Bestiario de la Sociedad de la información

Slogans, cliches y sus peligros inminentes

Beatriz Busaniche

"Jamás hubo semejante posibilidad de conocimiento y semejante probabilidad de oscurantismo"

Boris Ryback

Desde hace algunos años se ha impuesto tanto en medios de comunicación, en organismos internacionales, en ONGs como también en círculos académicos, la idea de que las nuevas tecnologías de información y comunicación (TICs) y el ingreso a la denominada "sociedad de la información" traerán aparejada una mejora en la calidad de vida, el desarrollo y el bienestar de la humanidad. Hasta las Naciones Unidas se han hecho eco de semejante postulado y desde hace varios años se trabaja en el marco de la Cumbre Mundial sobre la Sociedad de la Información, con miras a reducir la denominada brecha digital y a cumplir las metas de desarrollo del milenio[1].

Sin embargo, el hecho de que las TICs en sí mismas mejoren la calidad de vida de las personas no está comprobado de ninguna manera en tanto no se saneen previamente las brechas sociales fundamentales: la pobreza, el hambre, el analfabetismo, las pandemias.

Pese a esta reflexión que suena más bien a sentido común, el camino que estamos recorriendo en los últimos años en relación a estos temas está plagado de tecnoutopías que fomentan la construcción de clichés y frases hechas que se presentan como hecho en la pretendida "nueva sociedad".

La historia del proyecto de "Sociedad de la Información", como bien dice Armand Mattelart[2], tiene varios capítulos desde que en 1975 la OCDE adoptó el concepto. Pasó por varias ideas como las "autopistas de la información", pasando por el proyecto de National Information Infraestructure de los EEUU, y luego por las iniciativas de la Unión Europea en el mismo sentido. En 1995, en Bruselas, los miembros del Grupo de los 7 ratificaron el concepto de "global society of information" que se vería impulsado definitivamente a partir de la cumbre de Okinawa del 2000.

Es particularmente importante detenerse en los documentos de Okinawa. La cumbre del G8 realizada en Japón emitió la "Carta de Okinawa sobre la Sociedad Global de la Información"[3]. Esa carta estableció la "agenda" de la "sociedad de la información", e incluyó la creación de la Digital Oportunities Task Force, una fuerza de trabajo integrada por gobiernos, corporaciones y algunas organizaciones no gubernamentales invitadas para establecer un plan de acción basado en la carta de Okinawa.

Este trabajo no pretende analizar esos documentos. Sin embargo, recordar su existencia y lineamientos es imprescindible para entender por qué se han impuesto en el discurso de la "sociedad civil", y luego, incluso y a fuerza de reproducción constante en los medios masivos de comunicación en el sentido común, algunos de los clichés que conforman el "imaginario sobre la sociedad de la información".

El propósito de este trabajo es justamente presentar y someter a crítica algunos de estos clichés que van en sintonía con muchos de los conceptos desplegados en la carta de Okinawa. Desenmascarar estos clichés es el primer paso para dejar de reproducirlos.

Cada uno de los temas apenas esbozados en este trabajo merece un ensayo en sí mismo, por las implicancias de cada uno tanto en términos sociales, económicos como jurídicos. Este breve "bestiario" sólo pretende iniciar una discusión, despertar sospechas e invitar a pensar críticamente sobre las palabras que poco a poco van entramando nuestro imaginario e impregnan nuestro sentido común.

Slogan N°1: "La ruta desde la pobreza hacia el empoderamiento comienza con el click de un mouse"[4]

Créase o no, expertos en el área de "sociedad de la información" publican este tipo de afirmaciones en revistas especializadas. A los hechos me remito. Este cliché sintoniza perfectamente con la Carta de Okinawa ya citada y fundamentalmente entronca con los documentos de la Cumbre Mundial sobre la Sociedad de la Información. El intento de Informatizar la pobreza no propone soluciones concretas para el problema real y concreto: la pobreza y la más injusta distribución de la riqueza de la cual la humanidad tenga memoria.

Por su parte, el Plan de Acción de la CMSI presenta como premisas los objetivos de conectar todas las aldeas del planeta, todas las escuelas del planeta, llevar computadoras, cables y conectividad a todos los rincones del globo. Esto, presentado así, no es más que un redireccionamiento de fondos de financiación de las agencias de cooperación, los organismos internacionales y los gobiernos hacia el sector privado y las escasas cinco o seis empresas globales capaces de efectuar semejante titánica tarea. Sin contar que la mayoría de los gobiernos se endeudarán a partir de créditos otorgados por los organismos internacionales, justamente, para informatizar la pobreza.

Lo que es más grave es que estos postulados que se podrían encuadrar dentro del "reclamo por infraestructura" no provienen solo del sector de las grandes corporaciones, que es en definitiva el principal beneficiado, sino que vienen justamente de muchas organizaciones de la sociedad civil y de un gran porcentaje del sector académico que se hacen eco de la tecnoutopia reinante de que las computadoras fomentan el "empoderamiento" de las poblaciones marginadas (sea lo que sea que signifique la palabra "empoderamiento").

Por otro lado, nos enfrentamos al dilema de que ignorar la revolución de las comunicaciones y los cambios que trae aparejados en el mundo del trabajo, las relaciones sociales, la educación y la libre distribución de conocimiento nos dejaría aún más rezagados entre las naciones del planeta. Entonces nos encontramos ante la exigencia de hacer una valoración crítica y planear estratégicamente el uso de las nuevas tecnologías de información y comunicación.

