODEL PENAL CODE § 223.1 (2)(a) (1962).

67. John Perry Barlow, *The Economy of Ideas*, WIRED, Mar. 1994, 84.

68. Ver, por ejemplo, Esther Dyson, *Intellectual Value*, WIRED, julio 1995, 136, 138-39 ("Controlar las copias... se transforma en un desafío complejo. Usted puede controlar algo estrechamente ya sea limitando la distribución a un grupo pequeño y de confianza, o... eventualmente su producto encontrará el camino a un extendido auditorio que no está dispuesto a pagar por él, si es que alguno se ubica en el primer escenario."); John Perry Barlow, *A Cyberspace Independence Declaration* (feb. 9, 1996) <<http://www.eff.org/barlow>> ("Sus conceptos legales de propiedad, expresión, identidad, movimiento y contexto, no se nos aplican. Ellos están basados en la materia (matter). Aquí [*sic*] no hay materia).

69. Cf. Dyson, *supra* nota 68, 141 (sugiriendo, por ejemplo, que en la era Internet, "las compañías exitosas [de software] están adoptando modelos de negocios en los cuales son pagadas por los servicios más que por el código"; y que [e]l valor real creado por la mayoría de las compañías de software descansa en las redes de distribución, en las bases de usuarios entrenado, y en sus marcas, no en su código").

70. Ver NICHOLAS NEGROONTE, BEING DIGITAL 58 (1995) ("En el mundo digital no solamente la sencillez [de hacer copias] es lo determinante, sino también el hecho que la copia digital es tan perfecta como la original y, con un buen computador, aún mejor."); Barlow, *supra* nota 67 ("En nuestro mundo, cualquier cosa que la mente humana pueda crear puede ser reproducida y distribuida infinitamente sin costo"); Dyson, *supra* nota 68, 137.

("[La Red] permite copia contenido esencialmente gratis ..."); Nicholas Khadder, Project, *Annual Review of Law and Technology*, 13 BERKELEY TECH. L.J. 3, 3 (1998) ("Recientemente, por ejemplo, Internet ha permitido a los usuarios distribuir y vender información muy ampliamente y a un costo marginal despreciable para el distribuidor.").

71. Ver *Developments*, *supra* nota 10, 1650-51 (describiendo los "[r]ights-management containers" como una alternativa).

72. Ver Mark Stefik, *Letting Loose the Light: Igniting Commerce in Electronic Publication*, en INTERNET DREAMS: ARCHETYPES, MYTHS, AND METHAPORS 219, 226-27 (Mark Stefik ed., 1996); Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing* [hereinafter Stefik, *Shifting the Possible*], 12 BERKELEY TECH. L.J. 137, 139-407 (1997); Mark Stefik, *Trusted Systems*, SCI AM, Mar. 1997, at 78, 78-81.

73. Ver 17 U.S.C. § 109 (1994).

74. Para los detalles técnicos ver Stefik, *Shifting the Possible*, citado arriba en la nota 72, 139-44.

75. U.S. CONST. art. I, § 8, cl. 8.

76. Carta de Thomas Jefferson a Isaac M<sup>c</sup>Pherson (agosto. 13, 1813), en 6 THE WRITINGS OF THOMAS JEFFERSON 175, 180 (H.A. Washington ed., 1854).

77. En el interés de la revelación (disclosure), actualmente me encuentro defendiendo en forma gratuita a un cliente en un caso que plantea interrogantes acerca de las limitaciones de la Primera Enmienda a la Cláusula de Derechos de Autor. Ver *Eldred v. Reno*, N° 1: 99 CV00065 (D.D.C. 1999).

78. 471 U.S. 539 (1985).

79. *Id.* 558.

