

LAS LEYES DEL CIBERESPACIO*

Lawrence Lessig**

Siendo conciente de las cuestiones que la regulación plantea, el autor nos alerta respecto a la tendencia controlista que Estados Unidos está implantando en este nuevo campo de acción social que es el ciberespacio.

Esta postura - contradictoria a los valores de libertad que el país norteamericano propugna - podría resultar peligrosa puesto que podría atentar contra las políticas internas que cada estado busque aplicar en el espacio real, problema que se agrava tras considerar que la tendencia norteamericana es predominante en la regulación del ciberespacio.

Antes de la revolución, la Rusia Zarista tenía un sistema de pasaportes interno. La población detestaba este sistema. Los pasaportes indicaban el estado del cual provenía uno y esta indicación determinaba los lugares a donde uno podía ir, con quiénes podía asociarse uno, lo que uno podía ser. Los pasaportes eran distintivos que otorgaban acceso, o lo impedían. En suma, controlaban lo que en el Estado ruso los rusos podían conocer.

Los Bolcheviques prometieron cambiar todo esto. Ellos prometieron abolir los pasaportes internos. Y así lo hicieron poco después de tomar el poder. Los rusos eran de nuevo libres para viajar a donde quisieran. A dónde podían ir ya no era determinado por un documento que se les exigía llevar con ellos. La abolición del pasaporte interno simbolizó la libertad para el pueblo ruso – una democratización de la ciudadanía en Rusia.

Esta libertad, sin embargo, no habría de durar. Una década y media después, ante la perspectiva de campesinos hambrientos invadiendo las ciudades en busca de comida, Stalin trajo de regreso el sistema de los pasaportes internos. Los campesinos estaban de nuevo atados a sus tierras (una restricción que permanecería hasta el fin de los setentas). Los rusos estaban una vez más restringidos a lo que su pasaporte permitía. Una vez más, para acceder a Rusia, los rusos debían mostrar algo acerca de quiénes eran.

* Artículo traducido por Oscar Trelles y Jorge Trelles bajo la supervisión de José Luis Cúneo Galdós. Este trabajo fue presentado en Taipei, en marzo de 1998, como parte de la Conferencia Taiwan Net '98.

** Profesor de la Facultad de Derecho de la Universidad de Harvard.

El comportamiento en el mundo real – este mundo, el mundo en el cual estoy ahora hablando – está regulado por cuatro tipos de limitaciones. La ley es sólo una de las cuatro limitaciones. La ley regula por medio de sanciones impuestas *ex post* – deja de pagar impuestos y probablemente vayas a la cárcel; roba mi carro y probablemente también vayas a la cárcel. La ley es el más conocido de los reguladores, pero es sólo uno de los cuatro.

En segundo lugar, están las normas sociales. También regulan. Las normas sociales –entendimientos o expectativas acerca de cómo uno debe comportarse, cuya exigibilidad no se da a través de un sistema centralizado de cumplimiento normativo, sino a través de entendimientos y expectativas de casi todos los miembros de una comunidad – dirigen y limitan mi comportamiento en un mayor espectro de situaciones que cualquier ley. Estas normas me indican qué ropa usaré –un traje, no un vestido; ellas nos indican que ustedes deben sentarse silenciosa y educadamente, por al menos 40 minutos, mientras hablo; ellas organizan cómo interactuaremos una vez terminada la charla. Las normas guían el comportamiento; en este sentido, funcionan como una segunda regulación limitadora.

El mercado es una tercera limitación. Regula a través del precio. El mercado limita el monto que puedo gastar en ropa; o lo que puedo generar dando discursos; indica que puedo cobrar menos por lo que escribo que Madonna, o menos por mi canto que Pavarotti. A través del mecanismo del precio, el mercado determina mis oportunidades, y a través de este rango de oportunidades, regula.

Y, finalmente, está la limitación de lo que algunos pueden llamar la naturaleza, pero que yo llamaré “arquitectura”. Ésta es la limitación que impone el mundo como lo encuentro, aun si el mundo que encuentro es un mundo hecho por otros. El que no pueda ver a través de la pared es una limitación a mi habilidad de saber qué está ocurriendo al otro lado de la habitación. El que no haya rampas de acceso a una biblioteca limita el acceso de una persona en silla de ruedas. Estas limitaciones, en el sentido al que me refiero, regulan.

Entonces, para entender una regulación debemos entender la suma de estas cuatro limitaciones operando conjuntamente. Cualquiera individualmente no puede reflejar el efecto de las cuatro juntas.