No se puede afirmar que el uso de TICs elimine la exclusión, pero si es altamente probable que su "no apropiación" sí la fomente. Estamos en un mundo que tiende cada día más a la automatización mientras que la red Internet supone la mayor redistribución de conocimiento jamás vista por la humanidad y pone al alcance de las comunidades y las personas una herramienta potente de comunicación. Pero el real aprovechamiento de esas potencialidades no viene dado por el mero hecho de "acceder a la

computadora", sino más bien por la capacidad de las personas de hacer un uso significativo de esta nueva forma cultural.

Por lo tanto, es imprescindible analizar el impacto de los planes y programas de "conectividad", analizar los entornos donde se van a instalar los centros de "acceso" y trabajar el uso de TICs con una visión que incluya las problemáticas de la pobreza y la marginación, sin olvidar un análisis previo de la infraestructura existente. No sólo se trata de comprar computadoras y llevarlas a las localidades más remotas y/o marginadas, sino evaluar previamente las condiciones en las que se instalará un punto de acceso en materia de energía, arquitectura y necesidades sociales de la localidad.

Esto implica establecer políticas de mediano y largo plazo en materia de TICs, educación, ciencia y tecnología y no simplemente reclamar y mantener planes de conectividad de corto plazo.

Slogan Nro. 2: "Las personas que no accedan a nuevas tecnologías de información y comunicación, para el caso, computadoras e Internet, están condenadas a ser analfabetos digitales"/"la alfabetización informática es aprender a usar computadoras".

Hay varios planos diferentes para plantear este problema. En primer lugar, dejar aclarado que la instalación de infraestructura informática no soluciona por si misma el problema del analfabetismo en un mundo donde hay 800 millones de personas que no han adquirido las competencias básicas de escritura, lectura y comunicación para ser consideradas como personas alfabetizadas.

Por otro lado se debe entender a qué se denomina "analfabetismo digital", un concepto popularizado para describir a las personas que no saben "usar**"** una computadora.

La incorporación acrítica de nuevas TICs en el mundo educativo, incluso puede tener un severo impacto negativo, sobre todo en los casos en los que la incorporación se realiza basada en software propietario[5]. En esos casos, la inclusión de software propietario fomenta una visión oscura de la informática, donde los niños no pueden ejercer su curiosidad y derecho de aprender cómo funciona la computadora, sin infringir los términos de uso y las licencias del software. El uso de software propietario en educación contradice los postulados básicos de la educación fundada en la libertad y la cooperación.

La alfabetización informática real no es aprender a "usar" una computadora o un determinado programa, sino esencialmente, comprender el lenguaje cultural y comunicacional que subyase a la misma. El software es la técnica cultural de la nueva era, y por tanto, para ejercer el Derecho Humano al libre acceso a la cultura que promulga la Declaración Universal de los Derechos Humanos en su artículo 27[6] es necesaria una toma de conciencia sobre las implicancias sociales y culturales del lenguaje computacional.

Incluso, personas que acceden a Internet y al mundo de las computadoras, siguen siendo en muchos casos "analfabetas digitales" en tanto no han aprendido la nueva técnica cultural de la era digital. Una verdadera alfabetización informática no pasa por el uso de un procesador de texto y de una planilla de cálculo, sino por la comprensión, incluso lingüística, de la técnica cultural y comunicativa que representa el software en la actualidad. En un mundo donde el código es la ley y la arquitectura de información determina lo que podemos o no podemos hacer o decir[7], el conocimiento de ese código es

fundamental para una ciudadanía democrática. ¿Quién escribe el código que cada día regula más aspectos de nuestra vida? Una educación que pierda esto de vista pone en riesgo nuestra potencialidad e hipoteca nuestra voluntad ciudadana en el presente y el futuro[8].

Veamos este tema con un poco más de detalle ya que es crucial. El proyecto de "sociedad global de la información" propone llevar alcance informático a todas las aldeas del planeta y fomentar las iniciativas de e-gobierno. Es decir, que se planea un mundo informatizado. Sin embargo, nadie habla sobre el control de esas computadoras.

Volvamos al concepto: "el código es la ley", en este caso, el código informático, el texto escrito que le da instrucciones a una computadora. En un mundo informatizado y automatizado al extremo, cada vez más, serán las máquinas las que "decidan" a partir de las instrucciones redactadas en código, qué es lo que las personas podemos o no podemos hacer o decir.

El código cada día más se nos impone como ley "no negociable" (nadie puede tratar de convencer a un cajero automático de que le entregue dinero si el cajero lo niega, el código, basado en determinadas variables entrega o no el dinero, y allí no hay emergencia, diálogo o negociación posible).

Saber quién escribe ese código y cómo está escrito es crucial en términos de independencia, libertad y derechos ciudadanos. Imaginemos un mundo en el cual el código sea el que nos permita entrar o salir a nuestro trabajo, votar nuestros representantes en el gobierno, pagar nuestros impuestos, estudiar, dar exámenes, recibir atención médica sanitaria, expresarnos, opinar... etc., etc., etc. Por si esto suena exagerado, valga recordar que los proyectos y documentos de "sociedad de la información" del G8 y de la Cumbre Mundial sobre Sociedad de la Información hacen especial hincapié en políticas de e-gobierno, e-aprendizaje, e-salud y demás proyectos "e".

La información de los Estados, información que por ley el Estado recopila y almacena de sus ciudadanos, no puede estar bajo formatos y programas redactados con código que el propio Estado y la ciudadanía no sea capaz de fiscalizar, y mucho menos, con código redactado por alguna corporación de algún otro país. Entregar la potestad del control de la información y las bases de datos de un Estado es la peor pérdida de soberanía que un gobierno puede efectuar y que de hecho efectúa[9].