80. Ver Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 360-63 (1999); David Lange, *Recognizing the Public Domain*, 44 LAW & CONTEMP. PROBS., Otoño 1981, 157, 175-76, 178 (comparando la propiedad intelectual con un terreno que puede ser arruinado por la colonización); Jessica Litman, *The Public Domain*, 39 EMORY L. J. 965, 967, 1023 (1990) (advirtiendo que el "dominio público es lo primero que el derecho debiera defender de la materia básica que hace la autoría posible" y, de esta manera, "permite a los derechos de autor evitar la confrontación con la pobreza de algunas de las asunciones en que se encuentran basados").

81. Ver Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968), reimpreso en PERSPECTIVES ON PROPERTY LAW, 132, 133 (Robert C. Ellickson, Carol M. Rose & Bruce A. Ackerman eds., 2d ed. 1995).

82. Ver Mark A. Lemley, *The Economics of Improvement in Intellectual Property Law*, 75 TEX. L. REV., 989, 1083-84 (1997) (argumentando que la "propiedad intelectual representa un 'delicado balance' entre los derechos de los dueños de propiedad intelectual y los derechos de los usuarios, entre ellos, la próxima generación de usuarios," y que ciertas limitaciones a los derechos de los dueños de propiedad intelectual son, por lo tanto, necesarios par estimular mejoras); Litman, *supra* nota 80, 968 ("El dominio público debería ser entendido no como la esfera del material que no merece protección, sino como un instrumento que permite al resto del sistema trabajar dejando la materia prima para crear a disposición de los autores para su uso."); Stephen M. McJohn, *Fair Use and Privatization in Copyright*, 35 SAN DIEGO L. REV. 61, 66 N° 32 (1998) ("El dominio público es, por sí mismo, un recurso clave para la producción futura de trabajos creativos.").

83. Ver, por ejemplo Hardin, *supra* nota 81, 133-34.

84. Ver Benkler, *supra* nota 80, 360-64.

85. Ver 17 U.S.C. § 107 (1994). El uso justo garantiza el derecho a los usuarios de material protegido por derechos de autor de utilizar dicho material de una forma limitada, con prescindencia de los deseos del dueño del material. Así, por ejemplo, yo podría parodiar un trabajo protegido por derechos de autor, aun si el autor lo objetara. Para una discusión de los límites de la parodia como uso justo, ver Lisa Moloff Kaplan, Comment, *Parody and the Fair Use Defense to Copyright Infringement: Appropriate Purpose and Object of Humor*, 26 ARIZ. ST. L.J. 857, 864-82 (1994). Ver también McJohn, *supra* nota 82, 86-87, 94-95 (usando las decisiones de la Corte sobre el uso justo en el caso de la parodia para apoyar el argumento que el rol del uso justo es mucho más amplio que el de constituir una solución a los altos costos de transacción envueltos en el licenciamiento).

86. Ver RICHARD A. POSNER, LAW AND LITERATURE 407 (2d ed. 1998); William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 358-59 (1989).

87. Ver Melville B. Nimmer, *Does Copyright Abridge the First Amendment Guarantees of Free Speech and Press?*, 17 UCLA L. REV. 1180, 1197-98 (1970) (argumentando que la Primera Enmienda protegería la reimpresión de fotografías de la masacre de My Lai aun si esta reimpresión no quedara comprendida por los contornos de la ley de derechos de autor; ver también Triangle Publications, Inc. v. Knight-Ridder Newspapers, Inc., 626 F.2d 1171, 1184 (5th Cir. 1980) (Tate, J., concurrente) (argumentando que "bajo circunstancias limitadas, el privilegio de la Primera Enmienda podría, y debería existir donde la utilización de la expresión protegida por derechos de autor es necesaria para el propósito de transmitir pensamientos o expresiones"); Sid & Marty Krofft Television Prods., Inc. v. McDonald's Corp., 562 F.2d 1157, 1171 (9th Cir. 1977) ("Deberían existir ciertas instancias poco comunes donde las consideraciones relativas a la Primera Enmienda deberían operar limitando la protección de los derechos de autor para las expresiones gráficas de noticias importantes para el público (newsworthy)."); Wainwright Sec. Inc. v. Wall St. Transcript Corp., 558 F.2d 91, 95 (2d Cir. 1977) (citando Nimmer, *supra*, 1200) ("Algún día, [ciertos casos] podrían requerir que los tribunales distingan entre la doctrina del uso justo y limitación constitucional emergente a los derechos de autor contenida en la primera enmienda").