Esta es la era del ciber-liberalista. Es un tiempo en el cual cierta “publicidad” sobre el ciberespacio se ha desarrollado. Dicha “publicidad” es la siguiente: el ciberespacio es inevitable y, no obstante, el ciberespacio no puede ser regulado. Ninguna nación puede vivir sin él, sin embargo ninguna nación será capaz de controlar el comportamiento en él. El ciberespacio es ese lugar en donde los individuos son, inherentemente, libres del control de los soberanos del espacio real. Es, en las palabras de James Boyle, la gran trampa tecnológica –naciones del mundo, no pueden vivir sin él, pero naciones del mundo, cuando lo tengan, no vivirán por mucho con él.

Mi objetivo hoy es dar una diferente visión del ciberespacio. Mi objetivo es atacar esta “publicidad” ya que, desde mi punto de vista, el mundo en el cual estamos entrando no es uno de libertad perpetua; o más precisamente, el mundo en el cual estamos entrando no es uno. El ciberespacio tiene el potencial de ser el espacio más completo y extensamente regulado que jamás hayamos conocido en cualquier lugar, en cualquier momento de nuestra historia. Tiene el potencial de ser la antítesis de un espacio de libertad. Y al menos que entendamos este potencial, al menos que veamos cómo esto puede llegar a ser, posiblemente nos durmamos a lo largo de esta transición entre la libertad y el control. Pues ésta, desde mi punto de vista, es la transición de la que estamos siendo testigos actualmente.

Ahora quiero demostrar este argumento haciendo uso de la introducción inicial –la historia acerca de la Rusia bolchevique, y la idea sobre la regulación–, pues juntas sugerirán hacia dónde está yendo el ciberespacio y, más importante, cómo podemos esperar que el ciberespacio llegue ahí.

Primero la idea: al igual que en el espacio real el comportamiento en el ciberespacio está regulado por cuatro tipos de limitaciones. La ley es sólo una de esas limitaciones. Pues no obstante la “publicidad”, hay leyes regulando el ciberespacio en este mismo momento –derecho de marcas, leyes de difamación o acoso sexual, todas las cuales limitan el comportamiento en el ciberespacio en la misma manera en que lo hacen en el espacio real.

También hay, tal vez sorprendentemente, normas sociales en el ciberespacio –reglas que regulan el comportamiento, y exponen a los individuos a sanciones por parte de otros. Aquéllas también funcionan en el ciberespacio como hacen las normas sociales en el espacio real, amenazando con sanciones *ex post* de la comunidad.

Y lo mismo ocurre con el mercado. El mercado limita el ciberespacio de la misma forma que en el espacio real. Si cambia el precio por el acceso, las limitaciones sobre el acceso variarán. Si cambia la estructura en el cobro por acceso, la regulación del acceso marginal variará, de la misma manera, dramáticamente.

Pero para nuestros propósitos, la más significativa de estas cuatro limitaciones al comportamiento en el ciberespacio es la análoga a la que llamé "arquitectura" en el caso del espacio real. A ésta la llamaré "código". Por código, simplemente me refiero al *software* y *hardware* que forma el ciberespacio tal como es –el conjunto de protocolos, de reglas, implementadas o codificadas en el *software* del propio ciberespacio, que determinan cómo las personas interactúan, o existen, en este espacio. Este código, como la arquitectura en el espacio real, determinan los términos en los que ingreso o existo en el ciberespacio. Como la arquitectura, no es opcional. Yo no puedo escoger si obedezco o no a la estructura preestablecida –los hackers pueden escoger, pero ellos son especiales. Para el resto de nosotros, la vida en el ciberespacio está sujeta al código, como la vida en el espacio real está sujeta a la arquitectura del espacio real.

La esencia de las limitaciones del código en el ciberespacio varía. Pero la forma como se experimentan no varía. En algunos lugares, uno debe ingresar una clave antes de obtener acceso; en otros, uno puede entrar con o sin identificación. En algunos lugares, las transacciones en las que uno interviene producen trazos que permiten rastrear la transacción hasta el individuo; en otros lugares, esta posibilidad de rastreo sólo se puede dar si el individuo así lo elige. En algunos lugares, uno puede hablar en un lenguaje que sólo el receptor puede oír (a través de la encriptación); en otros lugares, la encriptación no es una opción.

Las diferencias están constituidas por el código de estos diferentes lugares. El código o *software* o arquitectura o protocolos de estos espacios establecen estas características; son características seleccionadas por los creadores del código; éstas limitan cierto comportamiento permitiendo otro. Y en este sentido, éstas, como la arquitectura en el espacio real, regulan el comportamiento en el ciberespacio.

Entonces, el código, el mercado, las normas sociales y la ley, en conjunto, regulan el ciberespacio tal como la arquitectura, el mercado, las normas sociales y la

ley regulan el espacio real. Y mi posición es que, al igual que con las regulaciones del espacio real, deberíamos tener en cuenta cómo estas cuatro limitaciones operan en conjunto.