La proyección más peligrosa pero realista que se puede hacer frente a las negociaciones que se llevan a cabo en esta materia nos presentan un escenario futuro de control cada vez más estricto sobre nuestra acción ciudadana. Un mundo informatizado a extremos, con sistemas informáticos desplegados a lo largo de todo el planeta y una pequeña elite corporativa escribiendo las leyes que controlarán a las computadoras que controlarán a las personas que de ellas dependan para acceder a servicios básicos, educación, trabajo, o sencillamente relacionarse con sus gobiernos a través de lo que se está diseñando como estrategias de e-gobierno.

En tanto no se entienda esto como riesgo y se adopten las medidas preventivas apropiadas, vamos camino al mundo del Gran Hermano y lo que es peor, a pedido de muchas organizaciones de la sociedad civil que no contemplan estos temas y que se presentan preocupadas por la brecha y la exclusión digital.

Visto así y en el actual contexto, la única medida preventiva en este caso es que el software sea libre, que cada Nación soberana base la educación de su ciudadanía en una formación básica esencial para comprender y participar activamente en la redacción de sus códigos/leyes y que las Universidades (al menos las públicas) basen la educación de los profesionales de la informática exclusivamente en software libre[10].

Slogan Nro. 3: - "A mayor acceso a la información, más democracia".

La sobreabundancia de información, hiperinformación, no necesariamente contribuye a una sociedad más democrática, más bien puede tener efectos contrarios. En tanto no se reconozca, fortalezca y la ciudadanía revalide y ponga en marcha su derecho a la comunicación y a la libertad de expresión, incluyendo allí la libertad de expresión vinculada al trabajo de programadores y hackers en lenguaje informático libre, no podremos construir una sociedad más democrática.

La instalación de centros de acceso a Internet sin que las personas se apropien realmente de las nuevas tecnologías de información y comunicación no hace más que fomentar el "consumo" de información y NTICs sin que eso necesariamente se traduzca en mayor democratización. Incluso, la instalación acrítica y no planificada de estos puntos de acceso, sin involucramiento pleno de las comunidades destinatarias, puede provocar un fuerte impacto negativo sobre la cultura local.

Por su parte, es claro que el uso de software propietario o privativo[11] no fomenta una real apropiación de las nuevas tecnologías de información y comunicación, en tanto mantiene oculto y jurídicamente inviolable el mecanismo de funcionamiento del sistema, impide compartir las aplicaciones bajo pena judicial y obstaculiza la acción de estudiar y profundizar en la investigación de los sistemas. Sin contar los riesgos de plagar un país de computadoras cuyo control esta absolutamente fuera del alcance de quienes las utilizan y que llegado el caso responderán las órdenes de quien programó el software y no a sus verdaderos dueños. El control de una computadora siempre, irremediablemente, estará en manos de quien escribe y por tanto domina el software al que responden las máquinas. No hay computadora capaz de negarse a hacer lo que su software le indica, y ese software, en tanto sea privativo y cerrado, será un software desarrollado como caja negra, inviolable, imposible de estudiar y fiscalizar que responderá a la empresa que lo haya desarrollado.

Por otro lado y en paralelo a esta discusión sobre Internet, las computadoras y el software, existe todo un cúmulo de tecnologías de comunicación no basadas en Internet que son esenciales para la democratización del conocimiento y la información. En esto, la democratización del espectro radioeléctrico y los medios comunitarios, especialmente las radios, son factores clave de participación ciudadana en el ámbito de las comunicaciones. No en vano, estas cuestiones están fuertemente rezagadas en la agenda de debates sobre la sociedad de la información previstos por el G8.

Slogan Nro. 4:- "Existen nuevos delitos que es necesario legislar y modificar el código penal para construir una sociedad de la información más segura".

No existen ciberdelitos, existen delitos. Con la excusa de los ciberdelitos y el ciberterrorismo, algunos gobiernos y corporaciones hacen cabildeo para legislar en favor de la aplicación de regímenes jurídicos de control más estrictos sobre toda la ciudadanía. La utilización de nuevas tecnologías para secuestros y atentados (sean teléfonos celulares, páginas web o correo electrónico) es parte del cambio que estamos viviendo, pero pretender instaurar un régimen de control sobre las comunicaciones de toda la ciudadanía en nombre de la ciberseguridad es una flagrante violación a los derechos humanos. Vigilar a toda la ciudadanía es romper con la garantía esencial de que toda persona es inocente de delito hasta tanto se pruebe lo contrario[12].

La pregunta concreta es: ¿cometer delitos tradicionales bajo formas no tradicionales justifica la creación de nuevas figuras penales? Es decir, ¿cometer una estafa utilizando un sitio web es diferente que cometer una estafa utilizando alguna otra metodología? ¿Coordinar un ataque terrorista a través de redes de e-mails es una forma diferente denominada ciber-terrorismo o es sencillamente terrorismo?

Existe una fuerte discusión alrededor de esto. ¿Es necesario crear nuevas figuras penales? La ONU considera que si y ha emitido una serie de documentos clasificando los delitos informáticos según su tipo en: fraude, falsificación y sabotaje.

Al menos así lo indica el documento presentado en el marco del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente Viena, 10 a 17 de abril de 2000[13].