88. Ver *supra* p. 528.

89. Ver Stefik, *Shifting the Possible*, *supra* nota 72, 139-41.

90. Ver *id.* 147.

91. Ver *Developments*, *supra* nota 10, 1649-56 (describiendo los posibles problemas con una solución de código a las violaciones a los derechos de autor y argumentando que, aunque los gobiernos no debieran intervenir en dichas soluciones hasta que los problemas se vuelvan evidentes, las acciones legislativas son apropiadas si, en los hechos, las soluciones de código perturban el balance de la ley de derechos de autor).

92. Ver, por ejemplo, Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217, 237 (1996) (concluyendo que el "ciberespacio debería ser un entorno tanto, sino más, hospitalario que el espacio 'real' para las transacciones sobre derechos de propiedad"); Raymond T. Nimmer, *Article 2B: An Introduction*, 16 J. MARSHALL J. COMPUTER & INFO. L. 211, 220 (1997) (argumentando que el contrato debería gobernar las transacciones sobre información digital porque la regulación [legislativa o judicial] de los términos es un derecho de contratos inaceptable en la era de la información).

93. Cf. Nimmer, *supra* nota 92, 228-31, 234-35 (1997) (recomendando cambios en el derecho contractual que hagan este tipo de acuerdos exigibles judicialmente).

94. Por supuesto existen dos importantes excepciones sobre las cuales no he trabajado aún: arbitraje y mecanismos de solución alternativos.

95. Mi argumento aquí no es que en este tipo de acuerdos siempre se encuentran involucrados valores que consideramos propiamente públicos. No creo que cada vez que mi hijo negocia con mi hija el lavado de los platos existan consideraciones de carácter constitucional a ser tomadas en cuenta. Sin embargo, dado el alcance del efecto de las transacciones realizadas a través de Internet sobre el comercio, el hecho que algunos contratos sean realmente "privados" no significa que los contratos del ciberespacio sean generalmente "privados".

96. Ver Restatement (Second) of Contracts: Excuse of a Condition to Avoid Forfeiture § 229 (1979).

97. Esta es una posición bastante difundida. Para un ejemplo de estos argumentos, ver: Morris R. Cohen, *The Basis of Contract*, 46 HARV. L. REV. 553, 585-92 (1933); Morris R. Cohen, *Property and Sovereignty*, 13 CORNELL. Q. 8, 21-30 (1927); y Robert L. Hale, *Bargaining, Duress, and Economic Liberty*, 43 COLUM. L. REV. 603, 626-28 (1943); Robert L. Hale, *Coercion and Distribution in a Supposedly Non-Coercive State*, 38 POL. SCI. Q. 470, 488-91 (1923).

98. Por ejemplo, los autores del código pueden dejar disponible el código, como un código abierto, Ver *infra* nota 105, o pueden publicar las aplicaciones importantes de programación de interfase (APIs) que hacen simple el evadir las regulaciones del gobierno.

99. Ver Communications Assistance of Law Enforcement Act (CALEA) Púb. L. Nº 103-414, 108 Stat. 4279 (codificado en 47 U.S.C §§ 1001-1010) (requiriendo a las compañías de teléfonos que seleccionen una arquitectura que facilite la intervención telefónica).

100. Ver Audio Home Recording Act, 17 U.S.C § 1002 (1994) (describiendo el requisito de conformarse con un sistema que limite la copia en serie); Ver también U.S. DEP'T OF COMMERCE, INTELLECTUAL PROPERTY AND NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS (1995) (describiendo brevemente el nuevo sistema requerido).