Un ejemplo –un contraste entre una regulación en el espacio real, y la misma regulación en el ciberespacio –hará más claro este punto. Piensen acerca de la preocupación que existe en mi país (algunos podrían llamarla obsesión) respecto de la regulación sobre indecencia en la red.

Esta preocupación despertó en los Estados Unidos a comienzos de 1995. Su origen fue un incremento extraordinario en el número de usuarios comunes de la red y, por consiguiente, un incremento en su uso por niños, así como un incremento aun más extraordinario en la disponibilidad de lo que muchos llaman 'porno' en la red. Un estudio sumamente controversial (y sobretodo defectuoso) publicado en la Revista de Derecho de la Universidad de Georgetown informaba sobre una red inundada por pornografía. Tanto "Time" como "Newsweek" publicaron artículos de portada sobre su disponibilidad. Y senadores y congresistas fueron bombardeados con demandas para regular la "ciberpornografía".

No hay duda que la furia en ese momento era grande. Pero uno podría preguntar por qué esta furia sobre la pornografía en el ciberespacio era tan grande. Ciertamente hay más pornografía en el espacio real que en el ciberespacio. ¿Por qué entonces la furia sobre el acceso a pornografía en un lugar donde la mayoría de los niños no tiene acceso?

Para entender el por qué, piensen por un segundo acerca del mismo problema tal como se da en el espacio real. ¿Qué regula la distribución de pornografía en el espacio real?

Primero: en Estados Unidos, las leyes en el espacio real regulan la distribución de pornografía a niños – leyes que exigen a los vendedores de pornografía verificar la edad de los compradores, o leyes que requieren que los vendedores se ubiquen en una parte determinada de la ciudad, usualmente alejada de los niños. No obstante, las leyes no son la más importante de las limitaciones impuestas a la distribución de pornografía a los niños.

Más importante que las leyes son las normas sociales. Éstas prohíben a los adultos vender pornografía a los niños. Aun entre los distribuidores de pornografía esta restricción es relativamente efectiva.

Y no sólo las normas sociales. El mercado también, pues la pornografía cuesta dinero, y los niños no lo tienen.

Pero la limitación más importante del espacio real es a la que yo me he referido como arquitectura, dado que todas las otras regulaciones en el espacio real dependen de la limitación llamada arquitectura. Las leyes, normas sociales y mercado pueden discriminar en el espacio real debido a que es difícil en éste esconder que se es un niño. Por supuesto, un niño puede ponerse un bigote, usar zancos y tratar de entrar a una tienda para comprar pornografía. Pero en la mayoría de los casos los disfraces fallarán. En la mayoría de casos, será muy difícil esconder que es un niño. Así, normalmente las limitaciones basadas en ser un niño son limitaciones que pueden ser efectivas. El ciberespacio es diferente. Aun si asumimos que las mismas leyes que se aplican al espacio real se apliquen al ciberespacio, y aun si asumimos que las limitaciones de las normas sociales o del mercado también se aplican, aun así, subsiste una diferencia radical entre los dos espacios. Pues mientras que en el espacio real es difícil esconder que se es un niño, en el ciberespacio el esconder quién se es, o más precisamente, esconder características de quién se es, es la cosa más simple del mundo. Lo normal en el ciberespacio es el anonimato. Y debido a que es tan fácil esconder quién se es, es prácticamente imposible que las leyes y normas sociales se apliquen al ciberespacio. Para que estas leyes se apliquen uno tiene que saber que está negociando con un niño. Pero la arquitectura de este espacio simplemente no proporciona esta información.

Ahora el punto importante es ver la diferencia, e identificar su fuente. La diferencia es una diferencia en lo que quiero llamar la 'regulabilidad' del ciberespacio –la capacidad de los gobiernos para regular el comportamiento en éste. Como es ahora, el ciberespacio es menos regulable que el espacio real. Hay menos que el gobierno puede hacer.

La fuente de esta diferencia en la regulabilidad es una diferencia de la arquitectura del espacio –una diferencia en el código que constituye el ciberespacio tal como es. Mi posición es que su arquitectura lo hace esencialmente irregulable.

O así lo hizo en 1995, y en 1996, cuando el Congreso de los Estados Unidos logró su objetivo de aprobar un

intento para enfrentar este problema –la Ley de Decencia en las Comunicaciones¹. Voy a hablar un poco de lo que ocurrió con dicha ley, pero primero quiero marcar este periodo, y diferenciarlo de donde nos encontramos ahora. Era la arquitectura del ciberespacio en 1995 y 1996 la que lo hacía esencialmente irregulable.

Llamemos a esa arquitectura Red 95 –como en 1995–, y aquí están sus características: en la medida que uno tuviese acceso a la Red 95, uno podía navegar sin identificarse. La Red 95 era la Rusia bolchevique. La identidad o características de uno eran invisibles en la red en ese entonces, con lo cual uno podía entrar y explorar sin credenciales –sin un pasaporte interno. El acceso era abierto y universal, no condicionado a credenciales. Era, en un sentido restrictivo del término, un momento extraordinariamente democrático. Los usuarios eran fundamentalmente iguales. Esencialmente libres.