Esos documentos de Naciones Unidas indican que "dado que las computadoras y las redes pueden ser objeto a la vez de uso legítimo y de uso ilícito, se impone la conclusión de que entre quienes exploran las oportunidades del nuevo medio hay personas y grupos impulsados por motivos delictivos." Es extraño que los expertos que trabajan estos temas no analicen este tipo de afirmaciones desde el más llano sentido común: todo entorno humano puede ser objeto a la vez de uso legítimo y de uso ilícito (valga como ejemplo sencillo el automóvil, usado infinidad de veces para cometer actos ilícitos y millones de veces para usos legítimos, sin embargo, no se ha tipificado como crimen la figura de "asesinato mediado por automóvil" ni se han abierto capítulos de discusión sobre "delitos automotrices").

La ONU expresa que "por delito cibernético se entiende todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos. En principio, el concepto abarca todo delito que puede cometerse en un medio electrónico. En este marco, la palabra delitos denota formas de comportamiento generalmente definidas como ilegales o que probablemente serán declaradas ilegales en breve plazo".

Entre las especificaciones que plantea la ONU aparecen dos subcategorías de delitos informáticos:

a) el delito cibernético en sentido estricto, o delito informático, que contempla todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos y los datos procesados por ellos, y
b) delito cibernético en sentido lato (delito relacionado con computadoras), que incluye todo comportamiento ilícito realizado por medio de un sistema o una

red informáticos o en relación con ellos, incluidos los delitos como la posesión, el ofrecimiento o distribución ilegales de información por medio de un sistema o una red informáticos.

Veamos algunas cuestiones puntuales. La posesión, ofrecimiento o distribución ilegal de información incluiría seguramente la copia ilegal de contenidos amparados ya por leyes de copyright, lo cual está contemplado en otras normas jurídicas, por lo que no es necesario trabajar sobre eso. Lo mismo ocurre con los "datos personales", que se encuentran amparados bajo las leyes de habeas data.

Mientras que por el lado del delito cibernético en sentido estricto, la dificultad aparece claramente cuando el informe de ONU comienza a explicar de qué se trata esto diciendo por ejemplo que se debe tipificar como delito el "acceso no autorizado, a veces denominado piratería informática", cuando es públicamente conocido que cualquier administrador de redes puede estar en la franja límite de este delito mientras está probando la seguridad de las mismas. Por otro lado, el uso de la palabra "pirata" en un documento de este tenor muestra un nivel de exageración extraordinario al comparar este tipo de acciones con la piratería, que según el diccionario es un acto de bandalismo por parte de piratas, un ladrón que recorre los mares para robar. No se puede tipificar en estos casos lo que se denomina "piratería" como robo, ya que en ninguno de estos casos que se mencionan como "piratería", las personas se "apropian de bienes ajenos" por lo mismo que el documento señala en su comienzo: "los datos como tales sólo pueden controlarse mediante operaciones lógicas y no mediante actos físicos, por lo que resulta difícil tratarlos en estado puro, en el ámbito legal, como si fueran objetos tangibles."

Es decir, los datos no son "cosas"[14] según la definición propia del código civil: "A los efectos de lograr un claro significado jurídico de la palabra "cosa" debemos remitirnos al artículo 2311 del Código Civil de la Nación que define a ésta como los objetos materiales susceptibles de tener un valor." Los datos, en tanto representación de la información para su tratamiento mediante un ordenador, no son objetos materiales y tienen valor marginal cero, porque su reproducción es pasible de multiplicación infinita, por tanto, tampoco pueden ser considerados "bienes". Un bien, en la teoría de los valores y tal como explica el diccionario de la real academia española, es la realidad que posee un valor positivo y por ello es estimable. Los datos no encajan en esta categoría.

Así, la cuestión de los ciberdelitos y el ciberterrorismo es particularmente compleja y provoca fuertes discusiones sobre la tipificación de nuevos delitos que no necesariamente son nuevos, sino que son los mismos delitos ya tipificados pero ejecutados a través de medios innovadores. Toda discusión en este sentido debería enmarcarse en reales mecanismos de control de quienes tendrían capacidad de ejercer vigilancia y considerar como fundamento de toda nueva normativa la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales[15] y el Pacto Internacional de Derechos Civiles y Políticos[16].

Slogan Nro. 5: - "seguridad versus privacidad".

Está casi instalada la idea de que, en pos de mayor seguridad, los ciudadanos debemos resignar nuestro derecho a la privacidad. En la agenda de discusión abierta en torno a la "sociedad de la información", el tema de una red más

segura aparece como prioritario, sobre todo tras los ataques a las Torres Gemelas en septiembre del 2001.

En la lucha contra el terrorismo y el delito, estamos caminando hacia un mundo de control sobre toda la ciudadanía conectada[17] (De ahí también el interés por la "conectividad" en tanto podría convertirse en una nueva forma de control social) El derecho humano a la privacidad, consagrado en la DUDDHH[18], parece ser uno de los más vapuleados en la sociedad de la "información". En los EEUU, por ejemplo, existen hoy leyes que permiten al gobierno realizar vigilancia global sobre todas las comunicaciones e incluso recibir reportes de las lecturas de los ciudadanos en bibliotecas públicas, todo en nombre de la vigilancia global para la "seguridad." La corporación Aol Time Warner reconoció, a través de su Directora Ejecutiva para Política Global Alix Schijman[19], que tiene un mecanismo de control sobre todos los e-mails de sus usuarios, a quienes no informa de tal medida, como política de lucha contra la pornografía infantil. Sin embargo, esta medida que no se somete a consideración de los usuarios, viola el derecho básico a la privacidad, mientras que pone bajo sospecha y vigilancia a toda la ciudadanía que utiliza esos servicios, sin que medie autorización judicial ni monitoreo ciudadano alguno.