101. Digital Millennium Copyright Act § 120, Pub. L. N°s. 105-304, 112 Stat. 2860, 2863-72 (1998).

102. Ver *id.*

103. Ver Implementation of Section 551 of the Telecomm. Act of 1996, Video Programming Ratings, Fed. Communications Comm'n, 13 F.C.C.R. 8232 (1998); Technical Requirements to Enable Blocking of Video Programming Based on Program Ratings, Fed. Communications Comm'n, 13 F.C.C.R. 11248 (1998).

104. Ver Security and Freedom Through Encryption (SAFE) Act, H.R. 695, 105 Cong. (1997).

105. En este análisis he hecho una importante presunción simplificadora que no hago en otros escritos. Ver Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L. J. 759 (1999). En este caso yo asumo que estos autores de códigos -los objetivos (targets) de la regulación del Estado- están escribiendo



códigos cerrados, en oposición a códigos abiertos. El código cerrado es aquel que no se transmite con su código fuente y que no resulta fácilmente modificable. Si un estándar o protocolo es construido dentro de este código cerrado, es poco probable que los usuarios, o quienes adoptan ese código, puedan deshacer el estándar. El código abierto es diferente. Si el gobierno enviara un determinado estándar o protocolo dentro de un software de diseño de código abierto, los usuarios o adherentes podrían ser siempre libres de aceptar o rechazar la porción diseñada por el gobierno. Así, si el espacio de la aplicación es esencialmente un software de fuente abierta; el poder regulatorio del gobierno disminuye.

106. Ver *id.* en 767-68 (reflexionando sobre el conflicto).

107. Ver Robert W. Gomulkiewicz, *How Copy left Uses License Rights to Succeed in the Open source Software Revolution and the Implications for Article 2B*, 36 HOUS. L. REV. 179, 182-85 (1999); Richard Stallman, *The GNU Operating System and the Free Software Movement*, en OPEN SOURCES: VOICES FROM THE OPEN SOURCE REVOLUTION 53, 56-57, 60-60, 69-70 (Chris DiBona, Sam Ockman & Mark Stone eds., 1999) [de aquí en adelante OPEN SOURCES].

108. Esto no es técnicamente preciso, pero el espíritu de la metáfora es correcto. Para proteger el código de ser capturado, las licencias de software ponen muchas condiciones sobre el uso de la fuente abierta. Algunas condiciones pueden parecer técnicamente inconsistentes con la idea de comunidad. Quizá una mejor descripción implicaría unos comunes que se protegieran a sí mismos (self-enforcing commons). Ver Chris DiBona, Sam Ockman & Mark Stone, *Introduction to OPEN SOURCES* *supra* nota 107, en 1, 2-3 (describiendo la GPL Licencia Pública General publicada para los consumidores del código de fuente abierta). De acuerdo a la descripción, GPL: dice básicamente que usted puede copiar y distribuir el software licenciado bajo GPL a voluntad, con tal que usted no impida a otros de hacer lo mismo, cobrándoles por el software mismo o restringiéndolos con licencias adicionales. El GPL también requiere que los trabajos, derivados de trabajo licenciado bajo GPL, sean licenciados bajo GPL.

*Id.*

109. Ver *id.* Esther Dyson, *Open Source*, RELEASE 1.0, nov. 1998, en 1; Gomulkiewicz, *supra* nota 107; *supra* nota 105; Glyn Moody, *The Wild Bunch*, NEW SCIENTIST, Dec. 12, 1998, en 42; Tim O'Reilly, *Lesson from Open Source Software Development*, COMM. ACM., abril 1999, en 33; Larry Seltzer, *Software Returns to Its Source*, PC MAG., Mar. 22, 1999, en 166; Jeff Ubois, *Open Source Control*, WINDOWS TECHEDGE (Feb. 1999) <[http://www.windowstechedge.com/wte/wte-1999-02/wte-02-oss\\_p.html](http://www.windowstechedge.com/wte/wte-1999-02/wte-02-oss_p.html)>; Brough Turner, *Open Source Software Infuses CTI*, CTI MAG. (Mar. 1999) <<http://www.tmcnet.com/articles/ctimag/0399/0399horizon.htm>>