Fue contra este contexto –el contexto de la red como era en 1995– que la Corte Suprema recién revisó la Ley de Decencia en las Comunicaciones. Dos cortes de inferior jerarquía habían atacado la ley por ser violatoria del derecho a la libertad de expresión. Mientras, millones observaban las deliberaciones de la corte en el caso –observaban en el ciberespacio, mientras los argumentos eran reportados, debatidos y criticados.

Finalmente, en junio del año pasado,² la Corte confirmó la decisión de las cortes inferiores, declarando la ley inconstitucional. Las razones por las que era inconstitucional no son tan importantes para nuestros propósitos aquí. Lo importante es la retórica que llevó a la Corte a esa conclusión.

Ello por cuanto la decisión se apoyó de forma crucial en afirmaciones sobre la arquitectura de la red tal como era –esto es, sobre la arquitectura de la Red 95. Dada esta arquitectura, la Corte concluyó que cualquier regulación que intentase mantener a los niños fuera de la pornografía sería una regulación demasiado gravosa para los hablantes y escuchadores. Como era la red, la regulación sería demasiado gravosa.

Pero lo que fue significativo era que la Corte hablaba como si la arquitectura de la red en 1995 –Red 95– fuese la única arquitectura que la red podía tener.

¹ N. del T.: *Communications Decency Act* en el original.

² El discurso fue realizado en 1998.

Hablaba como si hubiese descubierto la naturaleza de la red, y estaba entonces decidiendo acerca de la naturaleza de cualquier regulación posible de la red. Pero el problema con todo esto es, por supuesto, que la red no tiene una naturaleza. No hay arquitectura alguna que sea esencial para el diseño de la red. La Red 95 era un conjunto de características, o protocolos, que constituían la red en un momento dado. Pero nada obliga a que estas particularidades, o protocolos, siempre caractericen a la red como ésta siempre será. Y en efecto, nada de lo que hemos visto en los últimos dos años debería llevarnos a pensar que ello será así. Un ejemplo demostrará el conjunto más sencillamente. Antes de ser profesor de Harvard yo enseñaba en la Universidad de Chicago. Si uno quería acceder a la red de la Universidad de Chicago, uno simplemente debía conectar su máquina a uno de los terminales localizados alrededor de la universidad. Cualquier máquina podía conectarse a estos terminales y, una vez conectada, cualquier máquina tendría acceso completo a la internet. El acceso era anónimo, completo y libre.

La razón de esta libertad fue una decisión de la administración. Pues el rector de la Universidad de Chicago era Geof Stone, un ex decano de la facultad de Derecho de la Universidad de Chicago, y un reconocido estudioso de la libertad de expresión. Cuando la universidad estaba diseñando su red, los técnicos preguntaron al rector si debería permitirse la comunicación anónima. El rector, citando el principio de que las reglas de la universidad sobre expresión serían tan protectoras de la libertad de expresión como la Primera Enmienda, dijo que sí: uno tendrá el derecho a comunicarse en la universidad anónimamente, ya que la Primera Enmienda de la Constitución garantizaría el mismo derecho tal como lo haría frente al gobierno. De esta política surgió el diseño arquitectónico de la red de la Universidad de Chicago.

En Harvard, las reglas son diferentes. Uno no puede conectar su máquina a la red de Harvard salvo que la máquina esté registrada –autorizada, aprobada, y verificada. Sólo miembros de la comunidad universitaria pueden registrar su máquina. Una vez registrada, todas las interacciones con la red pueden ser monitoreadas y son identificadas en relación con una máquina en particular. En definitiva, la expresión anónima no está permitida en esta red –es contra las reglas. El acceso puede controlarse sobre la base de quién es uno; y la interacción puede ser rastreada sobre la base de lo que uno hizo.

La razón para este diseño también está basada en la decisión de un administrador - un administrador me-

nos interesado en las protecciones otorgadas por la Primera Enmienda en este caso. Controlar el acceso es el ideal de Harvard; facilitar el acceso era el ideal de Chicago; tecnologías que hacen el control posible fueron, por esto, escogidas en Harvard; por ello, tecnologías que facilitaban el acceso fueron elegidas en Chicago.

Ahora bien, esta diferencia entre las dos redes es bastante común actualmente. La red de la Universidad de Chicago es la arquitectura de la internet en 1995. Es, de nuevo, Red 95. Pero la arquitectura de Harvard no es una arquitectura de internet. Es más bien una arquitectura de intranet. La diferencia es simplemente ésta: dentro de una intranet, la identidad está suficientemente determinada para que el acceso sea controlado y el uso monitoreado. Los protocolos subyacentes siguen siendo TCP/IP –los protocolos fundamentales o subyacentes de la internet–. Pero encima de este protocolo se encuentra una serie de otros protocolos destinados a facilitar el control. La red de Harvard es la *internet plus*, en donde el *plus* es el poder de controlar.