La vigilancia no sólo se efectúa a través de las redes, sino incluso a través de cámaras de video instaladas en diferentes sitios incluyendo tanto ámbitos públicos como vigilancia en puestos de trabajo (es notable la cantidad de cámaras de vigilancia callejera instaladas en ciudades como Barcelona por ejemplo).

Aclaremos un punto: seguridad no debe oponerse a privacidad, más bien debe complementarse. El respeto del derecho a la privacidad debe estar basado en un sistema de comunicaciones seguras por el cual ante cualquier otra cosa, se prioricen los derechos ciudadanos y políticos.

En la puja ficticia de "seguridad vs. Privacidad" viene triunfando la seguridad y por amplia mayoría. Por ejemplo, la "criptografía" es considerada por muchos países, incluyendo Argentina, como un arma de guerra. En 1998, 33 países reunidos en el Congreso de la Paz de La Haya firmaron el acuerdo de Wassenaar que incluye las tecnologías de cifrado complejo como armas de guerra. [20]... Considerando el nivel de exposición de las comunicaciones electrónicas a través de la red, el derecho a cifrar las comunicaciones privadas debería ser defendido con firmeza[21].

En paralelo también parece ser que el derecho a la privacidad es lo primero que muchos ciudadanos entregan a la hora de recibir algún servicio de la red. Tal vez por desconocimiento de los derechos o sencillamente por no asignarle la importancia fundamental que tienen, todos los días, millones de ciudadanos y ciudadanas entregan su derecho a la privacidad a cambio de algún servicio como una cuenta de correo webmail gratuita. Veamos como ejemplo un caso concreto muy popular: cuando firmamos términos de uso de determinados servicios de correo electrónico de Hotmail cedemos *el derecho a: copiar, distribuir, transmitir, mostrar y comunicar públicamente, duplicar, modificar, traducir y cambiar el formato del envío al proveedor del servicio de correo*[22.] ¿Cuántos firmamos este tipo de cosas sin siquiera enterarnos? ¿Cómo defender un derecho que no se conoce y/o se cede de una manera tan sencilla a cambio de un servicio gratuito?

Trabajar estos temas requiere en primer lugar la defensa de nuestros derechos a la privacidad y a la seguridad en forma equitativa y contar con una ciudadanía capacitada y en alerta para resguardar sus propios derechos.

Slogan Nro. 6: - "Una copia más, un músico menos". "Por cada copia 'pirata' desaparece un artista".

Este es el slogan promocional abreviado de Capif, la Cámara Argentina de Productores e Industriales de Fonogramas. El derecho de autor está consagrado en la Declaración Univesal de los Derechos Humanos, pero antes está consagrado también el derecho de toda persona al libre acceso al conocimiento, la cultura y los beneficios del progreso científico. La DUDDHH[23] pretende con este reconocimiento de ambos derechos, establecer un equilibrio justo entre ellos, relación que está lejos de ser justa en el actual régimen.

El actual sistema de copyrights, patentes y marcas, mal denominado bajo la engañosa expresión de "propiedad intelectual"[24] tal como está en estos momentos beneficia mayoritariamente a las grandes corporaciones que administran las creaciones intelectuales, y en muchos casos amenazan con sojuzgar aún más a los países del tercer mundo y frenar cualquier posibilidad de desarrollo de las economías del sur. La disputa entre conocimiento libre y conocimiento monopolizado es crucial en la construcción de las sociedades del conocimiento[25].

El impacto de la estructura libre de la red sobre las obras intelectuales ante una redistribución del conocimiento jamás vista en la historia de la humanidad es fuerte y pone a disposición de las personas una forma original y sustancialmente nueva de compartir y generar conocimiento. La red, tal como está concebida, ataca directo al corazón de las corporaciones de la denominada "industria cultural" al generar mecanismos de libre circulación de arte, música, textos, software, es decir, facilitar más que en ningún otro momento de la historia de la humanidad, el derecho humano al libre acceso al conocimiento y la cultura y todos los beneficios que esto reporte.

Frente a la posición de las empreas discográficas que ven como sus negocios se diluyen en la red a manos de millones de personas que comparten cultura, podemos oponer claramente la alternativa de la música libre y los testimonios como el de Ignacio Escolar, que pide por favor que "pirateen" sus canciones, criticando fuertemente el modelo de las discográficas y avalando la idea de que su sustento fundamental proviene de conciertos, remeras y otras actividades vinculadas con su actividad de músico, que dejan en un lugar mínimo las regalías por derechos de autor[26].

Pero son muy fuertes los intereses que están en contra de esta libre distribución y de esta capacidad de las personas en red de socializar conocimiento a un costo marginal ínfimo. Una fuerte discusión se da en torno a las leyes que regulan los monopolios de "propiedad" intelectual. Lo cierto es que es urgente revisar y cuestionar las políticas de patentes y copyrights y no dejarse engañar por clichés.