110. Ver Lessig, *supra* nota 105, en 767-68.

111. Ver, e.g., Robert L. Stern, *The Commerce Clause Revisited - The Federalization Of Intrastate crime*, 15 ARIZ. L. REV.. 271, 274-76 (1973) (discutiendo *United States v. Five Gambling Devices*, 346 U.S. 441 (1953), en que la Corte dejó sin efecto el § 3 de la Johnson Act, estatuto 64, 1135 (1951), que requería a fabricantes y a distribuidores enviar cuentas mensuales de ventas y de salidas, y registrarse anualmente con el Abogado General). El precedente para la "doctrina de los documentos requeridos", que exime los "documentos requeridos" de la protección de la Quinta Enmienda, es *Shapiro v. United States*, 335 U.S. 70, 77-78 (1965), que restringió la aplicación de esta doctrina requerida de registro y autorreporte para propósitos genuinamente regulatorios. Ver también *Haynes vs. United States*, 390 U.S. 85, 95-100 (1968) (decidiendo que los requisitos de reporte (reporting requirements) violaban la Quinta Enmienda porque no eran de naturaleza regulatoria); *Grosso v. United States*, 390 U.S. 62, 66-69 (1968) (igual); *Marchetti v. United States*, 390 U.S. 39, 54-57(1968) (igual).

112. Ver Digital Millennium Copyright Act § 1201, Pub. L. Nos. 105-304, 112 Stat. 2860, 2863-72 (1998).

113. Ver, e.g., Pamela Samuelson, *The Digital Rights War*; WILSON Q., Otoño 1998, 48, 52-53; Pamela Samuelson, *A look at ... Whose ideas, Anyway? Facing a Pay-Per-Use*, WASHINGTON POST, Nov. 1, 1998 en C3.

114. El gobierno ya está explorando la idea, pero a mi parecer, no muy bien. Ver *GSA's Federal Technology Service Issues ACES RFP* (visitado en oct. 4, 1999) [gsa.gov/acces/rfp/pannc.html](http://gsa.gov/acces/rfp/pannc.html) <<http://www.gsa.gov/acces/rfp/pannc.html>> ("ACES [Access Certificates

for Electronic Services] [Certificados de Acceso para Servicios Electrónicos] se pretende que proporcione identificación, autenticación y la no-renegación vía el uso de la tecnología de firma digital como medio para que individuos y entidades de negocio sean autenticados al acceder, retirar y someter información con el gobierno").

115. Cf. JOHN RAWLS, A THEORY OF JUSTICE 133 (1971). (Una tercera condición [para un concepto de derechos] es el de la publicidad... El punto de la condición de la publicidad es hacer que los partidos evalúen conceptos de la justicia como constituciones morales públicamente reconocidas y completamente eficaces de la vida social; Meir Dan-Cohen, *Decision Rules and Conduct Rules: On Acoustic Separation in Criminal Law*, 97 HARV. L. REV. 625, 667-73 (1984) (evaluando los argumentos para la transparencia mientras que se concluye que esa transparencia también posee costes significativos).

116 Ver RICHARD ALLAN BARKER, THE SENATE OF THE UNITED STATES: A BICENTENNIAL HISTORY 24-25 (1988).

117. Ver Administrative Procedure Act, 5 U.S.C. § 553 (1994) (requiriendo que las reglas legalmente obligatorias sean promulgadas de un procedimiento que dé aviso de ellas y las comente.

118. 500 US 173 (1991).

119. 410 U.S. 113 (1973).

120. *Rust*, 500 U.S. en 180 (citando 42 C.F.R. § 59.8(b)(5) (1989)).