Estas dos arquitecturas reflejan dos filosofías acerca del acceso. Reflejan dos conjuntos de principios o valores, sobre cómo debe controlarse la expresión. Mi argumento es que ejemplifican la diferencia entre regímenes políticos de libertad, y regímenes políticos de control. Rastrear la diferencia ideológica entre la Alemania Oriental y la Occidental; entre los Estados Unidos y la antigua República Soviética; entre la República de China, y la China continental. Representan la diferencia entre el control y la libertad –y manifiestan esta diferencia a través de la arquitectura o el diseño del código. Estas arquitecturas permiten la existencia de valores políticos. Son, en este sentido, políticas.

Ahora bien, no ofrezco este ejemplo para criticar a Harvard. Harvard es una institución privada; es libre, en una sociedad libre, para invertir sus recursos en la forma que quiera. Por el contrario, mi punto es simplemente hacerles notar cómo las arquitecturas son muchas, y cómo la elección de una es política. Y cómo, al nivel de una nación, la arquitectura es inherentemente política. En el mundo del ciberespacio, la elección de una arquitectura es tan importante como la elección de una constitución. Pues en un sentido fundamental, el código del ciberespacio es su constitución. Establece los términos bajo los cuales las personas adquieren acceso; fija las reglas; controla su comportamiento. En este sentido, tiene su propia soberanía. Una soberanía alterna, compitiendo con las soberanías del espacio real, en cuanto a la regula-

ción del comportamiento de los ciudadanos del espacio real.

Pero la Corte Suprema de los Estados Unidos trató el tema de la arquitectura como si la arquitectura de este espacio hubiese estado dada. Opinó como si sólo existiese un diseño del ciberespacio –el diseño que tenía.

En esto, la Corte Suprema no está sola. Pues desde mi punto de vista, el error más grande de los teóricos del ciberespacio –de eruditos, y especialmente abogados pensando en la regulación de este espacio– es este error de la Corte Suprema. Es el error del naturalismo aplicado al ciberespacio. Es el error de creer que la arquitectura que tenemos es la arquitectura que siempre tendremos; que el espacio nos garantizará libertad; que por necesidad eliminarán gobiernos que quieren control.

Este punto de vista está profundamente equivocado. Profundamente equivocado porque mientras nosotros celebramos la libertad “inherente” de la red, la arquitectura de la red está cambiando debajo de nosotros mismos. La arquitectura está mutando de una arquitectura de libertad a una arquitectura de control. Está mutando ya sin ningún tipo de intervención gubernamental, a pesar de lo cual el gobierno está rápidamente viendo cómo podría intervenir para acelerar la mutación. Y donde el gobierno está ya interviniendo, lo está haciendo de una forma diseñada para cambiar esta misma arquitectura en una arquitectura de control para hacerla, como ya he dicho, más regulable. Mientras los eruditos prometen libertad perpetua, construida dentro de la arquitectura de la propia red, los técnicos y políticos están trabajando juntos para cambiar la arquitectura, para apartarla de la arquitectura de la libertad.

Como los teóricos del espacio, debemos llegar a comprender este cambio. Debemos reconocer las consecuencias políticas de este cambio. Y debemos asumir responsabilidad por estas consecuencias. Por cuanto la trayectoria del cambio es inequívoca, y el fruto de esta trayectoria, veneno.

Como constitucionalistas, por tanto, debemos confrontar una pregunta fundamentalmente constitucional. ¿Si existe la opción de elegir entre una arquitectura de control y una arquitectura de libertad, entonces cómo resolvemos estas preguntas de índole constitucional? ¿Si las arquitecturas son muchas, acaso la Constitución por sí misma nos guía en la selección de una de ellas?

En mi punto de vista, los valores constitucionales sí implican una arquitectura del espacio. En mi punto de vista, los valores constitucionales deben guiarnos en nuestro diseño de este espacio. Y, en mi punto de vista, los valores constitucionales deben limitar los tipos de regulación que estas arquitecturas permiten.

Pero en mi punto de vista está ausente la idea que ocupa el rol del gobierno en el ciberespacio. En efecto, mi nación –que por muchos años ha sido el símbolo de la libertad en un mundo donde ésta era rara– ha adoptado el liderazgo en formar la arquitectura de la internet, de una arquitectura de libertad a una arquitectura de control. Es decir, una arquitectura que adoptó la tradición de libertad expresada en nuestro pasado constitucional, a una arquitectura que es fundamentalmente antagónica a dichas tradiciones.