Ya que en defensa de la apropiación privada del conocimiento vamos camino a un sistema de control cada vez más estricto sobre la libre distribución de conocimiento. Las grandes corporaciones nucleadas en lo que se denomina TCG, Trusted Computing Group, antes conocido como Trusted Computing Platform Alliance (TCPA), han desarrollado lo que se denomina "Trusted Computer", o "informática fiable"

<http://linuca.org/body.phtml?nIdNoticia=207>. TCPA es una alianza de Microsoft, Intel, IBM, HP y AMD que promueve un estándar para un ordenador "más seguro". Su definición de "seguridad" es controvertida; las máquinas construidas según sus especificaciones serán fiables desde el punto de vista de los proveedores de software y la industria del contenido, pero no fiables desde el punto de vista de los dueños. De hecho, las especificaciones TCG transfieren el control último del ordenador a quienquiera que escribiera el software que este ejecuta, quitando el control de la computadora de manos de su dueño para transferirlo a la corporación desarrolladora del software[27]. De esta manera, los millones de usuarios "no fiables" para la industria del contenido quedan anulados en su capacidad de decidir sobre sus computadoras, que tienen la capacidad de impedirles ejecutar lo que la industria no desea que se ejecute. Así, la máquina es fiable para la corporación y convierte en fiable por imposición de limitaciones a su dueño. Si bien se desarrolla para proteger los derechos intelectuales de los derecho-habientes del copyright de los "contenidos", las implicancias de una arquitectura de control sobre la ciudadanía y los países puede tener un alto impacto.

Slogan Nro.7: "En la jungla de Internet... sólo (nombre de ISP) te protege"[28].

¿Cómo es posible que en sólo 3 o 4 años, Internet haya dejado de ser el mundo maravilloso donde todos íbamos a comprar, vender y conseguir pareja y se haya convertido en una jungla?

Hoy, los principales proveedores de Internet se hacen eco de los males de la jungla: **el spam y los virus**. Y prometen fórmulas estratégicas para protegernos de estos agresivos agentes del mal.

Para frenar los cúmulos de spam, los proveedores de servicios de Internet utilizan sistemas de filtrado automático que bloquean los mensajes que contienen determinadas palabras claves o remitentes definidos por el mismo proveedor. De esta manera, la empresa se arroga la función de elegir cuáles son las comunicaciones que enviará a nuestras casillas de correo. Esto es similar a dejar que el cartero elija, en base al color de los sobres, el nombre del remitente o alguna otra variable, qué sobres tirará en nuestros buzones y cuáles considera que nosotros "no deseamos recibir".

En paralelo se ofrece la opción de enviar los mensajes considerados spam a un repositorio que el usuario puede revisar periódicamente para chequear lo que ha ido a parar a la carpeta de "indeseables".

Otra es la historia con los virus, protagonistas de portadas de los diarios más importantes del mundo.

Primero, una aclaración: las soluciones al problema de los virus están mucho más cerca de lo que se propagandiza en los medios: la solución a los virus es utilizar un sistema operativo y aplicaciones estables y seguras[29] y no sistemas llenos de fisuras y grietas de seguridad.

Lo que ocurre en los medios de comunicación con relación a los virus es que están siendo usados para afianzar la campaña de criminalización del mundo hacker y promover la descarga de actualizaciones (parches de seguridad) del sistema operativo hegemónico, sin que ninguna de las personas que lo utilizan sepa realmente qué es lo que está obligado a descargar a su computadora y cuáles son las consecuencias de esto.

Existen varios intereses alrededor de los virus.

En primer lugar aclaremos algunas cuestiones que tienen que ver con el desarrollo social de los sistemas. Si un hacker detecta una falla de seguridad en un sistema libre, recibirá un fuerte reconocimiento de su comunidad si logra solucionarlo. En cambio, si alguien reporta fallas de seguridad en los sistemas propietarios puede ser acusado del delito de acceder en forma no autorizada a un sistema o red informática, tal como pretende la documentación ya citada de la ONU sobre delitos informáticos. La penalización de este tipo de conductas como "delitos" pondrá en jaque los sistemas mismos de seguridad que pretende defender, ya que privaría a las personas de uno de los recursos más probados de fiscalización de seguridad en las redes.

Pero hay mucho más detrás de los virus. Existe un negocio montado alrededor de los virus que tiene que ver con las empresas proveedoras de "antivirus". El uso masivo de sistemas operativos no permeables a los virus terminaría con el negocio de estas empresas.

Mientras tanto, los usuarios de computadoras basadas en software propietario siguen en permanente riesgo, por un lado, por la cantidad de grietas de seguridad de estos sistemas[30] a punto tal que el propio gobierno de los EEUU ha recomendado dejar de usar algunos de los programas propietarios más divulgados. A esto se suma la no responsabilidad por parte de la empresa proveedora ante las pérdidas provocadas por esta causa y la necesidad permanente de actualizar, bajar parches y mantener la computadora conectada a la red central de la empresa desarrolladora de software, obligando al usuario a mantener una confianza ciega frente al proveedor que por términos de licenciamiento priva al ciudadano del derecho a conocer el funcionamiento de su computadora.

Mientras tanto, los diarios del mundo se hacen eco de algún adolescente brillante que ha logrado programar algún virus capaz de infectar millones de computadoras del planeta provocando estruendosas pérdidas a millones de personas y empresas del mundo. ¿Es lógico que las empresa sigan sometidas a semejantes riesgos financieros habiendo soluciones inmediatas y confiables?

Slogan Nro. 8: "La brecha digital se reduce con acceso a las nuevas tecnologías de información y comunicación."

En primer lugar hay que aclarar que la idea de **brecha digital** que divide al mundo entre "conectados" y "no conectados" no es otra cosa que una manifestación más, y seguramente no la más importante, de las brechas sociales que dividen al mundo no sólo entre quienes acceden o no a las TICs, sino, entre quienes reciben alimentación básica o no, quienes tienen acceso a agua potable, alimento, abrigo, salud y educación. En un planeta con más de 800 millones de personas sin alfabetización básica, hablar de la "brecha digital" como prioridad parece un despropósito. Sin embargo, es importante discutir esto, ya que es una brecha más y por tanto un problema para nuestro futuro y el de todas las regiones menos desarrolladas del planeta. Pero veamos esto con otra perspectiva.