121. Ver Transcript of Oral Argument, *Rust*, 500 U.S. 173 (N<sup>os</sup>. 89-1391, 89-1392), disponible en 1990 WL 601355, at \*3-\*27 (oct. 30, 1990).

122. Ver Robert A. Caro, *The Power Broker: Robert Moses and the Fall of New York*. 318 (1974).

123. Para un poderoso ataque a la falla del gobierno de mantener la transparencia en su regulación, ver A. Michael Froomkin, *It Came from Planet Clipper: The Battle Over Cryptographic Key "Escrow"*, 1996 U. CHI LEGAL F. 15.

124. Cuán afirmativamente debiera hacerlo el gobierno es una pregunta más difícil. Al menos debemos tener claridad acerca de lo que debiera y no debiera hacer. Por ejemplo, en una propuesta reciente de relajar los controles de encriptación, la administración aún conservaba claridad sobre su deseo de mantener el secreto sobre las técnicas investigativas utilizadas para vigilar las conductas en línea. Ver Transcript of White House Briefing (sept. 16, 1999) <<http://www.epic.org/crypto/legislation/cesa/briefing.html>> Mientras ciertas técnicas serán sin duda adecuadamente confidenciales, el alcance y la naturaleza del control del gobierno sobre la arquitectura de la encriptación no debería serlo.

125. Ver, e.g., Bill Frezza, *Cyberspace Jurisprudence: Who Shall Punish Evil?*, INTERNETWEEK, feb. 1, 1999, a25.

126. Ver PRIVACY ONLINE, *supra* nota 12, 41 ("La autorregulación efectiva es deseable toda vez que permite a las empresas responder rápidamente a los cambios tecnológicos y emplear nuevas tecnologías para proteger la privacidad del consumidor ... Hasta hoy día, sin embargo, la Comisión no ha visto emerger un sistema de autorregulación efectiva."). No obstante, en julio de 1999, la FTC envió un nuevo reporte al Congreso, concluyendo que las "iniciativas autorregulatorias descritas [por el reporte] reflejaban los sustanciales esfuerzos y el compromiso de los líderes de la industria hacia las prácticas justas de información". FEDERAL TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 12 (1999).

127 Ver *Developments*, *supra* nota 10, 1601-03 (describiendo el problema del spam, las varias soluciones legales que han sido propuestas y las implicancias a nivel de la Primera Enmienda de estas soluciones); ver también Aliza R. Panitz & Scott Hazen Mueller, *Frequently Asked Questions About Spam* (visitado agosto. 14, 1999). <<http://spam.abuse.net/faq.html>> (respondiendo preguntas frecuentes acerca del spam y refutando defensas comunes frente al spam).

128. Ver David E. Sorkin, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 BUFF. L. REV. 1001, 1010 N° 47 (1997).

\* Un reenvío de correo por terceras partes ocurre cuando un servidor de correos procesa un mensaje de correo en que ni el emisor ni el receptor son usuarios locales. Ver <<http://mail-abuse.org/tsi/ar-what.html>> y <[http://www.sans.org/infosecFAQ/email/mail\\_relay.htm](http://www.sans.org/infosecFAQ/email/mail_relay.htm)> Visitados oct. 11 2001 (N. de los T.).

129. Ver ALAN SCHWARTZ & SIMSON GARFINKEL, STOPPING SPAM: STAMPING OUT UNWANTED EMAIL AND NEWS POSTINGS 90-91 (1998); Kenneth Cukier, *ISPs and Corporates Overcome by Spam*, COMMUNICATIONSWEEK INT'L, enero. 19, 1998, 26.

130 Ver SCHWARTZ & GARFINKEL, *supra* nota 129, 90 (advirtiendo que un servidor "no debería permitir computadores desconocidos [reenviar mails], a fin de que no dejar a los spammers tomar ventaja del servidor para ocultar sus huellas"); *News Briefs: Spammers Still Find Too Many Open Doors*, NETWORK WORLD, julio 12, 1999, 6 (citando un informe según el cual aproximadamente 17% de los servidores de correo electrónico continúan abiertos al tráfico de reenvíos).