Pero ¿cómo? ¿Cómo puede el gobierno hacer estos cambios? ¿Cómo pudo el gobierno realizar este control? Muchos no pueden ver cómo el gobierno puede resolver este control. Por tal motivo, en los pocos minutos que restan a mi charla de hoy, quiero mostrarles cómo. Quiero graficarles el sendero en el cual estamos, y hacia donde, me temo, estamos yendo. Quiero que ustedes vean cómo estos cambios son posibles y cómo el gobierno puede ayudar a que sean permanentes.

Regresen entonces conmigo a la idea que empezó este ensayo –el punto sobre las diferentes modalidades de limitación– y noten algo importante sobre la idea que hemos remarcado poco antes. Dije al inicio que debemos considerar a la ley como sólo una de las cuatro modalidades de limitación; que debemos considerarla sólo como una de las partes de la estructura limitadora utilizada para regular.

Uno podría considerar lo dicho como un argumento acerca de la insignificancia de la ley. Si hay tantas fuerzas reguladoras distintas a la ley, esto podría sugerir que la ley por sí misma puede hacer relativamente poco.

Pero dense cuenta de lo que debería ser obvio. En el modelo que he descrito, la ley está regulando por regulación directa –regulando al individuo a través de la amenaza del castigo. Pero la ley también regula de otras formas. Es decir, regula indirectamente y directamente. Y regula indirectamente cuando regula estas otras modalidades de limitación, de forma tal que éstas regulen de forma distinta. Esto es, puede regular normas sociales, de forma que éstas regulen de forma diferente; puede regular el mercado, para que éste regule de forma diferente; y puede regular la arquitectu-

tura, de forma que la arquitectura regule de forma diferente. En cada caso, el gobierno puede influenciar en las otras estructuras de forma que éstas limiten conforme con los fines del gobierno.

La misma regulación indirecta es posible en el ciberespacio. Pero aquí, sugiero, la regulación indirecta será aun más importante. Pues aquí, el gobierno puede no sólo regular indirectamente para lograr un fin esencial del gobierno. Más importante aún, el gobierno puede regular para cambiar la propia regulabilidad del espacio. Así, el gobierno puede regular las arquitecturas del ciberespacio, de forma tal que el comportamiento en el ciberespacio se vuelva más regulable –en definitiva, para que se convierta en una arquitectura potencialmente más regulable que cualquier otra cosa que hayamos conocido en la historia del gobierno moderno.

Dos ejemplos van a clarificar el punto anterior –un primer ejemplo, en el cual el gobierno regula para lograr un objetivo esencial particular, y un segundo ejemplo, que fluye del primero, en el cual el gobierno regula para incrementar la regulabilidad.

El primer ejemplo es la regulación de la encriptación. La preocupación del gobierno con respecto a la encriptación está referida al uso de la tecnología para proteger la privacidad –la habilidad de esconder el contenido de las comunicaciones de los ojos de terceras personas, ya sea que dicha tercera persona sea el gobierno, o un vecino entrometido. A lo largo de la historia de la tecnología, el gobierno estadounidense ha regulado fuertemente la tecnología; por un tiempo amenazó con prohibir su uso; ha prohibido sistemáticamente su exportación (como si sólo los estadounidenses entendieran las matemáticas avanzadas); y por un tiempo tuvo la esperanza de inundar el mercado con una tecnología de encriptación estándar que dejase una puerta abierta trasera para que el gobierno pudiese entrar.

Las más recientes propuestas son las más significativas. Este noviembre último, el FBI propuso una ley que requiriese a los fabricantes asegurar que cualquier sistema de encriptación tenga una habilidad de recuperación clave o una puerta trasera, de modo tal que los agentes del gobierno, si lo necesitaban, pudiesen tener acceso equivalente al contenido de dichas comunicaciones.

Esta es la regulación del código por parte del gobierno, para regular indirectamente el comportamiento. Es

una regulación indirecta en el sentido que describí párrafos atrás y, desde una perspectiva constitucional es brillante. No es brillante porque sus fines sean buenos; es brillante porque la Constitución estadounidense, al menos, ofrece muy poco control sobre regulaciones gubernamentales de este tipo. La Constitución estadounidense ofrece muy poca protección en contra de la regulación gubernamental sobre los negocios; y dado los intereses comerciales existentes, dichas regulaciones tienden a ser efectivas.

Mi segundo ejemplo se desprende del primero. Por cuanto, un segundo uso de la encriptación es la identificación – al igual que ocultar lo que alguien dice, la encriptación, a través de certificados digitales, puede ser utilizada para identificar a una determinada persona. Con la habilidad de identificar a alguien, el gobierno puede determinar de dónde proviene la persona, o cuántos años tiene. Y con esta habilidad – a través de la certificación de documentos de identidad (pasaportes en la autopista de la información) – los gobiernos pueden regular el comportamiento más fácilmente en esta autopista. Esto recrearía el poder de controlar el comportamiento, recrear el poder de regular.