Ciertamente, el acceso a la infraestructura es fundamental para reducir la brecha digital, pero no es suficiente. Los programas de conectividad no parecen ser efectivos si no se los acompaña con políticas educativas, sanitarias y de comunicaciones para que las personas se apropien y hagan un uso socialmente significativo de las nuevas TICS. ¿Qué significa el uso socialmente

significativo? Eso puede discutirse según los contextos sociales y culturales, pero una cosa es clara y cierta: sin una política general de inclusión, el cableado y la instalación de TICs no garantiza la reducción de la brecha digital, si es que se toma la decisión política de trabajar para angostar la publicitada brecha.

La noción de Brecha Digital es otro concepto construido en el marco del proyecto de "sociedad de la información" y como tal, antes de correr a solucionar el problema, es necesario indagar críticamente las circunstancias que lo rodean y las reales implicancias del mismo.

¿Cuál es nuestro rol en tanto comunicadores sociales frente a esto?

Estos slogans han impactado y prometen impactar todavía muy fuerte en el "imaginario de la sociedad de la información". Desde los medios de comunicación masivos se ha hecho mucho para instalar estos conceptos. Mientras que en los ámbitos de la comunicación social y las ciencias sociales en general, todavía hay una fuerte brecha en relación al análisis de todos estos conceptos. El rol de los comunicadores en la denominada "sociedad de la información" es clave pero aún no aparece como protagónico.

El mundo de la ciencia y la tecnología es cada vez más complejo y difícilmente accesible a las personas con formación humanística. En muchos de estos campos, las humanidades han quedado rezagadas, sobre todo frente a esta lucha en la que recién aparece un involucramiento tenue de las ciencias sociales. El campo del impacto de las nuevas TICs en el desarrollo y la sociedad de redes ha sido estudiada mucho ya por investigadores como Manuel Castells por ejemplo, pero muchos de ellos no han llegado a vislumbrar claramente la lucha contra el control monopólico del conocimiento.

En el mundo de los hackers, esta lucha lleva ya más de 20 años y fue originada por programadores, matemáticos, físicos, hombres y mujeres de ciencias duras[31].

Los errores clásicos hasta ahora en esta materia podrían caracterizarse de la siguiente manera:

- El primero fue y sigue siendo en muchos casos repetir la mayoría de estos clichés que aquí presentamos, que han sido reelaborados y reproducidos por una enorme cantidad de actores sociales involucrados, incluso del mundo académico.
- El segundo fue y sigue siendo el camino contrario al primero: el surgimiento de una forma de "luddismo" teórico y fuertemente crítico de la tecnología en sí, considerando que la tecnología es globalizadora y globalizante y que las ciencias duras son determinísticas mientras se desconoce la existencia de construcciones colectivas de resistencia social global de las cuales es imprescindible aprender. La cultura de los hackers y los movimientos sociales de software libre son una de las piedras angulares de la lucha.
- El tercero es considerar que las tecnologías son sólo herramientas. La perspectiva "instrumental" de las tecnologías impide comprender el mundo cultural actual en el que la ciudadanía debe actuar de pleno derecho. No comprender la cultura de la nueva era, la lucha por la libertad del conocimiento, pone piedras en el camino para la apropiación plena, justa, socialmente sustentable de las nuevas tecnologías para

contribuir en la construcción democrática de las sociedades del conocimiento basada en los derechos fundamentales.

La lucha por la libertad y la democratización del conocimiento es una macro-lucha a escala global que debemos librar y debemos hacerlo con redes (sociales y técnicas), tecnología y conocimiento. Pero esta lucha sólo se puede luchar deshaciéndonos de los clichés instalados acríticamente en el sentido común y de los temores que se nos presentan a la hora de aprender un idioma que nos desafía a comprender algo nuevo y muchas veces complejo.

Esta es una puja real hoy, en frentes distribuidos de todo el planeta: en cada computadora controlada por uno u otro sector de la lucha, en cada sistema operativo que se instala, en cada niño que aprende simplemente a usar una computadora o aprende a leer y dominar la técnica en profundidad. En cada opción que cada ciudadano o ciudadana de la red haga, decide el futuro de la red y con él, el de nuestras sociedades futuras. Puede parecer una lucha mesiánica o incomprensible para muchas personas, sobre todo para aquellas que dia a dia luchan por el sustento, la salud y los derechos básicos. Pero es la lucha en marcha, la lucha por el control del conocimiento que nos hará libres o esclavos: una sociedad de la información o sociedades del conocimiento libre.

Referencias

1. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote1ancwww.itu.int/wsis <http://www.itu.int/wsis>
2. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote2ancArmand Mattelart - Historia de la Sociedad de la Información. Paidos Comunicación. 1ra. Edición en Argentina. 2003. ISBN 950-12-7532-9
3. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote3anc<http://www.dotforce.org/reports/it1.html>
4. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote4anc<http://www.opendemocracy.net/debates/article-3-85-1953.jsp>
5. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote5ancEl propio Bill Gates, fundador de la empresa Microsoft, reconoció que prefiere que se copie ilegalmente software de su empresa para crear “adicción”, y luego cobrar licencias por su uso. “Although about three million computers get sold every year in China, people don’t pay for the software. Someday they will, though. And as long as they’re going to steal it, we want them to steal ours. They’ll get sort of addicted, and then we’ll somehow figure out how to collect sometime in the next decade.” Bill Gates, Julio 20, 1998 Revista Fortune
6. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote6ancArtículo 27 Toda persona tiene derecho a tomar parte libremente en la vida cultural de la comunidad, a gozar de las artes y a participar en el progreso científico y en los beneficios que de él resulten.
7. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote7ancEste concepto fue desarrollado por Lawrence Lessig en su libreo “El código y otras leyes del ciberespacio”. Ver <http://www.lessig.org/>
8. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote8ancPara ampliar el debate sobre “alfabetización informática” ver: Busaniche, Beatriz, “Analfabetización informática o por qué los programas

porpietarios fomentan el analfabetismo" <http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/analfa/>

9. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote9ancPara ampliar este debate sobre el uso de software por parte del Estado <http://www.hipatia.info/docs/dsl/> Trabajo realizado por la Organización Hipatia <http://www.hipatia.info/>
10. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote10ancSoftware Libre según la conceptualización de la Free software Foundation http://www.fsf.org/philosophy/free-sw.es.html. "Software Libre" se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. De modo más preciso, se refiere a cuatro libertades de los usuarios del software:
    - La libertad de usar el programa, con cualquier propósito (libertad 0).
    - La libertad de estudiar cómo funciona el programa, y adaptarlo a tus necesidades (libertad 1). El acceso al código fuente es una condición previa para esto.
    - La libertad de distribuir copias, con lo que puedes ayudar a tu vecino (libertad 2).
    - La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie. (libertad 3). El acceso al código fuente es un requisito previo para esto.
11. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote11ancEn español se recomienda la expresión "software privativo", en tanto es más elocuente que la expresión "software propietario" para describir un tipo de software que priva al usuario de sus derechos básicos frente al mismo.
12. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote12ancArtículo 11 de la Declaración Universal de los Derechos Humanos: "Toda persona acusada de delito tiene derecho a que se presuma su inocencia mientras no se pruebe su culpabilidad, conforme a la ley y en juicio público en el que se le hayan asegurado todas las garantías necesarias para su defensa."
13. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote13anc<http://www.uncjin.org/Documents/congr10/10s.pdf>
14. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote14ancFallo del juez Sergio Torres, del juzgado federal N °12: "una página web no puede asimilarse al concepto de cosa" en la causa sobre el reemplazo del sitio web de la corte suprema de justicia por un recordatorio del aniversario de la muerte de José Luis Cabezas. Fallo emitido el 20 de marzo de 2002. Existe un segundo fallo en este sentido en la causa iniciada contra un ex empleado de la firma Young & Rubicam por enviar virus a la red de computadoras de la empresa, el fallo de la Sala I de la Cámara Criminal y Correcional Federal sobreseyó al acusado al considerar que el envío de virus no podía encuadrarse dentro del delito de daños por el que había sido previamente procesado ya que este delito requiere que "se destruya o inutilice la cosa misma objeto de derechos de un tercero" y que el objeto material del delito sea "un bien mueble o inmueble o un animal" reafirmando así que los programas no son cosas.
15. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ -sdfootnote15anc<http://www.unhchr.ch/spanish/html/menu3/b/a_cescr_sp.htm>

16. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote16anc<http://www.unhchr.ch/spanish/html/menu3/b/a_ccpr_sp.htm>
17. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote17ancPara ampliar esto es recomendable leer - "Democracia vs. Fascismo. Libertad vs. Control. La contradicción fundamental de la sociedad del conocimiento." Saravia / Busaniche <http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/defasoco/>
18. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote18ancArtículo 12 de la DUDDHH: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."
19. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote19anc<http://weblog.educ.ar/sociedad-informacion/archives/002087.php>
20. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote20anc<http://www.pagina12web.com.ar/suplementos/futuro/vernota.php?id_nota=743&sec=13>
21. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote21ancDavid Casacuberta - El derecho a cifrar - <http://espora.org/biblioweb/derechoacifrar.html>
22. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote22anc<http://privacy.latino.msn.com/tou/><http://espora.org/biblioweb/derechoacifrar.html>
23. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote23anc<http://www.unhchr.ch/udhr/lang/spn.htm>
24. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote24anc<http://www.gnu.org/philosophy/words-to-avoid.es.html>
25. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote25anc<http://www.hipatia.info/>
26. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote26anc<http://www.baquia.com/com/20010118/art00001.html>
27. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote27anc<http://linuca.org/body.phtml?nIdNoticia=207>
28. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote28ancLa frase original es "En la jungla de Internet, sólo AOL te protege" Campaña publicitaria de la ISP Aol en Argentina empresa del grupo Aol Time Warner.
29. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote29ancComo por ejemplo los sistemas gnu/linux.
30. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote30ancEl gobierno de los EEUU ha recomendado públicamente dejar de usar Internet Explorer de Microsoft - <http://www.kb.cert.org/vuls/id/713878>
31. http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/bestiario/ - sdfootnote31ancVer los orígenes y fundamento del movimiento GNU en <http://www.gnu.org/home.es.html>

Presentado como ponencia en el Coloquio Internacional de Córdoba "Democracia y Ciudadanía en la Sociedad de la Información: desafíos y

articulaciones regionales". 23 24 y 25 de Junio de 2004 / Escuela de Ciencias de la Información. Universidad Nacional de Córdoba. MESA 1 CONOCIMIENTO Y PODER EN LA SOCIEDAD DE LA INFORMACIÓN. El papel de la información y el conocimiento en la sociedad actual. Consecuencias éticas y políticas. Las transformaciones de los sistemas comunicativos y educativos. El papel de los científicos, los intelectuales, los comunicadores y los educadores.