131. Ver John Fontana, *Slam the Spam Door*, INTERNETWEEK, agosto. 17, 1998, 1 (observando que "están aquellos que no tienen alternativa sino dejar sus reenvíos abiertos" y citando al administrador de un e-mail universitario quien explica que la solución es "vigilar condenadamente los logs").

132. Ver Roger Dennis, *Xtra's E-mail Problems Continue*, Christchurch PRESS, mayo 9, 1998, 27. ORBS, the "Open Relay Behavior-modification System", mantiene dichas listas negras. Ver *What is ORBS?* (visitado agosto. 14, 1999) <<http://www.orbs.org/whatisthis.cgi>>

133. Otros ejemplos de vigilancia antisпамmer abundan. Ver David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 163 N° 54 (describiendo Cancelmoose, "un ser ficticio que es operado bajo seudónimo en el ciberespacio y que ha asumido el liderazgo en la producción de 'cancelbots', comandos que cancelan postings en los Usenet newsgroups, en respuesta a los casos reportados de 'spamming'"); Richard C. Lee, Comment, *Cyber Promotions, Inc. v. America Online, Inc.*, 13 BERKELEY TECH. L.J. 417, 417 n.5 (1998) ("[M]uchas entidades relacionadas con correo basura [sic] han recibido el ataque de sistemas paralizantes, virus o aun la amenaza de daños físicos."); Joshua A. Marcus, Note, *Commercial Speech on the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245, 248 (1998) (contando la historia de dos abogados de Scottsdale, Arizona, cuya intensa práctica de spamming generó "correos de odio, amenazas de muerte y observaciones antisemitas (citadas omitidas)").

134. Ver Lawrence Lessig, *The Spam Wars* (visitado agosto. 17, 1999) <<http://www.thestandard.net/articles/display/0,1449,3006,00.html>>

135. Ver Kimberly Gentile, *U. Texas-Austin's Junk E-mail Service Nixed, Problems Cited*, U. WIRE, nov. 20, 1998, *disponible in* LEXIS, Wire Service Stories (reportando que los encargados oficiales de la computación en la Universidad de Texas se retiraron de ORBS después de recibir quejas que correos electrónicos completamente legítimos eran bloqueados, y citando a uno de estos encargados, quien señalaba que ORBS es "una medida demasiado estricta para implementarla en este momento"); Rob Hall, *Here's the Dumbest Idea to Hit the Net*, OTTAWA SUN, oct. 2, 1998, 51 (describiendo ORBS como un "método demasiado drástico para tomarlo").

136. Ver *Developments*, *supra* nota 10, 1602 (describiendo un caso en el cual la acción judicial de un ISP en contra de un spammer por ingreso no consentido fue acogida a tramitación).

137. Ver *id.* (describiendo alguna de las legislaciones propuestas).

138. Para comentarios sobre la regulación del spam, ver generalmente E. Hawley, *Taking Spam out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising via Electronic Mail*, 66 UMKC L. REV. 381 (1997); Sorkin, citado en la nota 128; Lee, citado en la nota 133; y Steven Miller, Comment, *Washington's "Spam Killing" Statute: Does It Slaughter Privacy in the Process?*, 74 WASH. L. REV. 453 (1999).

139. Ver Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1201 (1998) (observando que debe aspirarse a "los cambios [en la regulación gubernamental] cuando la velocidad de las comunicaciones incrementa dramáticamente y los costos de la comunicación disminuyen dramáticamente).

140. Ver Robert Fano, *On the Social Role of Computer Communications*, 60 Proc. IEEE 1249, 1253 (1972).

141. Este es el argumento central en LESSIG, *supra* 2.

142. Easterbrook, *supra* nota 1, 207.