Dense cuenta lo que ambas clases de regulaciones lograrán. Dado que los Estados Unidos es el mercado más grande para productos de internet, ningún producto puede tener la esperanza de tener éxito a menos que éste sea exitoso en los Estados Unidos. Por tanto, aquellos estándares impuestos exitosamente en los Estados Unidos se convertirán en estándares para todo el mundo. Y estos estándares facilitarán, primero, la regulación y, secundariamente, asegurarán que las comunicaciones en internet puedan ser intervenidas por cualquier gobierno que siguió los procedimientos descritos en la ley. Pero los estándares que esos gobiernos tendrían que cumplir no son estándares de la Constitución estadounidense. Éstos serán cualquiera de los estándares que cualquier gobierno local tenga –ya sea que estemos ante el gobierno de China continental o el gobierno de Suiza.

La consecuencia es que el gobierno de los Estados Unidos estaría exportando una arquitectura que facilita el control, y un control de parte no sólo de gobiernos democráticos, sino de cualquier gobierno, por más represivo que éste sea. Es así que los Estados Unidos pasaría ser de un símbolo de libertad, a un mercachifle de control. Habiendo ganado la Guerra Fría, estaríamos fomentando las técnicas de nuestros enemigos de ese entonces.

¿Cómo debemos responder? ¿Cómo deben ustedes – como soberanos independientes de la influencia de cualquier gobierno extranjero– y nosotros, constitucionalistas liberales, responder? ¿Cómo debemos responder ante las movidas de un poder político y económico dominante en influenciar la arquitectura de la arquitectura dominante en la regulación del código –la internet?

Los soberanos deben percatarse de lo siguiente: que el código del ciberespacio es por sí mismo una clase soberana. Es un soberano en competencia. El código es, en sí mismo, una fuerza que impone sus propias reglas a las personas que están ahí, pero las personas que están ahí son también las personas que están aquí – ciudadanos de la República de China, ciudadanos de Francia, ciudadanos de cada nación en el mundo. El código los regula, aun cuando éstos están sujetos por derecho a la regulación de soberanías locales. Así, el código compete con las opciones políticas de las soberanías locales. Y en esta competencia, a medida que la red se convierte en un lugar dominante para los negocios y la vida social, se desplazarán a la regulación de las soberanías locales. Ustedes como soberanos tenían la influencia competitiva de las naciones. Sin embargo, una nueva nación está conectada a sus teléfonos, y su influencia sobre sus ciudadanos está creciendo.

Ustedes como soberanos, comenzarán a reconocer esta competencia. Y ustedes deben reconocer y cuestionar el rol especial que los Estados Unidos está jugando en esta competencia. En virtud de la distribución de recursos que controlan la arquitectura de la red, los Estados Unidos tienen un poder único para influenciar el desarrollo de dicha arquitectura. Es como si la ley de la naturaleza se estuviese redactando, teniendo a los Estados Unidos en el lado de los autores. Este poder impone una enorme responsabilidad en los Estados Unidos –y ustedes deben asegurarse que ejercite dicho poder responsablemente.

El problema para los constitucionalistas –aquéllos preocupados en preservar las libertades sociales y políticas en este nuevo espacio– es más difícil.

Ahora regresemos a la historia que comenzó esta conversación –el mundo de los pasaportes internos. Una forma de entender la historia del ciberespacio que he contado hoy día está alineada con esta historia sobre la Rusia Zarista. El nacimiento de la red fue la revolución misma; la vida bajo la Red 95 fue la vida en la Rusia Bolchevique (las partes buenas, en las que el pasaporte interno se eliminó); la Red tal como se está volviendo es la Rusia de

Stalin, donde los pasaportes internos fueron requeridos una vez más.

Ahora, hay una trampa en esta historia –una trampa retórica que al menos tiende a oscurecer un hecho importante sobre la vida en el espacio real. Por cuanto todos nosotros vivimos en el mundo de los pasaportes internos. En los Estados Unidos, en muchos lugares, uno no puede vivir sin un carro; uno no puede manejar sin una licencia; la licencia es un pasaporte interno: dice quién eres, de dónde vienes, cuántos años tienes, si has sido condenado recientemente por algún delito; conecta tu identidad a una base de datos que revelará si has sido arrestado (hayas sido procesado o no) o si existe alguna orden judicial que ordene tu arresto en alguna jurisdicción del país. La licencia es el pasaporte interno del estado moderno Norteamericano. Y no hay duda que su habilidad de controlar o identificar es mucho mejor a la que había en la Rusia Zarista.

Pero en los Estados Unidos –al menos para aquéllos que no parecen ser inmigrantes o pertenecientes a una minoría desfavorecida– la carga de estos pasaportes es leve. La voluntad para regular, monitorear, rastrear, no es lo suficientemente fuerte en los Estados Unidos para sostener cualquier esfuerzo sistemático de usar estos pasaportes para controlar el comportamiento. Y esta voluntad no es lo suficientemente fuerte porque el costo de dicho control es demasiado grande. No hay puestos de control en cada esquina; a uno no le requieren que se registre cuando se mueve a través de una ciudad; uno puede caminar relativamente en el anonimato la mayor parte del tiempo. Las tecnologías del control son posibles, pero demasiado costosas. Y esta limitación en el costo es, en gran parte, la fuente de libertad. Es la ineficiencia de las tecnologías de control en el espacio real las que permiten la libertad en el espacio real.

Pero ¿qué pasaría si el costo del control cae dramáticamente? ¿Qué pasaría si emerge una arquitectura que permite el monitoreo constante; una arquitectura que facilita el rastreo constante del comportamiento y del movimiento? ¿Qué sucedería si emerge una arquitectura que a muy bajo costo permite la recolección de información sobre los individuos, sobre su comportamiento, sobre en qué quieren convertirse? ¿Y qué sucedería si la nueva arquitectura pudiese hacer todo esto de manera invisible, sin interferir en la vida diaria del individuo?

Esta arquitectura es el mundo en el que la red se está convirtiendo. Esta es la imagen del control en el que se está volviendo. Tal como en el espacio real, nosotros

tendremos pasaportes en el ciberespacio. Como en el espacio real, estos pasaportes pueden ser usados para rastrear nuestro comportamiento. Pero en el ciberespacio, a diferencia que en el espacio real, este monitoreo, este rastreo, este control del comportamiento, será mucho menos costoso. Este control es el que está detrás, el cual ocurrirá en forma efectiva e invisible.

Ahora, describir este cambio no es para señalar si éste es para bien o para mal. En efecto, sugiero que como constitucionalistas nosotros debemos tomar conciencia de una ambigüedad fundamental en nuestros actuales juicios políticos sobre la libertad y el control. Las personas están divididas en su reacción frente a la imagen de un sistema de control perfecto, pero, sin embargo, invisible. Muchos dirán que este sistema es maravilloso. Que es mejor para atrapar al culpable, con menos carga por el inocente. Pero muchos también dirán que este sistema es horrible. Mientras como gobierno profesamos nuestros ideales de libertad e independencia, habremos establecido un sistema de control mucho más efectivo que cualquier otro que haya existido en la historia.

Pero la respuesta a todo esto no es necesariamente renunciar a las tecnologías de control. La respuesta no es en insistir que la Red 95 sea la arquitectura perpetua para la red. La respuesta, en cambio, es encontrar la forma de trasladar a esta arquitectura de la red aquello que es notable e importante de las libertades actuales y de la democracia constitucional. El punto radica en ser críticos del poder de este soberano –el soberano emergente– así como somos críticos del poder de cualquier soberano.

Cuáles son estos límites: conforme el gobierno toma el control o influye en la arquitectura del código en la

red, como mínimo, nosotros debemos asegurarnos de que el gobierno no obtenga un monopolio en estas tecnologías de control. Nosotros debemos asegurarnos que los controles que construimos en cualquier democracia constitucional sean regulados en la regulación de esta constitución –el código. Nosotros debemos asegurarnos que las limitaciones de cualquier democracia constitucional –los límites eficientemente constituidos por declaraciones de derechos, y sistemas de control y balances– sean regulados por el código. Estos límites son los “bichos” en el código de una democracia constitucional –y como dijo John Perry Barlow, debemos introducir estos “bichos” en el código de ciberespacio. Debemos mejorarlos de tal forma que, por su ineficacia, puedan recrear de nuevo algunas de las protecciones que conocemos de hace mucho tiempo.

El ciberespacio está regulado –por leyes, pero no sólo por ellas. El código del ciberespacio es una de estas leyes. Debemos llegar a ver cómo este código es un soberano emergente –omnipresente, omnipotente, gentil, eficiente, en crecimiento– y debemos desarrollar en contra de este soberano los mismos límites que nosotros hemos desarrollado en contra de los soberanos del mundo real. Los soberanos siempre dirán –tanto del espacio real como del ciberespacio– que los límites, y las ineficiencias –los “bichos” – no son necesarios. Pero las cosas se mueven demasiado rápidas para tener tanta confianza. Mi temor no sólo es que contra este soberano no hemos aún desarrollado un lenguaje de libertad. Ni que tampoco tenemos tiempo para desarrollarlo. Mi temor es que mantengamos la voluntad – la voluntad de las sociedades libres de los últimos dos siglos, para construir constituciones que protejan la libertad, sin perjuicio de las eficiencias.